

5 CMET (2018) 102

Data Localisation and Enforcement of the Right to Privacy

by

—Vishal Rakhecha and Chittkrishna Thakkar*

INTRODUCTION

Data has become an indispensable component of the internet and therefore, the economy. Some of the largest companies in the world have built business empires around the collection and processing of data. This massive pool of data collected by these companies allows them to invade the private lives of an individual, and in more cases than not, without the individual's consent. These companies have been able to escape from the consequences of these intrusions because of a principle that lies at the very foundation of the internet- self-regulation.

The internet began as an effort to move away from centralized structures which had started to control individual lives more and more frequently; Bitcoin is the most recent and marked example of this pursuit.¹ This move towards a decentralized system was premised on the idea of having equal bargaining power between all the parties in it, in the sense that every single user and service provider will perform their function in a manner which serves the needs of the entire community; any attempt to illicitly benefit off another member would result in penalties or reprimands imposed by the community on the user or service provider in question. This principle of self-regulation which for long has been the stated goal of the Internet has failed and has led to increased corporate control over individuals' lives.

The complete lack of regulation coupled with the wanton collection of data has created a massive power imbalance.² Companies have gained knowledge about almost every aspect of an individual's life³ and the lack of viable alternative service providers forces consumers to stay with one service provider.⁴ It is at this stage that State intervention becomes necessary to prevent the breach of the rights



Page: 103

of its citizens. This intervention must be backed by a law which clearly demarcates the scope or jurisdiction within which it would apply. The jurisdiction should be fixed in a manner which ensures that the law is not only certain but also allows for a practical enforcement mechanism. This paper is an attempt to provide such a mechanism.

In the first section, this paper provides a justification for the constitutional need for the State to intervene. The next section deals with the inadequacy of extraterritorial application of laws to address the issue. The third section sets the context for the benefits of data localisation as a way forward. The fourth section presents the arguments against data localisation and explains why these concerns are misplaced. The last section concludes the paper by construing that data localisation will facilitate the protection of right to privacy.

CONSTITUTIONAL NEED FOR DATA PROTECTION

The constitutional scheme of rights is designed to protect and enhance individual liberty as an end in itself, and to promote the values which enhance societal equality and cohesion. The threat to these rights comes from multiple companies which manipulate individuals' behaviour for the best interest of such companies. The

companies are able to achieve this because of lack of regulations on their information collection. This section will, by using the example of Facebook, demonstrate one of the several ways in which such violations occur and how these violations have had devastating effects not just for the individuals concerned but also on values which are central to the idea of democracy.

The number of Indians using Facebook has recently surpassed 240 million, making it the country with highest number of Facebook users. Around 19% of the country's population is estimated to use Facebook.⁵ The social media giant collects a large amount of personal data from its users, ranging from general basic information about the user to his/her specific tastes and preferences. It amasses such data by keeping track of the users' online activity, *inter alia* the advertisements clicked on, the pages liked and the location of the user.⁶ The tracking is not only limited to the user's activity on Facebook but also extends to every website one visits while logged into Facebook.⁷ Even when a user is



logged out, Facebook knows what she is browsing because it is alerted every time a user loads a page with the option of a 'like/share on Facebook' button or when an advertisement is sourced from its Atlas network. It is estimated that Facebook uses 98 different data points to target ads to its users.⁸

By collecting such personal information Facebook intrudes on the fundamental right to privacy of all Indian citizens who are on Facebook, that is, approximately 241 million Indian citizens. An argument against this is the non-applicability of Fundamental Rights against private entities and that the users have consented to give this data. These remain grey areas which need to be considered here. Even though Fundamental rights are not directly enforceable against private entities, they could have indirect horizontal application when the government is under a constitutional duty to protect the citizens from certain actions by private individuals.⁹ There is no specific answer as to which fundamental right imposes this duty, but the Courts have primarily imposed such a duty in situations engaging with cases under Article 21, right to life.¹⁰

The Delhi High Court in *Uphaar Cinema* held that due to Article 21 there is an affirmative duty on the State to protect individual lives which obliges it to effectively regulate private property owners.¹¹ The case of *Vishaka v. State of Rajasthan*¹² can also be understood as an extension of the constitutional duty as envisaged under *Uphaar case*. Here the court directed the State to protect the citizens from sexual harassment regardless of the employer. Hence, in order to fulfil its constitutional obligation, the state is necessitated to enact a law against sexual harassment. Considering that the right to privacy was held to be a fundamental right under Article 21, unanimously by nine judges¹³, it would be fair to say that it also, like the above-mentioned cases under Article 21, imposes a constitutional duty on the State to protect the citizens' rights from being violated. This duty and the need to regulate private entities are hinted at by judges in the privacy judgment. The plurality judgment by four judges mentioned how in the age of information, dangers to privacy can also originate from non-state actors. In a separate but concurring judgment, Justice Sanjay Kishan Kaul clearly recognizes this obligation by stating that "*The right to privacy is claimed qua the State and non-State actors. Recognition and enforcement of claims qua non-state actors may require legislative intervention by the State.*"¹⁴



Now that the enforceability of right to privacy against private entities is established, it needs to be examined whether the collection of data by various companies leads to violation of privacy as per the standard set by the Supreme Court. The privacy judgment identifies three aspects as the core of the concept of privacy; the body, personal information, and decisional autonomy.¹⁵ Data collection by companies has an adverse effect on second aspect of informational privacy. In relation to that, the plurality judgment held that, informational control allows an individual to use privacy to retain control over his/her personal information. Among all judges there is a consensus with regards to the fact that informed consent is central to informational self-determination.¹⁶ This means that information can only be obtained from an individual after telling him/her exactly how it is going to be used and any use except that, would violate her right. Justice Kaul very clearly brings this out by mentioning, *"...the State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed."*¹⁷

To understand the nature and extent of this consent, it is important to consider the decision of *Canara Bank case* which, as per the operative order in the Privacy case, lays down the correct position of law. In this case three judges of the Supreme Court held that privacy deals with *'persons and not places'*, any documents of the customer with the Bank, must continue to *'remain confidential vis-à-vis the person'*, even if they are not at the customer's house and are voluntarily sent to a Bank.¹⁸ A joint reading of this would give the following preposition *"consent is not a one-time waiver of your right to control your personal information, but must extend to each and every distinct and specific use of that information, even after you have consented to the State collecting it from you."*¹⁹ When media giants like Facebook, Uber, Amazon, etc. collect data, this standard is not met at all. Majority of the users do not know how much information is collected, or how it is used so even if one says that there is *'consent'* one surely cannot say that the consent is *'informed consent'*.

The data collected provides an overarching image of an individual showing her entire profile: age, education level, location, relationship status, job, what she owns, political views and so on.²⁰ While such data points are normally



used for advertising, their usage is not limited to it. It also extends to the pages it recommends, the kind of news articles one sees and, also the kind of posts/comments/likes of friend of a user views in the newsfeed.²¹ The main objective of the media giant is to maximize the time a user spends on its website in order to gain higher revenues from advertising. To achieve this Facebook uses the data to ensure that users view posts about things they care about the most and posts they are most likely to engage with. Due to the extent of knowledge Facebook has about the users, it has developed the capacity to influence what users buy, how they feel and how they vote.²² Take for instance Brexit referendum, where, as per political strategist Gerry Gunster, Facebook was the game changer to persuade people to vote for Brexit.²³

Allowing Facebook to infringe on the privacy and to collect and use the data of users as per its whims and fancies also leads to violation of the Right to Freedom of Speech

& Expression.²⁴ This is because an important aspect of Free Speech & Expression is the fairness doctrine as per which, viewpoints are to be placed before the readers to enable them to draw proper conclusions,²⁵ while on Facebook, whatever one expresses reaches audiences selectively based on what they are likely to engage with. Of course, private parties are not compelled to publish/share everyone's view and have a substantial freedom in terms of the content that should be published for example, newspapers. But this is different because here the posts are selectively shown only to a group of people which is possible only due to the collection of sensitive personal data. Interestingly, 62% users are unaware that such a filtering exists and believe that at some or the other time of the day they would definitely see their friends' story.²⁶ Of the various theories justifying free speech such as instrumental theories (marketplace of ideas, speech promoting democracy, speech promoting truth and watchdog theory) and non-instrumental theory which values speech in itself as development of individual autonomy, the Supreme Court has primarily relied on instrumental relation between free speech and promoting and securing democracy.²⁷ Free speech not only promotes democracy but as per the Supreme Court, it is "*the very foundation of democratic way of life.*"²⁸ Hence, a violation of free speech would also mean a threat to democracy.



The extent to which the right to privacy is critical for the protection of democracy cannot be overemphasised. To achieve this, the State has to enact laws to regulate data management practices of entities. The Srikrishna Committee has been given the unenviable task of formulating the rules for data protection in India. The committee has to frame a scheme to mitigate the harms caused due to indiscriminate collection of data. It will have to, for example, set limits on the amount of information an entity has to collect from its users or at the very least provide the method through which the data has to be collected. It may also have to fix the extent to which even that collected data can be used/processed. The committee will also have to create a redressal method through which an aggrieved individual can enforce his/her rights.

The redressal method and the enforceability of these rules and regulations are going to be dependent on how the jurisdiction of the law is determined. The approach through which the jurisdiction is defined by the law becomes the primary factor in determining the viability of the avenues created to access justice. Any law formulated to develop such a method has to be certain in its scope so as to be able to inform entities whether it applies to them or not.²⁹ Additionally, a law would be futile if there is no method to enforce the rules and regulations. The next two sections will deal with the two varying methods of determining jurisdiction

EXTRA-TERRITORIALITY

A majority of the companies which operate in India are foreign companies, with servers outside India.³⁰ These companies do not always have offices in India. Even when they do, the Indian offices do not have control over the processing of the data. Any data protection law has to necessarily strive to include these companies within the scope of its jurisdiction. This is because these companies can have tangible effects on the online behaviour of individuals. Extraterritorial laws are one way to include these companies in its scope. Traditionally, the jurisdiction of a law extends to only the sovereign territory of the law-making authority, but if factors outside its territorial limits have a tangible effect on the well-being of the country, the need to regulate

these may arise.³¹ An extraterritorial law will have to fix the scope of or define the actors which will be regulated by it. Then, it must lay down the procedure by which it aims to enforce these laws.



Page: 108

Fixing the Scope of Extraterritorial Laws

The definition the law lays down to fix the extraterritorial scope of the law must set a standard for the kind of actions that makes an actor accountable to Indian regulations. Courts in various countries have developed several tests to determine their jurisdiction in relation to extraterritorial actors³²; this section will present the most commonly used metric, the *effects test*.

The first approach is the *Effects Test* or the *Intentional Targeting* approach. This test was developed in *Calder v. Jones*³³. Under the *Effects Test* what needs to be established is whether the act performed by the entity had an effect in the jurisdiction of the court and whether there was intention backing such an act. In addition to this, foreseeability is also a necessary condition.³⁴ An entity providing a service has to have foreseen that their action can have an effect in that particular jurisdiction; if there exists no foreseeability, then it creates an illegitimate expectation on the party to monitor each and every activity on its facility and user availing its service.

The Justice Srikrishna Committee in its White Paper has also suggested a few ways in which jurisdiction can be ascertained.³⁵ Of the three alternatives suggested, the first one refers to data stored on servers located within the territorial limits of India-which has been dealt with later on in the paper.³⁶ Under the second method, the scope of extraterritorial laws is decided on the basis of an enquiry of the entity carrying out a business in India in a consistent manner with the aim of profit. In the third method, the conduct of the service provider in offer is used as the determinative factor. Both the classifications are based on determining the intention of the parties involved.

There are several issues with the way these tests of effect and intention are to be used, either in isolation or together. A website can have an effect in a jurisdiction even when there is no intention involved; for example, in the case of Yahoo!, where the US website displayed anti-Semitic objects and French citizens could access it.³⁷ The French court held Yahoo! liable as it did not take steps to prevent people in France from accessing it.

The test to prove intention is based on identifying the steps taken to enter or avoid a particular jurisdiction.³⁸ The manner in which the internet



Page: 109

has grown makes it extremely difficult to demarcate the level of involvement required for a website to actually cater to a particular market.³⁹ There have been situations where a service was used in India without the entity ever intending for it to be used here; 'Reddit' for example was being used widely in India and only recently were features added to appeal to its Indian users. This ambiguity makes it difficult to frame a law which balances the interests of both, the service providers and the users.

Enforceability

Even after the determination of the scope of the law is made in a way that it is

broad enough to cover those entities which collect information about Indians, while still allowing it to be narrow enough to maintain a reasonable degree of foreseeability, there are issues with regards to how the law will be enforceable. The theoretical force of a law is not enough for it to be followed, there needs to be a strong mechanism to sanction those actions which are not in compliance with rules and regulations.⁴⁰ When it comes to companies which have a physical base in India or engage in trade in India, there exists a strong incentive to follow the laws here as their goods can be attached or the sale of their goods can be barred.⁴¹ Entities which are accessible through the internet do not always have physical offices in all locations where their service is provided. Even when they do, the branches do not have any actual powers in the use and processing of the data.⁴² The power is vested in the hands of the head office.

Law enforcement authorities could request data directly from the companies and there are countries which provide for laws to regulate this; for instance, the Electronic Communications Protection Act, which provides for the procedure for disclosure of information to a government service.⁴³ Under this Act, a foreign government official must first obtain the warrant of an American judge before they allow the entity to comply with such a request. Even in those circumstances, the entity can only transfer metadata related to the transaction and not the contents.

Sanctions can be imposed by entering binding bilateral or multilateral Mutual Legal Assistance Treaties (MLAT) with the countries hosting such data. These are entered into in order to collect and exchange information to



enforce laws.⁴⁴ The issue with MLATs is that it becomes tougher for a developing country like India to negotiate or enforce it with countries like China or USA, which have the majority of data regarding Indians. The treaties also have a certain degree of uncertainty attached to them, as the actual functioning of the treaty depends on the delicate political ties countries have.


Yet even in the best of political conditions, a long bureaucratic process is involved which further complicates the issue.⁴⁵ To provide an illustration on how this works out, take for instance a piece of information which is required from Amazon. The law enforcement body/police from India sends a request through a diplomat, authorised to do so, who communicates it to the United States' authority the Department of Justice's Office of International Affairs (OIA). This request then is taken to the US attorney's office who then passes it on to the judge under 28 U.S.C. § 1783. The judge then reviews the submission to check whether it meets the Fourth Amendment standard. It is then passed on to the FBI who forwards it to the data controller, in this case Amazon. If Amazon deems the warrant to be sufficient, it then passes the information back through the same chain. This entire process takes up to an average of ten months, sometimes more.

Such a framework is insufficient if not entirely futile when the requirement of a data regulator is to prescribe and work with the data controller to comply with the law. The vague and ambiguous tests, as referred to earlier to fix jurisdiction make it difficult to fix jurisdiction and determine who needs to work and ensure observance of the rules and regulations set by the regulator. The mere extension of jurisdiction to entities outside of the territorial borders do not meet the required standard of quick and efficient enforcement.

DATA LOCALISATION

The access to data stored on a cloud in a foreign country is restricted, as has been

demonstrated above by problems like competing claims of jurisdiction and other associated problems with extraterritoriality. Hence, a strong case can be made for data localization which refers to the storage and processing of data in the country where the data originates, while preventing the same to cross borders. There is a multitude of ways through which this can be done - it can be enforced by preventing information from crossing the national borders of a country,⁴⁶ by making the data subject's explicit consent to transfer


 Page: 111

data,⁴⁷ by imposing a tax on export of data,⁴⁸ by requiring the companies to save a local copy of the data being exported,⁴⁹ or by only allowing exports of data to countries with whom there is a prior agreement or who have comparable data protection laws.⁵⁰ For the purpose of this paper, 'data localisation' would refer to the mandatory storage and processing of personal data in the home country. Any other data can be exported only after explicit consent of the data subject is taken.

There are two assumptions precursory to any claim regarding data localisation. *Firstly*, that there exists a legal framework which regulates the kind of information that a company can collect from the subject. *Secondly*, that there exists a data authority which has power to penalise and impose sanctions in case of a breach.

The argument for data localisation is rooted in the need to safeguard the rights of data subjects as it allows for access to the data when there is a legitimate interest involved. The presence of data servers within the territory of India, means that they are within the territorial jurisdiction of the Indian state. Any such entity would then have to follow the laws of India. The physical presence of the data gives the Government the ability to subject the entities to the rules and regulations here. This reduces the problem around conflicting jurisdictional claims and eases regulatory compliance. For example, when data is stored in India the private entity will have to comply with India's Privacy laws. It also helps ensure efficacious legal remedy as data would be within the control of the defendant company (as it is not on foreign servers) and thus it is possible to get access to data as and when legally required.

Take for instance the present petition pending in the Apex court where the Petitioner Pallav Mongia has demanded for data localisation laws. The key claim of the petitioner is that despite huge amount of Indian internet traffic flowing through internet giants like Google and Facebook among others, all data is stored by them outside India. He argues that the local branches of these companies do not have control over the data and that this is evident from their affidavits in response to the requests for access to it. This acts as a huge impediment to efficacious legal remedy.⁵¹ This is also evident in *Microsoft Corp v. United States*⁵², in which a magistrate judge issued a search warrant

 Page: 112

*to Microsoft to produce certain data, but the company only partially complied with it by producing the data stored in US servers. The company refused to part with the data stored in Ireland, claiming it to be beyond the jurisdiction of the court.*⁵³

Another argument for data localisation is that it reduces the possibility of a country's citizens being subject to surveillance by foreign governments, because data within one's territory is easier to access. When foreign governments can easily access

sensitive data of another state's citizens, it also becomes a national security threat for that state and this threat can be avoided through data localisation. Of course, based on this reasoning an intuitive problem is that data localisation provides to give the government increased control over its residents' online activities, which raises the risk of infringement of citizens' right to privacy and freedom of expression and leads to curbing of dissent based on the personal data available to the state.⁵⁴ However, this assertion does not hold water, at least in India. Privacy is now a fundamental right due to which the State is under an obligation to not violate its citizen's privacy. Hence, any such violation would surely be prevented by the data protection law currently being drafted by a committee headed by Justice Srikrishna.⁵⁵ At the same time, any violation by foreign governments cannot be prevented and citizens would have no remedy in case foreign governments breach their privacy, which is not true in case of a violation by the Indian State. Data localisation could also have some economic benefits, it would lead to better infrastructure due to the investment necessary to store data in India.⁵⁶

OBJECTIONS TO DATA LOCALISATION

The following are the primary objections to data localisation. The greatest fallout of the Snowden revelations was the increased awareness among the people that their information is not safe with American corporations as the government there has ready access to it. In response to this, countries across the world proposed 'data localisation' as a way to prevent surveillance by foreign governments. Scholars have argued that this knee-jerk response will do more damage than good to the privacy and security of the users,⁵⁷ that it



would lead to the *Balkanisation* of the internet, creating multiple internets hindering growth and innovation.⁵⁸

One of the foremost objections to data localisation is that the mandate for data localisation can enable the suppression of dissent; forcing information out of a local server is easier than from a server placed outside the country. Data localisation, even in its most basic form envisages the storage of at least personal information. Depending on the broadness of the definition, a government can force all companies providing any service to store the record of the entirety of a citizen's online activity in its own territory. This would immediately translate to control over its citizens' digital activities, putting critical information in the hands of the government. This can make it difficult for citizens to freely conduct their actions on the internet or express their views.⁵⁹ Scholars have cited the cases of repressive governments like Russia, China, Vietnam, among others, to show how these governments have used these laws to crackdown on dissidents.⁶⁰

The rapid transfer of data and the free-flow of information is at the core of the internet-based services. This has facilitated the creation of services like the Internet of Things (IoT) and Cloud Computing.⁶¹ All these come to be threatened due to the introduction of data localisation as it prevents such quick transfers of data. The internet was envisaged and created with the intention of having a borderless and territory less existence.⁶² As a result of this original conception, the design and architecture of the internet will have to be changed to adhere to the function in a world where data of a certain kind is store in a specific place. Most importantly, the associated costs with redesigning this entire system are massive.

The growth of the Internet to a large extent has been due to low costs of entry and

exit. This has allowed companies to disrupt the market with innovative ideas, and its borderless nature has made it easier to expand to newer markets. If data localisation laws are made mandatory, entering those countries becomes expensive; one would have to set up their server farms or rent space from a cloud-provider.⁶³ Consequently, this increased cost can possibly

 Page: 114


hinder the entry of newer firms in a country thereby reducing competition.⁶⁴ Companies may avoid India altogether as the costs of setting up and providing services would be huge thus decreasing foreign investment. Additionally, this would create an adverse effect on the competition and thereby the quality in the cloud-service industry. The local cloud providers will not have any global competitors, this lack of competition provides little incentive for the cloud-service providers to develop state-of-art security measures.⁶⁵

In terms of security, data localisation can change little. The Snowden revelations while providing an insight into how the NSA was able to access data in the USA also showed their ability to attack and retrieve data in foreign servers. In fact, there is a probability that the storage of data in one place can make it an easier target for attackers and foreign governments.⁶⁶

ANALYSING THE VIABILITY OF DATA LOCALISATION

The various objections against data localisation are either entirely misplaced or have exaggerated the possible harms. These arguments in most cases are divorced from reality, suggesting methods which have bureaucratic baggage attached to it. The benefits of data localisation outweigh the harms that may come from it.

An oft-repeated argument is that data localisation enables governments to suppress dissent and this leads to abuse of political rights of citizens. There are two layers to this argument, *firstly*, that having control over the data immediately translates to government monitoring of individuals' online activities. *Secondly*, that prevention of data transfers out of a territory are undertaken only by countries which have a poor human rights record. An assumption implicit in the first layer is that only western countries, which presently have data stored in their territories, are placed in a position to protect the rights of their citizens and those of the citizens of the world. This is a fundamentally flawed argument. Countries outside of the West can and have developed data protection laws.⁶⁷ As has been discussed above, the Indian Supreme Court has recognised the citizens' fundamental right to privacy, providing them with recourse for situations wherein their data might be used by the state resulting in violation of this right. This form of accountability can never be imposed on a foreign government and this critical factor is discounted by most analysts.⁶⁸ The second layer of the argument is that only repressive governments have

 Page: 115

laws relating to prevention of data transfers. This assertion falls flat when we look at how the European Union has dealt with this; it not only has a stellar human rights record, but also some of the most progressive data protection rules in the world. They have even formulated rules which create difficulties in transferring data outside of the Union.⁶⁹

Another argument forwarded is concerning associated costs to change the architecture of internet and that this disruption can prove to be extremely detrimental to the development of the internet as it exists.⁷⁰ This argument is unpersuasive for two reasons; *firstly*, the internet is not inherently unterritorial. Any assertion of such kind is utopian, as the internet is not borderless or beyond the conventional ideas of territorial jurisdiction.⁷¹ The internet is experienced by people differently depending on where they are located.⁷² The government has a massive influence over the way the internet functions because of the nature of regulations over the functioning of the infrastructure using which it operates. This control begins with what kind of devices are allowed into a country, broadband and internet policies of a country, censorship laws and privacy laws among others. Similarly, data stored on the cloud is also stored in physical servers, where some countries have greater access to the information as it is placed within their territorial limits and therefore are able to regulate it with ease.

Secondly, the internet as it exists has not been able to prevent harm to the privacy of the individual and the costs to the society because of this are considerably larger than any economic costs that will be incurred to remedy it. An internet with data protection and privacy ingrained in its design is far more beneficial to development. This measure is more likely to instill privacy by design. The associated costs that can arise are a fair trade-off to ensure that individuals' liberties are protected.

The argument that innovation is likely to suffer as data localisation measures are likely to prevent foreign entities from entering these markets due to the high cost of entry,⁷³ is not entirely applicable in the Indian context and its detrimental effects can be mitigated in the ways suggested below. A service provider, looking to expand his services will first look at the costs of venturing into newer markets and gains likely to be made by entering them. If the costs of setting up servers, for example, are not commensurate to the revenues that are to be gained from the market, they will not enter it. India is a massive market and any service provider with the intention to expand will look towards it as a possible market. This unique position which India enjoys gives it the privilege to enact laws like data localisation while still attracting foreign



investment. This is because it is financially viable for the service providers as they gain access to such a massive unsaturated market for either setting up their servers here or renting them from a local cloud-server provider.

These benefits may be limited to the larger players who have enough capital to setup or rent servers in India. The smaller entities will find it difficult to venture into India. To address this, the government can set a threshold where on basis of the number of users the data localisation will be enforced. If an entity has users below the particular threshold they would not have to store the data here. But a disclaimer would be shown to anyone accessing the service that the information is not being stored in India must be given and an option has to be provided, only after the explicit consent of the users is taken can the information be collected by the service provider. Such a mechanism has multiple benefits; it allows the market dynamics to play out at the lower levels while also ensuring that the services which the consumers favour are granted the space to operate. When and if these services do reach the required threshold, they will have to start storing the data in India. The primary reason why such a move is still likely to be beneficial to data rights is because consumers do not have a bargaining power with larger firms. They may probably be the only players in the market offering those services, which is why government intervention becomes

necessary. But, when it comes to smaller service providers, the same power hierarchies do not operate as consumers have a greater bargaining power allowing them to negotiate better policies or to switch to more secure alternatives.

It has been argued that information is likely to be less safe in countries which have not had servers earlier and thereby lack the technology or expertise to handle the change.⁷⁴ The development of servers may be in its nascent stage in India, but there is no reason to believe that foreign companies which will set up their server farms will not follow their own best practices or use the state-of-art technology. For that matter even local cloud-service providers will be able to benefit from the wealth of research available on the subject. Additionally, cloud-server providers will have to adhere not only to a minimum set of standards, but also face stiff competition locally as the Indian market is large enough for more than one cloud-server company to develop more secure servers.

A consequence of data being stored outside the country is that it gives the entities the freedom to impose unfair contractual obligations on Indian users. For example, a company may impose mandatory arbitration clauses in its terms and conditions or force the user to accept the company's home country as the only place to resolve disputes.⁷⁵ This creates an unfair burden on the consumer and makes legal recourse tougher for them. When data is stored in



India, then the contract becomes a uniquely Indian contract. The Indian courts can now look into the inherent logic and equity being provided by the contract.

Post-Snowden measures to protect the people have been met with arguments that the NSA's capabilities are extensive enough to conduct surveillance even in servers located outside USA. Even if this is true, it is no reason to provide the data of Indian citizens on a platter to NSA by not providing adequate protection to the data of Indian citizens. Lastly, considering that the state has a constitutional obligation to protect the privacy of its citizens coupled with the inadequacy and inefficiency of extraterritorial laws to do the same, it makes a strong case for India to adopt data localisation.

CONCLUSION

Large technology companies have for long collected data as per their whims and fancies. This acts as a massive intrusion into the right to privacy of the individual. There is the need for a law to deal with. These rules can be formulated to limit the scope of the data collected by these companies. This becomes necessary in the context of the scale and intensity with which these companies collect personal information. The definitive limit on data has to be fixed on the basis of goal sought to be achieved and limiting collection of data for only those purposes, as it would reduce the likelihood of unwarranted collection of data.

A data law can also reduce the extent to which data can be processed and limit the time for which it can be saved. It is the processing of massive amounts of data that gives Google and Facebook the insights required to manipulate people into spending more time on their websites. When there are restrictions placed on the ability of websites to process and draw inferences from these large data sets, a natural outcome is a reduction in their intrusions into people's lives. The level of intrusion decreases because these companies develop patterns about a person, something that simple raw data would not have been able to provide. The websites achieve this by allowing the most polarising views to stay on top of the newsfeed or video suggestions or page suggestion, this increases the average time spent per user. The newsfeed is directed

by an algorithm which decides the nature of the content to be shown to the users, it can then be argued that the problem is actually rooted in the algorithms and it is the design of the algorithms that ends up favouring polarising content over others. This position would seem to suggest that polarised newsfeed is not the fault of data collection.

However, algorithms working on machine learning are designed in a flawed manner to begin with. It is the knowledge or information collected from the users and its subsequent processing that makes an algorithm that much more powerful and efficient in dividing people based on their tastes and preferences. That a certain kind of post is more likely to make a user stay online comes



Page: 118

from these powerful data processing algorithms. Thus, the fact that these end up being one-sided or polarising is a consequence of the data processing. A step in this direction would be to place restrictions on what can be collected, processed and the period for which it can be processed or used. There is a massive likelihood of websites showing less divisive content. Being able to achieve these goals would lead to the protection of the right to privacy and the allied right of freedom of speech and expression.

Data localisation is instrumental in achieving these objectives. Extraterritorial laws, as have been shown, are weak as binding legal instruments as they have uncertain applicability depending on the political conditions within the country where the data is placed. They also provide little remedy if the foreign governments start illegally intercepting data of Indian citizens. Due to their bureaucratic nature they are also slower in providing critical data and inefficient in restraining the collection of data. This makes it an ill-suited method to protect the data rights of individuals. Data localisation, despite its economic costs, is able to ensure that there is a swift execution of orders. The compliance of the rules and regulations can be tested with greater certainty. The localised storage of data also makes the redressal mechanisms more meaningful as they remove the uncertainty attached with jurisdiction while also significantly reducing the time in which enforcement can be achieved.

It is here that the interplay between the right to privacy and data localisation becomes clear. Just like every right has to be attached with some mechanism to remedy its infringement, every iteration of a right to lay down its substance has to be attached with an enforcement mechanism. If this enforcement mechanism falls short of fulfilling to achieve the stated goals of protecting the right, it is futile. The right to informational privacy as a right has to be concretised by defining the information that can be taken, used and shared. This right has to be given a method to ensure that it is capable of being effectively enforced and data localisation is able to achieve this in a satisfactory manner.

— — —

* Students, National Academy of Legal Studies and Research University of Law, Hyderabad.

¹ Satoshi Nakamoto, '*Bitcoin: A Peer-to-Peer Electronic Cash System*' (*Bitcoin*) <<https://bitcoin.org/bitcoin.pdf>> accessed 15 February 2018.

² Monroe Price and Stefaan Verhulst, '*The Concept of Self-Regulation and the Internet*' in J. Waltermann and M. Machill (eds), *Protecting Our Children on the Internet: Towards A New Culture of Responsibility* (Bertelsmann Foundation Publishers 2000) <https://repository.upenn.edu/asc_papers/142/> accessed 15 February 2018.

³ Shoshana Zuboff, '*Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*' (2015) *Journal of Information Technology* <<https://link.springer.com/journal/41265/30/1/page/1>> accessed 15 February

2018.

⁴ Justus Haucap and Ulrich Heimeshoff, 'Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?' (2014) 11(1-2) International Economics and Economic Policy <<https://link.springer.com/journal/10368/11/1/page/1>> accessed 15 February 2018.

⁵ PTI, 'India Now Has Highest Number of Facebook Users, Beats US: Report' (Livemint, 14 July 2017) <www.livemint.com/Consumer/CyEKdaltF64YycZsU72oEK/Indians-largest-audience-country-for-Facebook-Report.html?utm_source=scroll&utm_medium=referral&utm_campaign=scroll> accessed 5 February 2018.

⁶ Caitlin Dewey, '98 Personal Data Points that Facebook Uses to Target Ads to You' (The Washington Post, 19 August 2016) <www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?utm_term=.e815d57607c7> accessed 14 February 2018.

⁷ *Ibid.*

⁸ *Ibid.*

⁹ Stephen Gardbaum, 'Horizontal Effect' in Sujit Choudhry, Madhav Khosla, and Pratap Bhanu Mehta (eds), *The Oxford Handbook of Indian Constitution* (OUP 2016).

¹⁰ *Ibid.*

¹¹ *Assn of Victims of Uphaar Tragedy v. Union of India*, 2003 SCC OnLine Del 377 : 2003 ACC 114.

¹² (1997) 6 SCC 241 : AIR 1997 SC 3011.

¹³ *KS Puttaswamy v. Union of India*, (2017) 10 SCC 1.

¹⁴ *Ibid* [584] (Kaul J).

¹⁵ Gautam Bhatia, 'The Supreme Court's Right to Privacy Judgment -III: Privacy, Surveillance, and the Body' (*indconlawphil*, 29 August 2016) <<https://indconlawphil.wordpress.com/2017/08/29/the-supreme-courts-right-to-privacy-judgment-privacy-surveillance-and-the-body/>> accessed 15 February 2018.

¹⁶ Gautam Bhatia, 'The Supreme Court's Right to Privacy Judgment IV: Privacy, Informational Self-Determination, and the Idea of Consent' (*indconlawphil*, 30 August 2017) <<https://indconlawphil.wordpress.com/2017/08/30/the-supreme-courts-right-to-privacy-judgment-iv-privacy-informational-self-determination-and-the-idea-of-consent/>> accessed 15 February 2018.

¹⁷ *KS Puttaswamy* (n 13) [637] (Kaul J).

¹⁸ *District Registrar and Collector v. Canara Bank*, (2005) 1 SCC 496.

¹⁹ Gautam Bhatia, 'Privacy, Informational Self-Determination, and the Idea of Consent' (n 16).

²⁰ Victor Luckerson, 'Here's How Facebook's News Feed Actually Works' (*Time*, 9 July 2015) <<http://time.com/collection-post/3950525/facebook-news-feed-algorithm/>> accessed 15 February 2018.

²¹ *Ibid.*

²² *Ibid.*

²³ Darragh MacIntyre, 'Facebook - The Secret Election Weapon' (*BBC News*, 8 May 2017) <www.bbc.com/news/uk-39830727> accessed 15 February 2018.

²⁴ Constitution of India, art 19(1)(a).

²⁵ *LIC v. Manubhai D. Shah*, (1992) 3 SCC 637 : (1992) 3 SCR 595.

²⁶ Motahhare Eslami and others, 'I Always Assumed That I Wasn't Really That Close to [Her]': Reasoning About Invisible Algorithms in the News Feed' <www.personal.umich.edu/~csandvig/research/Eslami_Algorithms_CHI15.pdf> accessed 15 February 2018.

²⁷ Lawrence Liang, 'Free Speech and Expression' in Sujit Choudhry, Madhav Khosla, and Pratap Bhanu Mehta (eds), *The Oxford Handbook of Indian Constitution* (OUP 2016).

²⁸ *Supt, Central Prison v. Ram Manohar Lohia*, AIR 1960 SC 633.

²⁹ Edgar Bodenheimer, *Jurisprudence - The Philosophy and Method of the Law* (Sixth Indian Reprint, Universal Law Publishing 2009).

- ³⁰ '7 Out of the Top 10 Companies Operating in India are from Outside India' (Alexa) <www.alexa.com/topsites/countries/IN> accessed 15 February 2018.
- ³¹ Justice S. Muralidhar, 'Jurisdictional Issues in Cyberspace' (2010) 6 IJLT 1.
- ³² *Ibid.*
- ³³ 1984 SCC OnLine US SC 58 : 79 L Ed 2d 804 : 465 US 783 (1984).
- ³⁴ Michael A. Geist, 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction' (2001) 16 Berkeley Tech LJ 1345, 1356.
- ³⁵ White Paper of Committee of Experts on a Data Protection Framework for India, <<http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited>> accessed 15 February 2018.
- ³⁶ *Ibid.*
- ³⁷ *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F 3d 1199 (9th Cir 2006).
- ³⁸ Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 Europe J. Int'l L 779.
- ³⁹ *Zippo Mfg Co. v. Zippo Dot Com Inc.*, 952 F. Supp 1119 (WD Pa 1997).
- ⁴⁰ Arthur T von Mehren, 'Enforcing Judgments Abroad: Reflections on the Design of Recognition Conventions' (1998) 24 Brooklyn J Int'l L 17, 18.
- ⁴¹ Penal Code, 1860, s. 4.
- ⁴² Salman, 'Supreme Court Issues Notice to Facebook, Google, Twitter, on Data Localisation' (MediaNama, 7 September 2017) <www.medianama.com/2017/09/223-supreme-court-issues-notices-to-facebook-google-twitter/> accessed 15 February 2018.
- ⁴³ Electronic Communications Protection Act, 2014, s. 2703 (US).
- ⁴⁴ Andrew K. Woods, 'Data Beyond Borders: Mutual Legal Assistance in the Internet Age' (Global Network Initiative, January 2015) <<https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf>> accessed 15 February 2018.
- ⁴⁵ Andrew K. Woods, 'Against Data Exceptionalism' (2016) 68 Stan L Rev 729.
- ⁴⁶ Pingp, 'The Great Firewall of China' (Torfox, A. Stanford Project, 1 June 2011) <<https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html>> accessed 15 February 2018.
- ⁴⁷ Datuk Seri Dr. Rais Yatim, 'Protecting Your Personal Data' (The Star Online, 24 May 2013) <www.thestar.com.my/news/nation/2012/02/12/protecting-your-personal-data/> accessed 15 February 2018.
- ⁴⁸ Anupam Chander and Uyen P Lê, 'Data Nationalism' (2015) 64 Emory LJ 677 <http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf> accessed 15 February 2018.
- ⁴⁹ Anupam Chander and Uyen P Lê, 'Breaking the Web: Data Localisation v. The Global Internet' (2014) Emory L J <<https://ssrn.com/abstract=2407858>> accessed 15 February 2018.
- ⁵⁰ European Commission - Press Release (Europa.eu, 2 February 2016) <http://europa.eu/rapid/press-release_IP-16-216_en.htm> accessed 15 February 2018.
- ⁵¹ Salman, 'Supreme Court Issues Notice to Facebook, Google, Twitter, on Data Localisation' (n 42).
- ⁵² 829 F 3d 197 (2nd Cir 2016).
- ⁵³ AK Woods, 'Against Data Exceptionalism' (n 45).
- ⁵⁴ Alexander Plaum, 'The Impact of Forced Data Localisation on Fundamental Rights' (Access Now, 4 June 2014) <www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/> accessed 15 February 2018.
- ⁵⁵ Surabhi Agarwal, 'Justice BN Srikrishna to Head Committee for Data Protection Framework' (The Economic Times, 1 August 2017) <<https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-to-head-committee-for-data-protection-framework/articleshow/59866006.cms>> accessed 15 February 2018.

⁵⁶ Jyoti Panday, 'Rising Demands for Data Localisation a Response to Weak Data Protection Mechanisms' (Electronic Frontier Foundation, 14 August 2017) <www.eff.org/deeplinks/2017/08/rising-demands-data-localisation-response-weak-data-protection-mechanisms> accessed 15 February 2018.

⁵⁷ Reema Shah, 'Law Enforcement and Data Privacy: A Forward-Looking Approach' (2015) 125 Yale LJ 543.

⁵⁸ Erica Fraser, 'Data Localisation and the Balkanisation of the Internet' (2016) 13:3 SCRIPTed 359 <<https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/>> accessed 15 February 2018.

⁵⁹ Alexander Plaum, 'The Impact of Forced Data Localisation on Fundamental Rights' (Access Now, 4 June 2014) <www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/> accessed 15 February 2018.

⁶⁰ Chander and Uyên P Lê (n 48).

⁶¹ Cyber-Physical Systems <www.nist.gov/el/cyber-physical-systems> accessed 15 February 2018.

⁶² Perry (n 2).

⁶³ Matthias Bauer Hosuk Lee-Makiyama, Erik van der Marel, Bert Verschelde, 'Data Localisation in Russia: A Self-Imposed Sanction' (ECIPE Policy Brief 2015) <www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf> accessed 15 February 2018.

⁶⁴ ECIPE Project Group, 'The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce' (US Chamber of Commerce, March 2013) <www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_Ir.pdf> accessed 15 February 2018.

⁶⁵ Chander and Uyên P Lê (n 48).

⁶⁶ *Ibid.*

⁶⁷ Graham Greenleaf and Whon-il Park, 'Korea's New Act: Asia's Toughest Data Privacy Law' (2012) 117 Privacy Laws & Business International Report 1-6.

⁶⁸ Puttaswamy (n 13).

⁶⁹ Regulation of the European Parliament and of the Council, (eu) 2016/679, art 45.

⁷⁰ Chander and Uyên P Lê P (n 48).

⁷¹ AK Woods (n 45).

⁷² Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006).

⁷³ Chander and Uyên P (n 49).

⁷⁴ Chander and Uyên P Lê (n 48).

⁷⁵ 'Statement of Rights and Responsibilities' (Facebook, 30 Jan 2015) <www.facebook.com/legal/terms> accessed 15 February 2018.

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.