Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

Misuse of Personal Data by Social Media Giants

Prakhar Tiwari[a]

[a]Guru Ghasidas University, Bilaspur, India

Received 30 January 2023; *Accepted* 18 February 2023; *Published* 22 February 2023

Social media platforms were discovered to connect people but now this technology is driving us apart. There are growing cases of stealing personal data by hackers but in this paper, we are not going to discuss that. Instead, in this paper, we'll discuss the misuse of personal data by social media giants, e.g., Google, Facebook, Snapchat, etc. The rise of social media has produced a significant number of safety and privacy vulnerabilities that had never been present before. The exploitation of big data becomes a more significant issue in terms of computer crimes and privacy concerns as social networks continue to collect enormous amounts of data and computing technologies advance in terms of speed and performance. Social Media companies handle the personal data of their users not appropriately and for that, they have developed an appalling reputation. Documentaries like Netflix's "The Social Dilemma" throws light on how these companies misuse the personal data of their customers and manipulate the minds of people.

Keywords: *personal data, social media, big data, privacy, technology.*

INTRODUCTION: HOW DO THEY COLLECT DATA FROM THEIR CUSTOMERS?

Behavioural, preference, and demographic data of the users are provided to social media platforms, through users' accounts on these platforms. "The stuff you post, like, accept or search about through your devices give this data. Big data companies and scientists, then collect this data and build personas about you that can determine your age and gender, what you like, and

much more."[1] Essentially, "big data companies are creating computer-based personalities based on information collected from your devices, that end up knowing more about you than your family and friends do."[2] Social media companies have the expertise to keep tabs on your friendships. It is frightening that they can monitor your relationships and can predict who your close friends are.[3] These applications also find the people you "should" add to your network. They are capable of doing all these things because when an account is created for the first time, people unknowingly permit to access their phone and email contacts. People do not "read all the terms and conditions of the agreement they are assenting to while signing up." Facebook, according to the Washington Post, "specifically request your permission with this as a way to scan your contacts to find similar users on your social media sites."[4]

Many times, we receive advertisements for the same products we want when we open these media applications. Weirdly, they track their customers' activities, conduct, and browsing history. They are capable of making an impression of what interests their customers by tracking them on the internet. Social media sites may always track your movements by utilising the location features of your device. These media platforms can advertise nearby cafes, shops, and even friends by using the location information on your device. When you sign up for a Facebook account, it requests permission to access your phone contacts or email contacts depending on whether you're using a smartphone or a computer. The site searches your contacts and other users' uploaded contacts for you when you permit it to do so to find users who are already logged into the network. That provides it with a pretty basic idea of whom you know in your social circles—but not how well you know them.

Facebook gives you more questions about yourself, such as "where you went to school", "when you were born", and "where you currently reside", to improve that map. Facebook's mapping algorithms "use every field in your profile and every interaction you have with others through

[1] Ciara Wake, '3 Ways That Social Media Knows You Better Than Your Friends and Family Do' *(Loyola University Maryland,* 2017) <https://www.loyola.edu/academics/emerging-media/blog/2017/3-ways-that-social-media-knows-you-better-than-your-friends-and-family-do> accessed 04 January 2023
[2] *Ibid*
[3] *Ibid*
[4] *Ibid*

that profile as a source of data." They are attempting to ascertain the network's structure, including the locations of the cliques, the individuals who connect them, and who is connected to whom. Facebook can assess your social network once it understands its structure and anticipate (with remarkable accuracy!) both the persons you are most likely to know right now and in the future. It's not magic, it is statistics. There are a predetermined number of "nodes," or individuals, in the network and a predetermined number of "edges," or relationships.[5] As a result, every missing connection between two nodes is statistically possible. However, not all connections are equally likely because not all nodes are made equal.

ALGORITHMS

Algorithms are "the technical device employed by social media networks to rank messages based on their importance rather than publication date". Users can prioritise the content they view first based on how likely they are to interact with it. For instance, algorithms choose which Instagram posts to suggest to you as you scroll through your account or which of your acquaintances' stories to show first on the homepage.[6] Utilizing machine learning, programmers can develop algorithms.[7] The procedure with which algorithms "learn" to perform activities with variable levels of human supervision is referred to as "machine learning."[8] To promote content discoverability, algorithms mediate content engagement through likes and comments. They also govern content flows by positive shadow bans as well as actionable recommendations. Additionally, computers sort and categorise material in ways that provide content producers with rewards and chances for interaction analogous to those found in markets.[9]

The purpose of an algorithm is "to deliver relevant information to users." Algorithms are employed to more naturally sort through the large volume of information that is exposed across

[5] Caitlin Dewey, 'How Facebook knows who all your friends are, even better than you do' (*The Washington Post,* 2 April 2015) <https://www.washingtonpost.com/news/the-intersect/wp/2015/04/02/how-facebook-knows-who-all-your-friends-are-even-better-than-you-do/> accessed 04 January 2023
[6] Maria Alessandra Golino, 'Algorithms in Social Media Platforms' (*Institute for Internet & the Just Society*, 24 April 2021) <https://www.internetjustsociety.org/algorithms-in-social-media-platforms> accessed 04 January 2023
[7] *Ibid*
[8] *Ibid*
[9] Maria Alessandra Golino (n 6)

each social media network. Algorithms generate content that can be more "interesting" for a user, "to the cost of those that are considered irrelevant or low-quality, either generally or to a specific person." Social media sites occasionally make explicit recommendations about the kind of content that they deem to be of a high calibre and hence promote on their platforms. This is about the criteria on which algorithms provide content. Additionally, "it should be remembered that social media sites are actual businesses that receive a portion of their income from marketing." This might involve advertising "a business or piece of content that public pages desire to advertise by paying social media platforms to have the algorithms do it for them."[10] Several considerations are taken into account when developing algorithms.

Some of these variables are content-related, therefore the goal of this kind of algorithmic design is to match a user's interests with postings that the system thinks they will "like based on the user's profile." If "users show interest in a particular tag or category, they are directed to other items in that category." Moreover, algorithms are capable of cooperating. Collaborative filtering "connects users with other users who seem to have similar interests and directs users to posts or videos that they would be interested in watching." This is the result of a previous search for that specific source by a user with a profile similar to yours.[11] In the sense that "they can recognise personal information, such as a user's precise location, and use it in their calculations", algorithms are aware of their context. Additionally, machine learning uses algorithms that mimic human intelligence to improve performance in particular activities, such as making suggestions. This makes it possible for them to recognise and learn about the outside environment.[12]

HOW DO THEY USE THAT DATA?

By grouping the data into user categories, data brokers could now package and sell the entire collection of information for marketing purposes. You might be labelled as a "football aficionado" or a "fitness enthusiast" somewhere, which will direct marketers when they

[10] *Ibid*
[11] *Ibid*
[12] *Ibid*

advertise to you. In general, "every website that is free to use is marketing your participation as its main selling point." This covers "both more general information like hobbies and interests as well as more specific information like names, birthdates, locations, IP addresses, gender, and device IDs."[13] Your use of free social media sites provides their creators with a wealth of information on what performs well and what doesn't, and they can use that information to charge for their "consulting" services on other websites and goods. This could be, for instance, the phrasing of a sponsored post on a social network page that stimulates interaction.

Websites gauge your "attitude" toward various topics. For instance, you may have seen that seemingly benign poll questions were utilised in newspaper pieces behind a paywall. "If you take the time to respond to any questions", the information you provide—which may include your opinions on social and political issues—will be extremely helpful to marketers and advertisers.[14]

Behavioural data, which is connected to engagement, track your physical interactions with social networking websites, from how you move your mouse cursor over the webpage to which one of two new website designs you visit more frequently. This aids the development of new functions that the site's designers hope you'll use more. The greatest approach to ensure you see more ads on social media sites is to keep you around for longer using behavioural and engagement data. For this reason, websites, for instance, have tended to favour content that is divisive or even dishonest. It may draw greater focus and stir up more controversy.

Platforms such as Facebook and YouTube could create tailored advertisements for you "if they have a complete data set on you." "These advertisements will be customized to your preferences, search history, and even your current location." You are the one who is specifically targeted by these actions.[15] Businesses are interested in learning about and purchasing information about your interactions with customer service or user assistance on social

[13] Caroline Delbert, '15 ways we give social media companies personal data' (*Stacker,* 26 October 2021) <https://stacker.com/business-economy/15-ways-we-give-social-media-companies-personal-data> accessed 04 January 2023
[14] *Ibid*
[15] *Ibid*

networking platforms, for instance. Sites can assist businesses in better planning marketing that will work on you "by tracking how you use these and other services."[16]Social media platforms frequently provide "user survey" options "that allow them to steal people's time for nothing in an easy method." They disguise this "as a technique to enhance your user experience, but once more, all it means is that by participating in the surveys, you are giving them more information they can use to develop you as a product to sell to marketers."[17]

Software development kits (SDKs) from third parties are frequently used in mobile apps, which is akin to placing a listening bug in a person's house or workplace. It's difficult for developers to say no—if they even want to—because "marketers pay to insert these data-mining pieces of code into apps."[18] Similar to free websites, free apps rely on your information to generate revenue.[19] Because they are essentially repackaging your photographs and material to display alongside adverts to your friends, social networks require some rights over them to function. The rights "required for these social media businesses to utilise your images and content—royalty-free"—are included in the user agreements you unconsciously check.[20]

When processing cultural content, these various algorithmic design theories have implications. For instance, Engineers can confine or at least direct "the distribution of a particular form of art or knowledge to a given area by instructing computers to construct algorithms depending on the geographic location of users."[21] Both positive and negative effects of algorithmic design can be thought of. Many times, algorithms are "developed to raise awareness or interest in the digital society about a certain issue." As a result, "some users may notice an increase in posts on politics, foreign films, nutrition, and diet in their news feed."[22]However, "the drawbacks of algorithmic design are frequently the subject of contentious debates on the issues surrounding algorithms." These debates frequently centre on "privacy concerns because algorithms use the user's personal information to "know" how to display content on the social media platform (for

[16] *Ibid*
[17] *Ibid*
[18] *Ibid*
[19] *Ibid*
[20] *Ibid*
[21] Maria Alessandra Golino (n 6)
[22] *Ibid*

example, sensitive data such as the geographical location of the user, the friends, and acquaintances they interact the most with, the pages and hashtags that they often search for, etc. are used by algorithms)." "In a similar vein, there are issues with how algorithms affect the views and pursuits of people on social media and, as a result, of the digital world."[23]

"Shadow bans" allow algorithms to prioritise "revenue-generating content while hiding or ignoring particular posts, potentially leading to knowledge gaps." "This component of algorithmic design is contentious since it implies that consumers should be able to choose which content is significant or deserving of admiration." "This could result in a divided and non-objective selection of who and what receives attention. Algorithmic design consequently determines which types of content or topics should be given priority in each feed and which artists, content creators, or brands deserve to gain more visibility than others. As a result, algorithmic design inexorably alters the spread of culture and shapes the digital ecosystem in a certain way."[24]

CONTROVERSIES

"Millions of Facebook users' personal information was illegally obtained by the British consulting company Cambridge Analytica in the 2010s, mostly for political advertising."[25]"The information was gathered using the 'This Is Your Digital Life' app, which data scientist Aleksandr Kogan and his firm Global Science Research created in 2013. The app asked users a series of questions to create psychological profiles of them and used Facebook's Open Graph technology to get the personal information of their Facebook friends. Up to 87 million Facebook profiles' data were collected by the app."[26] "The data was used by Cambridge Analytica to support Ted Cruz and Donald Trump's presidential campaigns in 2016. The British firm was

[23] *Ibid*
[24] *Ibid*
[25] Rosalie Chan, 'The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections' (*Business Insider*, 6 October 2019) <https://www.businessinsider.in/tech/news/the-cambridge-analytica-whistleblower-explains-how-the-firm-used-facebook-data-to-sway-elections/articleshow/71461113.cms> accessed 05 January 2023
[26] Sam Meredith, 'Facebook-Cambridge Analytica: A timeline of the data hijacking scandal' (*CNBC,* 10 April 2018) < https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> accessed 05 January 2023

also widely accused of meddling in the Brexit referendum. However, according to the official investigation, Cambridge Analytica was not involved 'beyond some initial enquiries,' and 'no substantial breaches' occurred."[27]

"Former Cambridge Analytica employee Christopher Wylie revealed information regarding the data misuse via his interviews with The Guardian and The New York Times in 2018. As a result, Facebook's CEO Mark Zuckerberg testified before Congress and the company issued an apology for its part in the data gathering."[28] "The Federal Trade Commission stated in July 2019 that it would punish Facebook $5 billion for privacy violations."[29] "For subjecting the data of its users to a 'serious risk of harm,' Facebook agreed to pay a £500,000 fine to the UK Information Commissioner's Office in October 2019."[30]"For years, other advertising companies have employed different psychological targeting techniques, and in 2012, Facebook patented a similar method. However, Cambridge Analytica's candour about their procedures and the standing of their clients—including the Trump presidential campaign and the UK's Vote Leave campaign—brought to public attention the difficulties with psychological targeting that academics have been cautioning against."[31] The incident raised people's awareness of privacy issues and the impact of social media on politics. Twitter saw a surge back then for the online movement #DeleteFacebook.

"Senator Ted Cruz of the United States worked with Cambridge Analytica in 2016 to support his presidential campaign. Cruz reportedly provided $5.8 million in services to the company,

---

[27] 'Cambridge Analytica 'not involved' in Brexit referendum, says watchdog' (*BBC,* 7 October 2020) <https://web.archive.org/web/20201009211245/https:/www.bbc.co.uk/news/uk-politics-54457407> accessed 05 January 2023

[28] Alexandra Ma, 'Everyone is talking about Cambridge Analytica, the Trump-linked data firm that harvested 50 million Facebook profiles - here's what's going on' (*Business Insider,* 19 March 2018) <https://www.businessinsider.in/tech/everyone-is-talking-about-cambridge-analytica-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-heres-whats-going-on/articleshow/63369055.cms> accessed 05 January 2023

[29] Julia Carrie Wong, 'Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports' (*The Guardian,* 12 July 2019) < https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations> accessed 5 January 2023

[30] 'Facebook agrees to pay Cambridge Analytica fine to UK' (*BBC,* 30 October 2019) <https://www.bbc.com/news/technology-50234141> accessed 05 January 2023

[31] Sandra C Matz & Ors, 'Privacy in the age of psychological targeting' (*Science Direct*, 2020) <https://doi.org/10.1016/j.copsyc.2019.08.010> accessed 08 January 2023

according to the Federal Election Commission. This was the beginning of Cambridge Analytica's development of individual psychographic profiles, despite the company's relative obscurity at the time. Then, using this information, customised ads were made for each person to influence their decision to support Cruz."[32]

"The information was utilised by Donald Trump's presidential campaign in 2016 to create psychographic profiles, which identified users' psychological traits based on their Facebook activity. With the help of this data, the Trump campaign team was able to micro-target specific US voters with relevant ads about the candidate. Ads were divided into various groups, primarily according to whether or not viewers were Trump loyalists or potential swing voters. The CEO of Cambridge Analytica explained that the trick was to figure out who might be persuaded to support their client or deterred from supporting their rival. Trump's supporters received images of him triumphantly winning as well as information about polling places. Instead, photos of Trump's more well-known supporters and disparaging images or thoughts about his rival, Hillary Clinton, were frequently displayed to swing voters. For instance, 'Make America Number 1 Super PAC' used the information acquired particularly to attack Clinton through carefully crafted ads that accused Clinton of wrongdoing to elevate Trump as a superior presidential contender." [33] There were allegations that Cambridge Analytica was also hired by a political party in India in the 2010 state elections. However, this cannot be proved because of the inadequate information in the public domain.

Now, the question arises if a third-party application alone can do so much through Facebook, then what would be the extent of harm Facebook itself could do with its users' data? Data is the new oil and the world has given enough data to these tech giants to manipulate people's opinions. Many of us have experienced the power of algorithms used in social media. There are many instances where we are shown advertisements of the same thing which we want at the

[32] Patrick Svitek & Haley Samsel, 'Ted Cruz says Cambridge Analytica told his presidential campaign its data use was legal' (*The Texas Tribune,* 20 March 2018) <https://www.texastribune.org/2018/03/20/ted-cruz-campaign-cambridge-analytica/> accessed 09 January 2023

[33] Alvin Chang, 'The Facebook and Cambridge Analytica scandal, explained with a simple diagram' (*Vox,* 2 May 2018) <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram> accessed 10 January 2023

time. Sometimes, we just think of a product and an advertisement for the same product appears on our mobile screens. This isn't magic or something rather this is the algorithm that works behind social media platforms. As we've already discussed that social media platforms know everything about us, our likes, dislikes, friends, relatives, location, etc., and they use our data to show characterized advertisements to us. Through this kind of advertisement, they can sell us anything be it any product or service or any political ideology.

Today, social media giants have the power of manipulating the world's perspective about any social, economic, political, religious, cultural, and environmental issue. They can do this only because of the huge amount of people's data they have with them. This is one of the biggest challenges humanity is facing. It will have a catastrophic effect on the whole of humanity and not just one country. It is bad, especially for democracies of the world. If social media giants today can change the election results in the world's oldest democracy, they can do it in any other democracy as well or probably they had done the same. People don't want to admit that propaganda works. Because to admit it means confronting our susceptibilities, horrific lack of privacy, and hopeless dependency on tech platforms ruining our democracies on various attack surfaces.

DATA PROTECTION LAWS

As more social and business activities move online, the importance of data security and privacy is becoming more popular and widespread. Significant concerns are raised by the collection, use, and sharing of personal information with outsiders without the knowledge or consent of the client. "137 out of 194 nations, according to the United Nations Conference on Trade and Development (UNCTAD), have laws in place to ensure the protection of personal information."

OVERVIEW OF GDPR

The General Data Protection Regulation (GDPR) is a set of rules that govern how personal data from persons inside and outside the European Union is collected and processed. After being passed in 2016, the GDPR took effect in its entirety two years later. It attempts to give users power over their data by holding businesses responsible for how they manage and treat this

data. Those websites that draw viewers from Europe are required to abide by the law since it applies regardless of where the websites are situated, even if they don't specifically sell their goods or services to EU people.

It was developed to regulate how businesses handle and make use of the private information they collect online from clients. It took the place of an earlier law called the Data Protection Directive. Additionally, it offers instructions for transferring data, whether it is done partially or entirely automatically. The law makes it difficult for businesses to use vague or imprecise language on their websites to mislead customers. Additionally, it guarantees that:

- Website users are informed of the data collected.
- By clicking a button or taking another action, visitors voluntarily consent to this information collection.
- Websites promptly inform users if any of their personal information is ever compromised.
- An evaluation of the site's data security is required.
- Whether an existing employee may fulfill this role without needing to acquire a dedicated data protection officer (DPO).

These requirements may be more stringent compared to those in the area where the site is located. Visitors must be aware of how to contact the DPO and other relevant staff members to exercise their EU data rights, which include the choice to have their presence on the website erased among other options. The site must also hire more staff and obtain more resources to fulfill such requests. To further protect consumers' data, the GDPR requires that any personally identifiable information (PII) that websites collect be either anonymized (rendered anonymous) or pseudonymized (the consumer's identity is replaced with a pseudonym). This makes it possible for companies to conduct more detailed data analysis, such as figuring out the normal debt ratios of their clients in a particular location—a calculation that could otherwise go beyond the basic goals of data acquired for figuring out creditworthiness for a loan.

Regardless of where websites and residents are based, the legislation applies to all 27 members of the EU and the EEA. As a result, it must be followed by any websites that draw users from Europe, even if they don't particularly target consumers in the EU. Thus, even if the data of an EU citizen is stored in the United States, the legislation still applies to it. A U.S. person living in the EU is similarly protected whenever they visit websites headquartered in the EU.

In India

Awareness regarding personal data security in India aroused back in 2016 when to better represent its connection with its parent business, Facebook, WhatsApp Inc., the most used messaging platform, amended its privacy policy to state that they will start distributing user data to them.[34] The amended privacy policy of WhatsApp was challenged in the Delhi High Court. In the Karmanya Singh Sareen case[35], the Delhi High Court issued the following directives to safeguard the interests of "WhatsApp" users[36]:

- Before September 25, 2016, if users want to entirely cancel their WhatsApp accounts, all of their information, data, and details should be removed from WhatsApp's servers and should not be shared with Facebook or any of its group companies.
- Users who choose to stay in WhatsApp will not have their current information, data, or details shared with Facebook or any of its group companies after September 25, 2016.
- Respondent Nos. 1 and 5, who is the Union of India, the Department of Telecommunications, and the Telecom Regulatory Authority of India Ltd. (TRAI) respectively, must take into account the problems with the operation of Internet messaging services like "WhatsApp" and decide as soon as possible whether it is possible to bring them under the statutory regulatory framework.

[34] Lily Hay Newman, 'WhatsApp Has Shared Your Data With Facebook for Years, Actually' (*Wired,* 8 January 2021) <https://www.wired.com/story/whatsapp-facebook-data-share-notification/> accessed 10 January 2023
[35] *Karmanya Singh Sareen v Union of India* MANU/DE/2607/2016
[36] *Ibid*

After the Delhi High Court verdict, the petitioners, "Karmanya Singh Sareen and Shreya Sethi, filed a Special Leave Petition in the Supreme Court challenging the Delhi HC verdict."[37] The case is still pending in a constitutional bench of the apex court. Meanwhile, in 2017, "a committee headed by retired Supreme Court Judge Justice BN Srikrishna was formed by the Union Government to create a framework for data protection in India."[38] As we all know that in the landmark case of K.S. Puttaswamy, in the year 2017, the apex court held the "Right to Privacy" as a "fundamental right under article 21 of the Constitution of India".[39] This prompted the government to start working on new data protection laws for the nation. In 2018, "the committee submitted its report on 'Data Protection Framework' to the Government."[40]

"In January 2021, yet again rolled out a new privacy policy and had given users time till 28 February 2021 to accept and update."[41] Some of the elements of the new privacy policy sparked discussions and appeared contentious: For instance, the new policy does not provide users with the chance to refuse the sharing of their data with WhatsApp's parent company, Facebook Inc. "WhatsApp has extended the deadline to update to May 15th, 2021 in response to public outcry."[42] The amended "Terms of Service and Privacy Policy" issued by WhatsApp Inc. in 2021 prompted "the Competition Commission of India (CCI) to commence suo moto proceedings and direct its investigative arm, the Office of the Director General (DG), to conduct an investigation."[43]

---

[37] 'Whatsapp-Facebook Privacy' (*Supreme Court Observer)* <https://www.scobserver.in/cases/karmanya-singh-sareen-union-of-india-whatsapp-facebook-privacy-case-background/> accessed 10 January 2023

[38] 'Justice Krishna to head expert group on Data Protection Framework for India' (*PIB,* 1 August 2017) <https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420> accessed 10 January 2023

[39] *Justice KS Puttaswamy & Anr v Union Of India & Ors* AIR (2017) SC 4161

[40] Surabhi Agarwal, 'Justice Srikrishna committee submits report on data protection. Here're its top 10 suggestions' (*Economic Times,* 28 July 2018) <https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-committee-submits-report-on-data-protection-herere-the-highlights/articleshow/65164663.cms> accessed 10 January 2023

[41] Tech Desk, 'WhatsApp updates terms of service and privacy policy: Why you need to accept it' (*Indian Express,* 16 January 2021) <https://indianexpress.com/article/technology/social/whatsapp-new-2021-terms-of-service-and-privacy-policy-new-changes-accept-or-delete-7134815/> accesses 10 January 2023

[42] Kanishk Gaur, 'WhatsApp's new policy: A privacy bogey?' (*Financial Express,* 14 June 2021) <https://www.financialexpress.com/life/technology-whatsapps-new-policy-a-privacy-bogey-2270823/#:~:text=However%2C%20due%20to%20an%20intense,Data%20Protection%20Bill%20in%20India.> accessed 10 January 2023

[43] *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users* Suo Moto Case No 01/2021

Under the Competition Act of 2002[44], it was prima facie believed that the 2021 Privacy Policy, which permitted the sharing of user data among Facebook Inc. (currently Meta Platforms Inc.) entities, constituted an abuse of dominance. The messaging service discriminates against Indian users in comparison to users in Europe when it comes to the option to reject the new privacy policy, the government claims. Due to legislation in the European Union (EU) known as the General Data Protection Regulation (GDPR)[45], WhatsApp users in Europe have the option to refuse the new privacy policy, which protects them from sharing data with Facebook, or gives them the choice to reject WhatsApp's new terms of service. A writ case "challenging the policy was filed before the Delhi High Court not long after it was announced."[46] The new privacy policy, it was said, allowed WhatsApp to profile users' data without any oversight from the government, violating the fundamental right to privacy. Therefore, the said CCI Order was initially contested by WhatsApp and Meta before the Delhi High Court because the CCI proceeded to direct an investigation into the 2021 Privacy Policy despite the Supreme Court's ongoing constitutional challenge to the policy. At first, a single-judge bench of the Delhi High Court dismissed the motions and ruled that the CCI would not lose its legal authority under the Act simply because a case involving the underlying arrangement was ongoing before the Supreme Court or a High Court. The Delhi High Court's two-judge quorum upheld the single judge's decision following an appeal.

The Delhi High Court Order was subsequently contested by WhatsApp and Meta before the Supreme Court, who once more argued that the CCI lacked jurisdiction while the Supreme Court was considering the legality of the 2021 Privacy Policy. However, the Supreme Court firmly decided that no intervention was necessary and supported the market regulator in its decision.[47] It was stated that after the CCI established a prima facie case of a breach of the Act's

[44] Competition Act 2002
[45] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L 119/1
[46] Akshita Saxena, 'Breaking- 'Virtually Gives 360-Degree Profile Into A Person's Online Activity': Whatsapp's New Privacy Policy Challenged In Delhi High Court' (*LiveLaw,* 14 January 2021) <https://www.livelaw.in/top-stories/whatsapp-privacy-policy-delhi-high-court-fundamental-right-to-privacy-168410> accessed 11 January 2023
[47] KR SRIVATS, 'Petitions dismissed. Supreme Court dismisses WhatsApp, Meta appeal against CCI probe' (*The Hindu Business Line,* 14 October 2022) <https://www.thehindubusinessline.com/info-tech/supreme-court-

provisions and began its procedures in response, the proceedings could not be said to be without jurisdiction.[48] The bench stated that the CCI's investigation should not be postponed any further. Additionally, the Delhi High Court's findings would only be considered prima facie or speculative and all arguments made available to Meta and/or WhatsApp would be open for examination by the CCI on their own merits.

Justice BN Srikrishna Committee, which was discussed earlier, "proposed a draft Personal Data Protection Bill in its final report in 2018."[49] The 2019 Bill was revised by Parliament once more, and it was clear that the 2018 Bill had changed significantly. The 2019 Personal Data Protection Bill was the name of the new law. The 2019 bill was sent to Joint Parliamentary Commission on December 11, 2019, for study and consideration. Originally scheduled to be presented to Parliament during the 2020 Budget Session, the JPC instead presented its report to both houses of Parliament on December 16, 2021, after receiving a 2-year extension. The JPC Report includes draft legislation dubbed the Data Protection Bill, 2021 as well as a list of policy recommendations on the subject and an examination of various sections of the 2019 Bill. However, the government of India, in an engrossing move, withdrew the 2019 bill from the Parliament on August 2022 by saying that the bill will be replaced by a new one with a more comprehensive legal framework. And as promised, it came up with a new bill titled "Digital Data Protection Bill, 2022" in November 2022.

2019 BILL

Foreign technology corporations that store the majority of Indians' data abroad criticised the measure because it compelled "all fiduciaries to store a copy of all personal data in India". But depending on the nature of the data, the Bill divides it into three groups and requires storage within Indian borders. The first group is Personal data which includes information that can be used "to identify a specific person, such as name, address, etc." Second group is "Sensitive

dismisses-whatsapp-meta-appeal-against-cci-probe/article66009649.ece#:~:text=The%20Supreme%20Court%20on%20Friday,CCI%20order%20directing%20a%20probe.> accessed 11 January 2023

[48] *Ibid*

[49] Surabhi Agarwal (n 40)

Personal Data" (SPD). "Financial, health, sexual orientation, biometric, genetic, transgender status, caste, and religious beliefs" are some examples of SPD. The third group is Critical Personal Data (CPD) which means "anything that the government may at any time deem crucial, such as information related to the armed forces or national security".

"Data mirroring" is the process of continuously "copying data (transaction logs) to a second storage location" while maintaining synchronisation between the two locations to increase availability and provide active backup and redundancy if the primary server fails or is negatively affected by a disaster. Microsoft SQL Server 2005 was the database software that first featured it. The Bill does away with the need for data mirroring (in the case of personal data). Only individual consent is needed for data transfer to foreign countries. SPD must only be stored in India, according to the Bill. Only under specific circumstances, such as with a Data Protection Agency's (DPA) clearance, can it be handled abroad. Whereas, it is provided that CPD must be processed and stored in India. The Bill requires fiduciaries to submit any non-personal data requested by the government to them. Data that has been anonymized, such as demographic or traffic trends, is referred to as non-personal data. This kind of information, which many businesses rely on to finance their business models, was not included in the 2018 draught. Additionally, the Bill mandates that social media businesses, who are classified as important "data fiduciaries" based on the "volume and sensitivity of the data" they handle, create their user verification system. The goal of this is to make users less anonymous and stop trolling.

The Bill asks for the establishment of a "Data Protection Authority" (DPA), which will be in charge of definition-making, evaluations, and audits. Each organisation will have a "Data Protection Officer" (DPO), who will work closely with the DPA on matters such as auditing, handling complaints, maintaining records, etc. The "Purpose limitation" and "Collecting limitation" clauses that are proposed in the bill restrict the collection of data to that which is required for "clear, precise, and legitimate" purposes. Additionally, it gives people the freedom to access and transfer their data as well as the right to data portability. Secondly, it gives people the freedom to access and transfer their data as well as the right to data portability.

Last but not least, it establishes the right to be forgotten. This right to revoke consent for data collection and dissemination has its origins in the "General Data Protection Regulation" (GDPR), a statute of the European Union. According to the bill, the fines would be "Rs. 5 crores, or 2% of global turnover, for small infractions and Rs. 15 crores, or 4% of global turnover, for more major infractions". Additionally, the company's chief executive officer could spend up to three years in prison.

Exemptions: The bill gives the power to the Union Government to "exempt any agency of the government from the application of the legislation". It includes exemptions for processing data without a person's consent for "reasonable purposes," such as securing the state, uncovering fraud or illegal activity, preserving evidence in legal proceedings, handling medical emergencies, credit scoring, running search engines, and processing publicly accessible data.

WHY IT WAS WITHDRAWN?

The Union government "withdrew the Personal Data Protection (PDP) Bill, 2019 from Parliament on August 4, 2022". Normally, the administration is free to make modifications to a measure once it has been introduced into Parliament before it is taken up for final deliberation and vote. Governments typically do this, for instance, if they want to take recommendations from legislative committees into account. If it had simply been a matter of incorporating the JPC's recommendations, this would have been the most likely course of action. But in this circumstance, the administration has completely abandoned the bill. After several rounds of public input, the bill was sent to the joint expert committee of the Indian Parliament for consideration. After conducting additional stakeholder interviews, the JPC proposed revising the draught Bill in late 2021. It has been highlighted that out of the 99 provisions of the Bill, the JPC ultimately recommended 81 amendments.

The 2019 Data Privacy Bill was largely retracted as a result of resistance from leaders in the digital economy, members of civil society, and the Government's Expert Committee. Indian firms that rely on data were frightened by limitations on the usage and export of that data. At the same time, Indian think tanks and civil society organisations criticised Bill's provisions that

gave the Indian government more surveillance capabilities and exempted their operations from oversight. Additionally significant is the JPC's recommendation that non-personal data be added to Bill's scope. The only regulatory precedent is a report from an expert committee on non-personal data from late 2020, which is the first time the regulation of non-personal data has been raised in India. It is (obviously) difficult to incorporate non-personal data protection aspects into a personal data law that is similar to the GDPR, which is another reason why the 2019 Bill was dropped. It has also been suggested that "all social media platforms that do not serve as intermediaries be recognised as publishers, held liable for the content they contain, and held accountable for the content posted on their platforms by users with unverified accounts". The government should also specify the voluntary user verification procedure and the minimum number of users for major social media platforms.

2022L

The Draft Digital Personal Data Protection Bill, 2022 was introduced in the Parliament in November 2022, i.e., 3 months after the withdrawal of the 2019 bill. The Bill will apply to the handling of digital personal data processed in India, whether the data is obtained online or offline and then converted to digital form. If the processing is being done to offer products or services or create profiles of people in India, it will also apply to processing done outside of India. The draft bill contains seven principles in its Preamble. They are: -

- Firstly, "usage of personal data by organisations must be done in a manner that is lawful, fair to the individuals concerned and transparent to individuals".
- Secondly, "personal data must only be used for the purposes for which it was collected".
- The third principle talks of "data minimisation".
- The fourth principle "emphasizes data accuracy when it comes to collection".
- The fifth principle "talks of how personal data that is collected cannot be 'stored perpetually by default' and storage should be limited to a fixed duration".
- The sixth principle says "there should be reasonable safeguards to ensure there is 'no unauthorized collection or processing of personal data'".

- The seventh principle states that "the person who decides the purpose and means of the processing of personal data should be accountable for such processing".

Two crucial rights for data principals are absent from the DPDP Bill, 2022. The right to data portability is the first. The "right to data portability" permitted the data principal to obtain all personal information they had given the data fiduciary and information the data fiduciary generated about them while processing it to deliver its services in a structured format. Giving data principals a wider range of platform options, this increased consumer welfare by fostering competition among data fiduciaries. For instance, the data principal may ask for the transfer of their data to another social networking platform if they were unhappy with the one they were presently using and use that platform's services without having to re-enter all of their personal information. This privilege is not provided for in the DPDP Bill, 2022.

The "right to be forgotten" is the second right that is sacrificed. Although not a fundamental right, the "right to be forgotten" enables the "data principal" to request that the "data fiduciary" stop disclosing their personal information going forward. The right to information for everyone else and the freedom of speech and expression must be balanced with this. This right is incorporated into the "right to erasure" by the DPDP Bill, 2022. The "right to freedom of speech and expression" of other people is compromised by this confusion between the broad right to erasure and the right to be forgotten, which is unique to the revelation of personal data. The DPDP Bill, 2022 maintains the strategy used in its earlier revisions about processing children's data. The "age of digital consent", which is the age at which a person can consent to the processing of their data, is still 18. In order "to process the personal data of children and adolescents under the age of 18", parental or guardian agreement would be necessary.

In the area of cross-border data flows, the DPDP Bill, 2022 significantly differs from the PDP Bill, 2019. A three-tiered classification system based on which personal data could be transported across borders was granted by the PDP Bill, 2019. While the government was interested in limiting cross-border data flows of sensitive personal data and critical personal data to facilitate easy legal access and to maintain "digital sovereignty," these data localization requirements were fiercely contested by the industry because they would result in a significant increase in

compliance and operational costs in the form of higher data storage costs and security risks. By authorising cross-border data transfer to "countries and territories" that have been informed by the Union government, the DPDP Bill, 2022 seeks to strike a balance between these worries. However, the proposed legislation does not include any recommendations or standards for the Union government to take into account while issuing this notification. It is up to the Union government to define the criteria using its authority to make rules.

The current draught significantly narrows the purview of the proposed Data Protection Board of India (DPB) in comparison to the regulatory framework envisioned under earlier iterations of the draught law, where the proposed regulator, the Data Protection Authority, was endowed with significant powers of regulation making, enforcement, and adjudication. The central government has been given the ability to make rules under about 14 of the DPDP Bill's 22 provisions. It would be true to say that the government itself has been vested with the maximum power, for instance, the power to designate "fair and reasonable" purposes for which it may treat personal data without consent is in the hands of the government. Also, the present Bill continues the strategy from the PDP Bill, 2019, and offers several exclusions to the state's processing of personal data. The PDP Bill, 2019, and the DPDP Bill, 2022 differ significantly in how they conceptualise sanctions: -

- The amount of fines that can be levied is substantially larger than what is specified in the PDP Bill, 2019, with a ceiling of 500 crores.
- It does not introduce any offences, in contrast to the PDP Bill, 2019.
- It forbids data principals from suing data fiduciaries for damages they have incurred as a result of unlawful processing, which can be considered a move that disempowers them.
- Fourth, the DPDP Bill, 2022 imposes obligations on data principals in a highly unusual step that may be unique among data protection legislations. A user faces Rs. 10,000 fees for filing frivolous grievances or providing fraudulent documentation while registering for an online service.

HOW WOULD THIS LEGAL FRAMEWORK PREVENT INCIDENTS LIKE THE CAMBRIDGE ANALYTICA SCANDAL?

Facebook – Cambridge Analytica scandal, which was earlier discussed in this article, was the one incident after which the whole world realized the need for a stringent personal data protection law. So, can we now say that this draft bill (if becomes an "Act") prevent the scandals like those mentioned above? Certain provisions in the bill will help to prevent such incidents. They are as follows: -

Users shall be informed regarding the purpose for which their data is being processed in simplified language: Section 6 of the bill provides that the Data Fiduciary shall "shall give to the Data Principal an itemised notice in a clear and plain language containing a description of personal data sought to be collected by the Data Fiduciary and the purpose of the processing of such personal data." It will have a retrospective effect, i.e., if the consent of a Data Principal has been taken before the commencement of this act, then also the Data Fiduciary shall have to abide by this provision. Notice in the simplified language would surely help users to understand the purpose of their personal data processing and reduce the risk of personal data abuse by social media giants or any other data fiduciary for that matter. Users will be aware of the purpose for which their data is being collected.

Consent: Section 7 of the bill provides that consent "means any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement to the processing of her data for the specified purpose." If the consent if taken for any purpose which violates the provisions of this bill shall be an invalid consent. Also, request for taking the consent shall be in a "clear and plain" manner. Again, this would help users to understand technicalities in a better manner. The right to withdraw their consent at any time has also been given. If a user opts to withdraw his consent then the processing of his data will cease to operate within a reasonable time. Further, it has been given that on the refusal to give consent to the processing of more personal data of a user, the data fiduciary cannot stop the services which were being provided earlier. Thus, making the user's consent invulnerable. Lastly, the burden of proof, in any proceeding, to prove that notice

under section 6 was given to the user and consent under section 7 was taken from the user will be upon the data fiduciary. Again, putting the data principle on a higher footing.

Transfer of data outside the territories of India: If this bill becomes an Act, then it would be really difficult for the data fiduciaries to transfer users' data to a foreign country as was the case in the Cambridge Analytica scandal. Storing users' data locally, i.e., Data Localisation was given weightage in the bill. Section 17 provides that the personal data of individuals shall only be transferred, outside India, to the countries recognized by the Central Government as safe. This would help prevent the situations like Cambridge Analytica scandal where the firm Cambridge Analytica was situated, outside the United States of America, in the United Kingdom. However, there are some exceptions regarding this provision in section 18 of the bill.

Right to erasure: Under section 13, the personal data of the users "that is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose" shall be erased. This would prevent the unnecessary retention of users' data. The users can also choose to delete all their data from the database of data fiduciaries.

Grievance redressal mechanism: There is a robust grievance redressal mechanism provided in the bill where a user can register his complaint if he feels that his data is not being used fairly or its processing does not align with the bill, with the Data Fiduciary and if he is not satisfied with them then he can register the complaint with the Data Protection Board, which is provided in the bill.

It is clear from the above-mentioned provisions that this bill would make data collection and process transparent and data fiduciaries accountable. To an extent, this bill will succeed in preventing incidents like such and protecting individuals' data in general but there are things which are still needed to be done to be effective in protecting the personal data of individuals.

WHAT CAN BE DONE FURTHER?

Restrict Psychographic Profiling: "Psychographics is a qualitative methodology used to describe traits of humans on psychological attributes."[50] "Psychographics has been applied to the study of personality, values, opinions, attitudes, interests, and lifestyles."[51] "Two approaches to psychographics include analysis of consumers' activities, interests, and opinions (AIO variables), and values and lifestyles (VALS)."[52] This method, as discussed earlier in this article, was also used in the Cambridge Analytica scandal in 2016. Marketers, advertisers, and researchers can develop thorough "psychographic profiles" of audience segments "by collecting and evaluating this data". These profiles are then utilised to develop pertinent messaging for those categories. This is a significant source of income for wearables, ride-sharing services, online delivery services, social networks, search engines, and other online marketplaces. And even if the Cambridge Analytica incident exposed the misuse of data, psychographic modelling will continue to be regarded as a crucial technique for data analysis to more effectively market to consumers. The 2022 bill has more to do with data mining techniques than psychographics in general. In today's world, Psychographic segmentation has become a key component in almost every sector. This is high time that we put the "right to privacy" and "right to freedom of speech and expression" on a higher footing than the profitability of businesses. Making Psychographic profiles of individuals should be completely banned or at least some restrictions should be put on these, e.g., making these profiles only based on demographic data.

A monopoly of Google and Facebook: From a competition perspective, Google and Facebook have destroyed the market of the online advertising industry. They have a duopoly. They, from the general public, do not charge anything because we, ourselves, are a currency for them. They have our data in exchange. The problem is considerably worse with Google because of its domination in both the operating system and ad network markets. Policymakers and decision-makers acted to safeguard competition in general during the formative years of competition

[50] William D Wells, 'Psychographics: A Critical Review' (1975) 12(2) Journal of Marketing Research 196–213
[51] Jairo Senise, 'Who Is Your Next Customer?' (*Strategy+Business,* 29 August 2007) <https://www.strategy-business.com/article/07313?_ref=> accessed 10 January 2023
[52] *Ibid*

law. This is because they believed that for democracy, an open society, innovation, and a functioning market, competition is a necessary ingredient. When Chicago school economists started to have an impact on US competition policy, they pushed for a concentrated focus on maximising consumer interest. Because of the adoption of this philosophy, competition regulators are now helpless spectators as internet titans ruin our economic and political system. We need to get back to the fundamentals of competition law, even if that means splitting Google into two entities. To prevent them from utilising vertical integration, the operating system should be separated from other services and goods. Start talking about the potential last steps of such a disintegration as a nation. Facebook, similarly, should be split in a country-wise manner. Its subsidiaries like Instagram and WhatsApp should also be split from the parent company and split in a country-wise manner.