

DATA TRADING IN THE DIGITAL ECONOMY

* HARISH RENGANATHAN¹

The article deals with how corporations indulge in illicit trading of user data, what are the laws in India and in other parts of the world that deal with user data and privacy, how is the user affected by the illicit data trading and how are corporations able to wash their hands off in this issue. We shall also deal with this issue from the consumer perspective and how the consumer can educate himself with respect to protecting his privacy from being targeted by companies. The article will also deal with the case of how “data is the new gold” and how it’s used to target consumers. as of how “data is the new gold” and how it’s used to target consumers. as of how “data is the new gold” and how it’s used to target consumers with contemporary examples.

Introduction

In February 2021, in the US, Chinese tech giant agreed to pay \$92 million to settle lawsuits alleging that the company misused the personal information of users and indulged in illicit trading of information behind the closed doors of users. Many lawyers call it one of the largest data privacy related settlements which applied to 89 million users (about twice the population of California), whose data was tracked and sold without their consent. Katrina Correl, one of the lawyers representing TikTok users said that "Social media seems so innocuous, but troubling data collection, storage, and disclosure can happen behind the scenes". Data belonging to minors as young as 6 years were found to have been stolen and sold off behind closed screens. TikTok has been under the scanner for over a year since its raise in popularity due to its parent company ByteDance’s close ties to the Chinese government which has been claimed by many to be an authoritarian surveillance state and an extended arm of the Chinese state, which aims to spread its digital footprint across the globe. These were claimed by Donald Trump, the former President of the United States, who had a cold relationship with China and its policies. This is just one example of how corporate tech giants target user data and sell it off without the consent or the knowledge of the user. This one issue itself raised enough doubts in the mind of netizens as what happens to their data in the hand of big tech corporate giants, and can they really trust them with their privacy. However, the question here is that whether data trading is fair according to global consumer laws and the various modes through which those affected can seek redressal and what're the modes through which compensation can be obtained and help raise awareness among other users.

¹ 3rd Year, B.A; LLB (Hons)SASTRA Deemed to be University

The other issue that is being brought into the limelight is the issue of Artificial Intelligence being used as a spyware by companies and how sometimes they can be used as a weapon to influence your opinions and in short, a handful of people will control and influence your day-to-day life. Legally the user when installing a new app or signing on to something online ignores the terms and conditions page and starts to accept the conditions without reading them. This is a technique used by many app developers to get away with their acts of illicit data trading.

According to a survey by a group called ProPrivacy.com, only 1% of internet users read the terms and conditions and it was easy to get away with putting up ridiculous things in the terms and conditions as many ignored them. So, the question of users themselves being responsible arises here.

Research Question

The question that's frequently being asked here is that how the consumers can be aware of their own rights and privileges that are legally available to them and to raise awareness among netizens that their data is vulnerable and they need to step up to safeguard their privacy. The other question being asked here is how corporate tech giants get away with all such practices.

Why is data valuable?

There's a saying that "data is the new gold". Has anyone wondered why data is said to be the new gold or why so many people are behind it. The first reason is data trading fuels consumerism. In our everyday life, especially while scrolling down through your social media feed, anybody would've come across a product that he had literally thought about buying or had a conversation with a friend regarding that product, then suddenly the person comes across an advertisement in his feed. This is because of his data being insecure and his conversations being overheard by device he owns and operates. This is a case of your privacy being violated by the companies that manufacture your phone, the company that developed the app, and the company that wanted you to see their ad in your social media feed. Sometimes this is done in coordination to enrich consumerism among netizens. Data isn't just demand for the purpose of consumerism, there're various other reasons as to why data is valuable, the reason being it could literally predict anything before it happens. In Japan, data regarding weather patterns influence not just the sale of cosmetics, but can predict massive natural disasters, just by observing and analyzing user data. User data in a geopolitical scale can even be weaponized against adversaries. This is according to Gene Sharp, a political analyst who listed more than 100 ways to paralyze and cripple a state. In his book "From dictatorship to democracy", he talks about how social media can influence political movements without making much noise and how they're proven methods to fuel political movements and overthrow governments.

This was evident in the 2011 Arab spring protests where social media played an important role in instigating protestors to hit the streets and oppose the sitting regime. So, it's a well-known thing that data is weaponized by many to advance their vested interests and suppress the privacy of the masses in general, speaking in both political and general terms. The term data also includes medical data, that is stored by Hospitals and pharmaceutical companies that are traded in the open market. So, data as we all know it its various forms is being targeted by various groups to advance their vested interests, which include spreading consumerism.

Laws regarding data protection

Globally, International privacy laws are guided by 5 principles. The principles are

- 1) **Notice;** Advising netizens of the privacy policies to secure their personal data
- 2) **Choice and consent;** To provide people with choices and consent around the collection of personal data.
- 3) **Access and participation;** To ensure that information is accessed by the correct set of people with the required protocols.
- 4) **Integrity and security;** To ensure that data is secure and there's no unauthorized access to user data.
- 5) **Enforcement;** Ensuring that all providers are aligned with any form of regulation that enforces compliance.

The biggest breakthrough in data privacy laws was the General Data Protection Regulation (GDPR) in 2018 in the European Union. This was recognized by many to have set the standards for many data privacy laws around the world. The characteristic of this legislation include enabling data protection authorities (DPAs) to make binding decisions and issue administrative sanctions including fines, the right to object to processing based on the controller's or public interests, an obligation to notify DPAs and data subjects about data breach, stronger consent requirements including biometric and/or genetic data in the definition of sensitive data and introducing data protection officers (DPOs) as a mandatory role in organizations that process personal data. In the United States, all laws are a patchwork of state and federal legislatures. However, it does have a variety of laws that deal with data privacy. The most referred ones are the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA). While not identical, these state laws are substantially like each other in several key aspects. Like the EU's GDPR, Brazil has enacted the General Data Protection Law (LGPD). This law is very similar in terms with the GDPR and has the same objectives, and in fact this is the first law of its kind in Brazil. This was enacted in the year 2020. In New Zealand an existing privacy bill was replaced by a newer one in 2020 to meet the standards set by the GDPR.

Other well-known legislations with respect to data privacy include the Digital Charter Implementation Act, 2022, known as Bill C-27, was introduced by the Canadian federal government, Singapore's Personal Data Protection Act (PDPA) which came into force in 2014, new Federal Act on Data Protection (nFADP) passed in 2020 and more. These laws are in sync with the 5 principles of data protection and that's why they along with the GDPR are highlighted in every issue with respect to data privacy. In India, the Information Technology Act, 2000, lays down the rules and regulations with respect to data protection. On August 24, 2017, a constitutional bench of 9 judges in the supreme court of India, in *Justice K.S.Puttaswamy (Retd.) v. Union of India*, upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution. This led to the formulation of a comprehensive Personal Data Protection Bill 2019. However, it was withdrawn in August 2022 considering a long list of recommendations for changes tabled by a Joint Parliamentary Committee that provided its report in December 2021. Later the Electronics and Information Technology decided to replace this bill with the Digital Personal Data Protection Bill, 2022. This was done as per the recommendations of the changes of the joint parliamentary committee.

Why data trading violates consumer rights?

Consumer rights include

- **Right to Safety**; The consumer has all rights to ensure that the product meets safety standards for his own well being
- **Right to Choose**; He has the right to choose from a variety of options available in the market and the producer has no say here.
- **Right to be informed**; The consumer has the authority to demand all information about the product he is purchasing.
- **Right to Consumer Education**; The consumer must be aware of his rights, so that ignorance doesn't get him exploited in the market.
- **Right to be heard**; The consumer can ensure that his grievances are heard to the public through various available means.
- **Right to seek compensation**; The consumer can seek redressal against exploitation, by approaching courts and various forums.

Data trading by corporations, especially by tech companies, seems to ignore a lot of consumer rights. Especially when their personal information is leaked out or traded without their consent. The consumer is being denied his right to be informed about what happens to his data, especially when he avails the services of companies that operate social media. The consumer can demand that his data be secured. Companies while trading in user data violate a lot of not just consumer rights but business ethics as well. In 2019 Facebook decided not to notify 530 million users about their data being breached.

This goes against the very right of the consumer to be informed about the product or the actions of the service provider. Facebook then publicly stated that they had no plans to notify users about data breaches. Facebook had to pay compensation of \$5 billion (about \$15 per person in the US) to the US Federal trade commission for violating an agreement to protect user privacy a week before the data breach issue erupted. Facebook is said to have a history of violating consumer rights to pursue vested interests.

Infact in the Edward Snowden case, this was highlighted by Edward himself. He warned that companies like Facebook worked with the National Security Agency (NSA) to create surveillance state. All data breaches in one way link to the user being spied upon, either by the corporation, or at the request of government agencies itself. Each action like these seems to fuel consumerism rather than free and fair competition. Many corporations believe that monopolies and consumer rights cannot coexist, hence they resort to such practices. Sometimes data trading can be classified under the umbrella of unfair trade practice, not only is the consumer deprived of his choice, but data trading gives an undue advantage to the producer. This is like a person or a group of people forcing their choices on the other rather than the concept of free market being played out here. As we saw in the case of TikTok, the company sold more than 89 million user data behind closed doors to various groups. All these groups are known to have indulged in shady transactions. So the consumer must be aware of his rights to assert his authority over the producer.

How can a consumer be responsible?

There's a saying that rights and responsibilities go hand in hand. A consumer must be responsible for being assured of his rights and as to how he can exercise the rights to ensure fair trade practices are carried out. But in certain cases, the consumer himself is to be blamed, as he himself opened the doors of his privacy to the company. A survey of 10000 users by McKinsey and company concluded that consumers felt comfortable with sharing their data with respect to a few business houses, especially those related to healthcare, although no business reached the 50% mark. This is an indicator that despite knowing the consequences many consumers are often ignorant about the threats they face. Ignorance can be detrimental, and history has proven that time and again. Another research concluded that only 1% of users read the terms and conditions of whatever they're accepting online, which ends up opening the curtains to data traders. Rights are powerful when they're exercised by those who are responsible. Along with consumer rights, comes consumer responsibilities as well, which include

- **Responsibility to be aware**; The consumer must be aware of whatever he consumes and must gain significant knowledge about the product or the service he avails.
- **Responsibility to think independently**; The consumer must have the ability to think and be clear about his wants and interests, how to safeguard them.
- **Responsibility to speak out**; The consumer must know how to put out his grievances to the correct authorities and get them to act.
- **Responsibility to complain**; It's the responsibility of the consumer to approach the right redressal forums and stake claims in a fair way.
- **Responsibility to be an Ethical Consumer**; They should be fair and not engage themselves with any deceptive practice.

The consumer must play his part to ensure that tech companies stay within their limits, and they must make sure that their rights are known to them and they are sure of how to stake their claims to seek the right compensation. A consumer who is ignorant of his own rights is one among those who ignores the terms and conditions of tech companies while signing in. The question of privacy is at the hands of the users themselves.

Why do companies get away with violations?

Companies which indulge in illicit data trade often don't face the wrath of the law. For example, a US\$5 billion fine is on air for Facebook, for its role in the Cambridge Analytica incident, and related practices of sharing user data with third parties. The exposure of this event has forced Facebook to take measures to improve its privacy controls and be forthcoming with users. Here Facebook was apprehended for massive privacy violations of users but was let off just with a fine and many weren't properly held accountable for their actions. This happens due to vague legislation that deals with data trading. Tech giants are multiple steps ahead of regulators and can exploit any grey areas in legislation they can find. When it comes to user data it's very difficult to point out what the actual crime is here and who is to be held liable. Even medium sized tech companies and e-commerce giants are known to have indulged in data trading behind closed doors. Regulators say that it's almost impossible to predict whether data will be misused by the tech company or not. This is why regulating everything has become difficult these days for authorities.

Consequences of illicit data trading

There're a lot of consequences of illicit data trading, as we have seen in the case of how data was weaponized by Facebook during the Arab spring of 2011 where personal data of users was used to fuel antigovernment protests in many countries by external actors. On an individual scale it is proven that invasion of privacy. Privacy as a concept is said to be more than just hiding things. It's a refuge of an individual from society's eye and is a part of his freedom. Privacy is also a space for self-monitoring and individual, and tech companies seem to target these. In the Cambridge Analytica issue, the concept of individual choice was being challenged here and the user was being displayed political advertisements with which he never ever had any personal connection and was vulnerable to external influences. This was done in the 2016 Presidential elections in the US to bring the outcome in the companies favor. Here the very concept of people's choice in a democracy was under threat here. In short data trading ends the very concept of individual privacy and choice. So, netizens must be aware about their activities online and must avoid sharing their personal data or opening their devices of social media accounts to suspicious individuals. Data trading from a consumer perspective is against the rights as the consumer is not being informed of the actions of the producer and by looking at the case of Cambridge Analytica, we can conclude that data trading behind closed curtains can be detrimental to ordinary citizens in general.

Conclusion

Data is being traded to influence one's personal choices which may include altering his preferences and choices. The producer wants to grab the attention of the consumer at any cost, and for that he must fuel consumerism through any means. For big corporations, pushing consumerism means pushing for establishing a monopoly over a particular thing and destroying competition in all ways possible. Social media companies work with other corporations and in most cases they're more than willing to sell user data to push more consumerism among people in general. Consumerism beyond a certain point destroys the interdependence that a society has and in the modern era, creates decarcerated consumers rather than sane individuals. So, the user must be aware of the rights and responsibilities so that he doesn't become vulnerable to exploitation.