White Paper

Centre for The Digital Future

Impact of the PDP Bill on the Start-up ecosystem in India

BY

CENTRE FOR THE DIGITAL FUTURE

NOVEMBER, 2021

Protection of an individual's privacy is a sine qua non in every democratic society. In India, after the 2017 Puttuswamy judgment of the Supreme Court, it is a constitutional requirement as well. Every legislation, whether existing or proposed legislation that violates or has the potential to violate privacy must conform to the principles laid down by the SC, viz. legality, legitimate goal and proportionality. The PDP Bill, 2019, has been under consideration by the Joint Parliamentary Committee (JPC) for almost two years. There has been much debate about several clauses of the Bill.

Provisions relating to privacy protection obligations of private entities collecting personal data have enthused some rights activists and disappointed others who felt they did not go far enough. On the other hand, many entrepreneurs are dismayed by the restrictions and their impact on innovation. There are other concerns too including the Bill's exclusive focus on privacy in the context of private service providers while largely failing to address concerns regarding privacy vis-a-vis the Government.

While debates on these issues have consumed public attention, there are other critical consequences of the proposed legislation that have failed to attract as much attention as they warrant. India has declared aspirations to a trillion dollar digital economy. Obviously, this aspiration requires a thriving digital and data economy that attracts investments and entrepreneurs while additionally being conducive to the advent and advancement of new technologies.

Regulations aimed at protecting privacy and security are no doubt essential. Yet, while crafting them, it is vital that the implications for the data and digital economy are clearly understood and factored in. It can be nobody's argument that privacy and security should be sacrificed at the altar of economic growth, entrepreneurship, technology advancement, tax revenue optimization, and so on. Rather, the moot point is whether we are adopting the approach that best reconciles the somewhat contradictory objectives of pursuing economic opportunities on the one hand and protecting privacy and security on the other. In other words, is the balance right?

It is well-recognized that, just as in the physical space, there is nothing like perfect security or perfect privacy in the digital space. We leave our homes every day, knowing that there are risks. When we cross the road, when we drive a car or a two-wheeler, when we undergo a medical treatment, we do so fully aware of the risks involved and comforted by the fact that there are laws that limit (though

not eliminate) that risk and that any willful violators of such laws will be punished and to the extent possible, victims compensated. That is the social contract in force. Is our thinking regarding digital privacy similarly structured?

For a country at India's stage of development and with the kind of potential that we have in digital and emerging technologies, it is important to protect privacy and security with an equally keen eye on simultaneously maximizing or at least optimizing the economic gains waiting to be tapped. It is unwise to ignore or be unaware of the impact of the former on the latter. Every society – be it USA, UK, Europe, China, Japan, Australia or any other, is in the process of finding a balance that is consistent with their societal values and economic imperatives. India needs to do so too, not by emulating or merely tweaking models adopted by others but by finding, or if needed, developing the model that best fits our unique context, needs and aspirations. Else we may find ourselves in the position of the trainer who taught a flea how to jump on command.

After cutting off two legs, he commanded the flea to jump, and it did. He detached two more legs and gave the command again and still, the flea jumped. Finally, after cutting off the last two legs, he repeated the command. This time, the flea did not jump. He noted sadly, that when you cut off all the legs of a flea, it is unable to hear a command. Are we in danger of doing something like that to our fledgling digital and data economy?

The impact of the PDP Bill on the start up eco-system in the country is a highly pertinent example of the kind of trade offs involved. What is interesting is that it offers an opportunity to put in place requisite controls and yet afford enough leeway to pursue valuable economic opportunities. Consider one key principle underlying many of the protection measures envisaged namely, empowerment of the individual. This principle is sought to be applied to both protection of privacy (aka "informed consent") and ensuring a fair apportionment of economic gains (DEPA paper of NITI Aayog) between platforms and individuals whose personal data is being used to create and thereafter abstract value.

This is a touchingly romantic, but entirely futile idea. We live in a world where technology is evolving so rapidly that even experts have a hard time keeping track of developments. At the same time, the sophistication of malicious actors is growing apace. Even people familiar with the perils of cyberspace often fall victim to intrusions by attackers or the traps they lay. To expect a lay user to protect her data solely by powers that the law vests in her is wishful thinking. Who

wants to be confronted by additional lengthy digital consent forms every time you click on a button to avail of a desired service? These agreements are drawn up by 1000$ an hour lawyers for companies whose valuations often exceed a trillion dollars. You are given a couple of minutes in your moment of need to make up your mind on whether you agree to the conditions or not. A more unequal and meaningless negotiation is hard to conjure up. This should convince anyone that such consents are utterly meaningless both when sought and when given. Would one feel more secure when the company gives me this option? Not really!

So, what is the solution then, one may ask. One possible approach is for service providers to be required to declare and publish their policy on privacy protection (most already do so), which can exceed, but not fall short of what is laid down by the law. The law itself should lay down and enforce a certain minimum level of protection for Personally Identifiable Information (PII), which all data fiduciaries whether a company or a government agency must comply with, and the state and its machinery enforce. After all, they are far better equipped to do so. Individuals can complain and seek remedies stipulated by the law if they believe their legal rights have been violated. Service providers should be restrained from seeking any general consent from users regarding use of their data.

Incidentally, such practices have been in the vogue. For example, in 1999 TRAI began tariff rationalization exercise with introducing the concept of 'standard tariff package' that was mandated to be offered for specific services like mobile and fixed line by every operator. Of course, customers had the option of choosing a different one if they so desired. Likewise, when private insurers were introduced, standard form contracts were devised. The insurance regulator also issued 'Guidelines on Standardization in Health Insurance'[1] while also allowing companies to offer other policies as well.

On one hand, such regulatory measures help in empowering individuals effectively by negotiating on their collective behalf a balanced contract with the service providers. This allows a lay user to choose either such a 'standard' choice while also being able to avail other options instead. On the other they also

---

1 https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/Guidelines%20on%20Standardization%20in%20Health%20Insurance%202016.pdf

encourage service providers to compete with prospects of innovation and qualitative differentiation.

As an instance of possible overkill in the PDP Bill, consider the provisions connected with the process of data collection related to consent and purpose limitation. Requiring providers to seek user consent for each instance of usage not explicitly sought by the user makes the entire chain of value creation and abstraction so cumbersome as to reduce the utility of the data to a small fraction of its intrinsic value. The convoluted process of consent envisaged in the Bill includes replaying the collected data to the data principal to check for its fidelity instead of a click wrap consent that is globally prevalent including in GDPR. This would seriously hamper data collection. Purpose limitation will also limit scope of innovation in services and scope of scaling up, even if as a case of unintended consequence.

It is also pertinent to note that to begin with, most start-ups focus on just one specific area or issue. This is a function of focus but also a function of directing the rather meager financial and technical resources in trying to solve one specific problem. However, once they crack that to a reasonable extent, they often enter into adjacent markets by leveraging the cumulative experience, expertise and other resources. The resources are not restricted to manpower and investable funds or technology but increasingly includes the data that had been collected in the context of the earlier service or services. Just imagine if they could not use that data for offering new services of offerings, would it really be possible for them to do so? Would Gmail have become viable if Google could not use the data it had collected earlier for search only? Likewise, could WhatsApp offer a payment service if it was limited to messaging only? Or, would Paytm have been able to offer E-Commerce if the data collected by it were limited to payments only?

Clearly by choking off using data collected for extremely specific purpose from being used for any other service, we would unwittingly make both the original proposition less likely to succeed or scale while making the second or third order innovations impossible, well almost.

If startups are not able to collect data easily enough and provide newer services based on intelligence and knowledge gathered from that data, there will be three kinds of adverse impact. Firstly, existing startups that are providing a specific service will not be able to scale up. Secondly, entrepreneurs planning to start a digital/data business will hold back. Lastly and most worrisome, investors

will stop making risk investments in startups. There will continue to be some investments in balance sheet companies as it happens now, but that is not India's collective expectation from digital startups. We need many more PayTMs and Zomatos to relaise the full potential of the digital economy.

We must recognize that foolproof security and 100% privacy are illusions, whether in physical world or in the digital world. Consequently, the principle of proportionality needs to be applied not just to platforms and service providers, but equally to the means envisaged in the law to protect privacy as also their impact on other highly desirable outcomes in terms of economic growth, jobs, innovation, and entrepreneurship.

Is trading off privacy for economic opportunity what is being suggested? Certainly not. Rather, what follows consequent to these arguments is a combination of several approaches to strike the right balance between protecting privacy and protecting economic opportunity. Easing the process of data collection with suitable safeguards and enabling more extensive exploitation of anonymized personal data are good candidates to start with.

The PDP Bill rightly excludes anonymized data from the definition of personal data. Yet, what is given with one hand could end up being taken back with the other. This issue is getting muddled by fears of de-anonymization. Naysayers cite the rising capability of big data and ML tools to do so. Excessive enhancement of anonymization requirements effectively erodes the value of the data without necessarily enhancing security or privacy. A better approach might be to lay down reasonable anonymization requirements for using personal data and making deanonymization and usage of such data thereafter, a punishable offence.

Unduly onerous conditions for collection, storage, processing, and anonymization of data create an environment in which only established platforms – typically global players that have deep pockets and which already possess vast pools of data and technical and legal expertise - can comply with the complex web regulations (or at least create an appearance of compliance). What follows is entirely in consonance with the law of unintended consequences. The booming startup eco-system, the growing but still nascent data economy and the birth of new technologies based on AI/ML that are built on top of the oceans of data we generate would all be severely impaired.

So why are the startups and entrepreneurs not protesting loudly enough? Maybe it is because no one wants to proffer an argument that appears to fall foul of champions of privacy, though in fact, it does not. Perhaps it is on the presumption that this is a zero-sum game so anything that restricts large platforms would be good for small players. Or perhaps the reticence is based on the consolation that the restrictions envisaged are applicable only to large platforms. These arguments are fallacious.

Large platforms have the ability and the financial and technical muscle to navigate the type of curbs envisaged in the draft PDP Bill. So, a collateral impact would be that existing large companies that have in the last 10 years collected a huge amount of static data from their users and continue to collect dynamic data sitting on a base of hundreds of millions of customers, will have deep enough pockets to continue to comply at least on paper with the rules and scale up.

Startups on the other hand, lack such resources and capabilities. So more unnecessary regulatory constraints on data means fewer startups and even fewer successful ones. This is dangerous for fair competition in the market. The exemption to small players is an illusory protection afforded to them. It implies that we are encouraging the perpetuation of the 'small is beautiful' syndrome and providing relief to small players – but only as long as they remain small. This is akin to the SME question. We need policy clarity on whether the policy is aimed at keeping SMEs small or helping them to grow big. In the digital world where network effects dominate, providing protection only so long as an entity is small is exactly wrong.

A significant part of India's economic aspirations is centered on the digital economy. We badly need the economic growth, the jobs, the innovation, and the entrepreneurship opportunities waiting to be unlocked. A more thoughtful approach to putting in place necessary safeguards to protect our rights while simultaneously protecting our economic opportunities is an imperative. The PDP Bill and the mode of its implementation is a good place to start.

The proposed authority would do well to broker such a grand bargain from the intermediaries on behalf of the individual users. That in and by itself would be a pragmatic way to advance both privacy and the impetus for start-ups!