Centre for
The Digital Future

Report

Impact of the proposed Data Protection Bill, 2021 on Indian start-ups

JULY, 2022

Lead authors

Nishant Chadha

Yuva Simha Korlabandi

Executive summary

The Data Protection Bill 2021 (henceforth the Bill) proposes a consent based framework to ensure individual privacy in the digital world. Its objectives include

- Protection of the digital privacy of individuals relating to their personal data
- A trustworthy framework for organizational and technical measures in processing of data
- Creating a collective culture that fosters a free and fair digital economy, sustainable growth of digital products and services

The consent based framework of the Bill is rather similar to the GDPR and aims to provide users complete control of their data, thus giving them the ability to protect their privacy in the digital world. The Bill, of course, has implications for user privacy and security online, and, since it regulates the use of digital data, for the workings of the digital economy.

This report is concerned with understanding the potential impact of the Bill on one aspect of this digital economy, digital start-ups. Thus, it should not be viewed as an evaluation of the Bill, which would necessarily include weighing the impact on users with the impact on businesses.

India has the world's third largest start-up ecosystem with 38,815 active start-ups as of 2021 and has seen an average of 4000 start-ups being launched annually since the last 13 years [1]. Sectors relying on the use of personal data, like fintech, consumer services and health tech have more than 10% of total active start-ups each.

Fintech has 11% of total active start-ups and is the most preferred start-up sector for seed funding. More than 50% of this funding to the fintech sector was received by lending tech and insurance tech sub-sectors, which intensively use personal data for their business activities.

Similar is the case with health tech and consumer services sector where the fastest growing sub-sectors are the ones that use personal data intensively. While these are some illustrations there are start-ups across sectors relying on the use of personal data which could see significant impact on their operations from the Bill.

Data protection (DP) regulation, whether directly, for example, through purpose or collection limitation, or indirectly, for example, through the consent framework, restricts ways in which data can be used and monetised. Therefore, if the regulation is well implemented and companies haven't already complied with these restrictions, the immediate impact of the regulation will be to reduce the level of activity in the digital economy. But in the long run such regulation may encourage 'responsible' innovation, i.e. innovation of new products or services which exploit personal data to the extent society is comfortable with. To an extent, such has been the case with environmental regulation. The role of policy is to facilitate such innovation and adjustment in the long run.

More to the purpose of this report, the question is also whether DP regulation will have a differential impact on start-ups, compared to incumbents? We believe that it will. For two reasons. First, start-ups have costlier access to finance compared to incumbents. This lowers their ability to meet compliance costs or make business process adjustments. Second, start-ups may not have matured data models yet. This means that the incidence of provisions like collection limitation may be more on them.

Early evidence from the European Union (EU) shows that the GDPR has asymmetrically impacted smaller firms and led to increased market concentration of more established

firms [7]. In the e-commerce space, it is estimated that loss of revenue for small firms is nearly double that of big firms [8]. And in the AI space, GDPR led to a reduction in the number of smaller web technologies and has increased the market share for established companies, thus raising concerns over possible negative externalities to market competition [9]. Therefore, at least in the short run the impact on start-ups is negative and asymmetrically higher.

To understand the potential impact of the Bill on start-ups we study various provisions of the Bill separately to theorise how each of them might impact start-up activity. We then validate our findings with a short online survey of start-ups.

We divide the costs that the Bill can impose on companies into two categories – pure compliance costs and business process redesign costs. Pure compliance costs – such as appointment of a data protection officer – are purely monetary and, more importantly, are certain. Business process redesign costs – such as redesigning the data model due to constraints imposed by collection limitation – require human resources and innovation. And are neither purely monetary nor entirely certain. We believe that pure compliance costs, because of their certain nature, can be internalised by markets and may not be too onerous. Business process redesign costs on the other hand can impose significant and asymmetric burden on start-ups.

Relevant provisions of the Bill that can impose business process redesign costs include those relating to notice and consent, purpose limitation, collection limitation, data localisation, data categorisation, and data portability. There are also provisions that will impose purely monetary and certain costs such as reporting of data breaches within 72 hours.

The consent framework limits how companies can use data. This will lead to an increase the costs of providing digital services and may also lead to an increase in the prices of such services for consumers. The impact for start-ups could be higher since they foreclose certain avenues of monetisation in the future for start-ups who do not yet have matured business models. They also limit the scope for experimentation. And seeking consent repeatedly can impose costs on both consumers and companies without improving privacy outcomes significantly.

Data localisation may not be as onerous in the long run, if the local data storage and processing sector grows rapidly.

Data portability can level the playing field between start-ups and incumbents by allowing consumers to move to newer companies without losing the value of their data held by the incumbent. Similar will be the effect of encouraging the sharing of non-personal data (NPD). However, in the design and implementation of both of these provisions dynamic incentives for data generation need to be respected.

The online survey confirms our theoretical analysis of the Bill. Based on the sample of responses two main points emerge. The start-ups perceive that the impact of the DP Bill will be mixed

1. The issue of purpose limitation and seeking fresh consent from the users at a later point in time is the most vexing for start-ups with almost 70% start-ups agreeing that seeking fresh consent will adversely impact their business operations.
2. The inclusion of NPD and data-portability may increase the access of start-ups to data. This may make up to some extent for increased cost of collecting new data. Start-ups consider this to be a positive move. About 60% of the respondents say

that NPD inclusion and data portability will positively impact their business operations.

The need for certainty in personal data regulation in India cannot be denied. And at a more fundamental level Indian society's desire to safeguard people's personal data and hence informational privacy online, as also expressed in the Supreme Court judgments, also demands a policy intervention. This report attempts to understand the impact of the DP Bill 2021 on Indian start-ups. We find this effect to be mixed.

There is now increasing realisation that the consent framework does not guarantee individual privacy online since it imposes a very high burden on the users [16]. As already mentioned above, there is evidence from the EU that the GDPR, relying on the consent framework, imposes asymmetric and high costs on start-ups. This report finds that this is likely to be the case in India too. This raises questions about the suitability of the consent framework as the core of the DP Bill. The attempt now should be to devise a regulation which provides real safety online for India's population and, if possible, is less damaging to start-up activity.

Table of contents

1.0 Data Protection Bill, 2021

While upholding the right to privacy as a fundamental right within the constitutional framework of India in 2017, the Supreme Court had recommended a robust legal regime for data protection while recognizing that *"Informational privacy is a facet of the right to privacy"*.[1]

Following this recommendation, a decade long process of framing rules for informational privacy online culminated in the Personal Data Protection Bill, 2018. After feedback and the recommendations of the Joint Parliamentary Committee (JPC) of the Indian parliament the Bill was introduced in a new "avatar" as the Data Protection Bill, 2021.

The new version of the Bill restricts itself to digital data. While the 2021 Bill deals primarily with personal data and its usage, it does bring non-personal data within the ambit of the Bill and thus the Data Protection Authority as well.

The objectives of the Bill are

- Protection of the digital privacy of individuals relating to their personal data
- A trustworthy framework for organizational and technical measures in processing of data
- Remedies for unauthorized and harmful processing
- Ensuring the interest and security of the State
- Creating a collective culture that fosters a free and fair digital economy, and sustainable growth of digital products and services
- Ensuring empowerment, progress and innovation through digital governance and inclusion

While there are significant differences in the two versions of the Bill, the core of the Bill is still a consent based framework to protect privacy online.

The consent based framework of the Bill is rather similar to the GDPR and aims to provide users complete control of their data, thus giving them the ability to protect their privacy in the digital world. The Bill, of course, has implications for user privacy and security online, and since it regulates the use of digital data, for the workings of the digital economy.

This report is concerned with understanding the potential impact of the Bill on one aspect of this digital economy, digital start-ups. Thus, it should not be viewed as an evaluation of the Bill, which would necessarily include weighing the impact on users with the impact on businesses.

The rest of this report is structured as follows – section 2 provides a brief background of the start-up ecosystem in India, section 3 lays out a conceptual framework to understand the impact of data protection regulation on economic activity, section 4 summarises some literature on the impact of the GDPR on start-ups in Europe, section 5 contains a theoretical analysis of the possible impact of various provisions of the Bill on start-ups, section 6 presents the results of an online survey carried out by CDF and section 7 concludes.

[1] https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

2.0 Start-up ecosystem in India – A background

India has the world's third largest start-up ecosystem with 38,815 active start-ups as of 2021 [1]. Indian start-up system is growing rapidly with an increased number of start-ups being launched, an increased number of $100 million funding rounds, and an increased number of start-ups becoming unicorns. Indian cities rank among top world cities for launching start-ups; cities like Bangalore, Mumbai and NCR region are among top 20 for launching start-ups. Indian start-up ecosystem has very high growth rate of 15% year-on-year for the year 2018. It is expected to grow at consistent annual growth rate of 12-15% [2].

Over 26 state governments have start-up policies to create, support and nurture vibrant ecosystem in their respective states. The central government has also taken a very active approach to build up the start-up ecosystem in India. E.g., the Atal Incubation Centres (AICs) were set up in multiple cities to nurture innovative start-up business to become scalable and sustainable enterprises while much needed financial support has been extended through various ministries and financial institutions. Furthermore, central government has provided schemes like Aspire, Stand-Up India, etc., to provide support to start-ups in different sectors and to different sections of people in India.

The start-up ecosystem has witnessed an average of 4,000 start-ups being launched every year for the past 13 years. The start-ups launched are not concentrated in a few sectors; rather they are spread across different sectors like enterprise tech, e-commerce, fintech, consumer services, health tech, etc. The data needs of different types of start-ups in different sectors are also different. For example, start-ups in sectors like enterprise tech, Deeptech, etc., require large volume of non-personal data, whereas start-ups in sectors like consumer services, health tech, fintech, etc., require personal data for their business activities.

Sectors, relying on personal data, like Fintech, consumer services and health tech have more than 10% of total active start-ups each. The start-ups in these sectors are very active in different stages of funding. Fintech has 11% of total active start-ups and is most preferred start-up sector for seed funding stage and growth stage has total funding of $12 Billion for years 2014-2020. More than 50% of this funding to fintech sector was received by lending tech and insurance tech sub-sectors, which require personal data for their business activity.

Similarly, consumer services which is most preferred sector for funding at bridge stage has sub-sectors foodtech and discovery which received more than 55% of total funding of $7.4 Billion to consumer services sector. Health tech, which is among the top five at all stages of funding has sub-sectors like fitness & wellness, online pharmacy and telemedicine, which got nearly 40% of the total $2.5 Billion funding for the Health tech sector. These sectors too depend on personal data for their business activity.

While the above are some illustrations of sectors where personal data dependent sub-sector start-ups get majority of the funding in the given sector, in every sector, there are sub-sectors where personal data is important for their business operations. Thus, the data protection bill could affect all possible sectors but the impact varies from sector to sector. This could affect the growth and innovation in different sectors differently and could lead to asymmetric growth of few sectors and hampering the all-round growth. This is obviously true in sectors where personal data is an important element for business operation.

It is thus important to understand the impact of the DP Bill on start-ups – as clearly, a number of high growth start-ups depend on the use of personal data. And as a second order effect, even creation of non-personal datasets will slow down with the slowdown in

the collection of personal data. This latter is because in many instances, if not most, personal data needs to be combined with non-personal data to derive value. E.g., insurance companies need to combine the personal driving distances with the non-personal road and traffic situations in which the driver drives to get an estimate of the risk of accidents. Or, a credit giving company needs not only the credit record of the individual but also the success, or failure, of similar businesses the borrower wants to invest in.

The next section introduces a conceptual framework to dissect the impact of data protection regulation on economic activity.

3.0 Data protection, economic activity and innovation

3.1 Data protection as social regulation

Regulation of markets broadly falls in three categories. Anti-trust regulation, economic regulation and social regulation [3]. Anti-trust regulation (also called competition regulation) focuses (mostly) on the otherwise unregulated sectors of the economy where we rely on competitive forces to ensure good economic results.

But not all markets can be competitive – as is often the case with natural monopolies. Economic regulation focuses on sectors – like telecom, power etc. – where we cannot rely on competitive forces to ensure efficient economic outcomes. This regulation can take the forms of controlling price and quantity or controlling entry and exit of players, etc.

Finally, there is social regulation – such as environmental regulation or safety standards – where competitive markets will not achieve socially desirable outcomes. For example, automobile safety standards were gradually tightened over time in the US in the 1960s and 70s because market competition did not lead to cars that were safe enough by socially acceptable standards. The requirement for social regulation can arise because of the presence of information asymmetries – such as in safety standards – or externalities – as is the case with environmental regulation.

Data protection is a social regulation – quite akin to safety standards. Digital companies primarily use personal data for one purpose – personalisation. This allows them to provide, and for consumers to enjoy, services that would not be possible without data. Examples of this include personalised search, customised plans and prices for services, etc. Business models for monetising these services range from subscription fees to advertising – where firms can use information derived from personal data and machine learning models trained on aggregated datasets to target advertisements better and, hence, providing more value to advertisers.

Data is non-rival and recombinant. This means that the use of data by one entity does not limit its use by another. And, that data can be repurposed and combined with other data to produce datasets that have more potential than either dataset individually does. Finally, the most important fact is that data is in itself not meaningful. What is meaningful is insights that can be drawn from it – and that requires the skill of human beings. Thus the same data will be used by different companies quite differently.

All of the above imply that there is information asymmetry between individual companies and consumers on what data is collected, why is it collected and how it is used. Data once collected is potentially usable for ever and in ways that are not comprehensible easily to the person whose data it is. Companies can thus, potentially use this data in ways which if the consumer was aware of, they may not have agreed to use the service. This will lower

consumer value and potentially also consumer trust in the market. This creates scope for a data protection regulation.

3.2 Impact of data protection on economic activity and innovation

Firstly, note that the impact of the proposed Data Protection Bill 2021 can be grouped into two heads – pure compliance costs and business process redesign costs. One of the requirements of the Bill is the appointment of a Data Protection Officer in the business. This is purely a monetary cost and is a part of compliance costs. In addition to cost of doing business, compliance costs have two properties --- they are uniform across the board for all companies and, they have no uncertainty associated with them.

The second set of costs, however, is related intricately to how companies use data to provide services and what their business models are. An example of this type would be business models which rely on intensively collecting data first and then monetising it. To generate value from data, they need to run data models with different types of data to get the "best fit". If the Bill restricts what type of data can be collected, or requires start-ups to declare upfront why they need certain types of data, this will restrict start-ups from experimenting with different data and, hence, restrict innovation. This increases uncertainty among start-ups --- not knowing whether the data they are collecting is enough --- and affects sectors differentially --- mix of personal and non-personal data to get the best model are different in different sectors. In this section we discuss the conceptual nuances to understand the business process redesign costs.

An important point to remember, and that we make in some detail below, is that the impact of any regulation isn't simply static – there is also a dynamic impact. And the dynamic impact is shaped by the regulation.

Imagine a two dimensional space in which we could arrange all existing technologies plus business models currently in use. The technologies are arranged on the x-axis in order of their time of invention with the newer technologies appearing to the right. On the y-axis we have a scale, that measures for each technology (and business model), how much personal data it exploits with business models using more data appearing higher up on the axis. Such a situation is represented in Figure 1 Panel A.

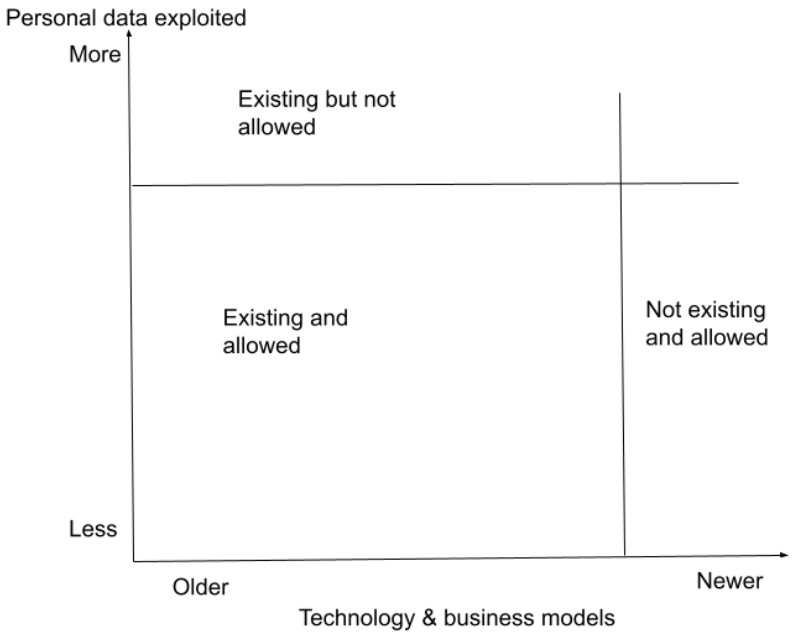


Figure 1: Allowable space for the operation of data businesses

The vertical line in the figure is the boundary of existing technologies. Business models to the left of this line are the ones that exist (or have been in the past). Innovation (either in technology or in business processes) of newer products or services would push this boundary to the right. Some of these technologies would rely on using personal data intensively while some may not. The horizontal line in the figure displays the ceiling of how much data exploitation is allowed. The area below this line are the business models that are allowed by regulation. Tightening of regulation will shift this line down. Thus current business practices that are allowed would lie in the rectangle labelled "Existing and allowed" as shown in the figure. The other labels can be similarly understood.

An illustration can make the use of this graphical framework clear. Take two existing models, an older and a newer, of personalised search. The older model is monetised through targeted advertising. This would be the case with, for example, Google Search. The newer model, Neeva (www.neeva.com) for example, is monetised through subscription fee. In this case, the first business model exploits data to a larger extent than the second one – since, as of now, they are not using inferred information to target advertising. How will they appear in the two dimensional space? Figure 2 illustrates this.

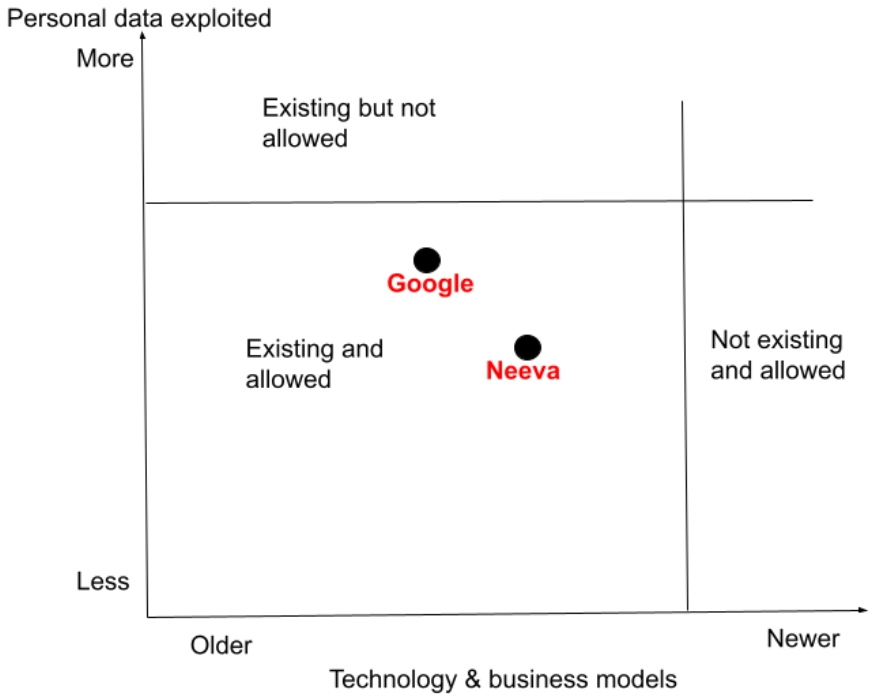


Figure 2: Mapping business models onto the allowable space

Following the tightening of data protection regulation (or in the present scenario, the introduction of such regulation) what data companies can collect, how they can use the data they collect is more restricted. Hence, this will result in this line moving lower, thus decreasing the allowed space for business operation. This is illustrated in Figure 3 below. The shaded area in the figure is the set of business models that are no longer allowed under the law. The size of this shaded area will be a measure of the **immediate loss** in economic activity due to data protection. Also no innovation can now take place above the threshold.

In the long run though, the situation may be different. Because in the long run technological innovations can push the boundary of what is possible out. This is illustrated in Figure 4. Thus in the long run, the regulation may direct innovation in the direction of technologies and business processes that do not exploit data in the same way as existing technologies.

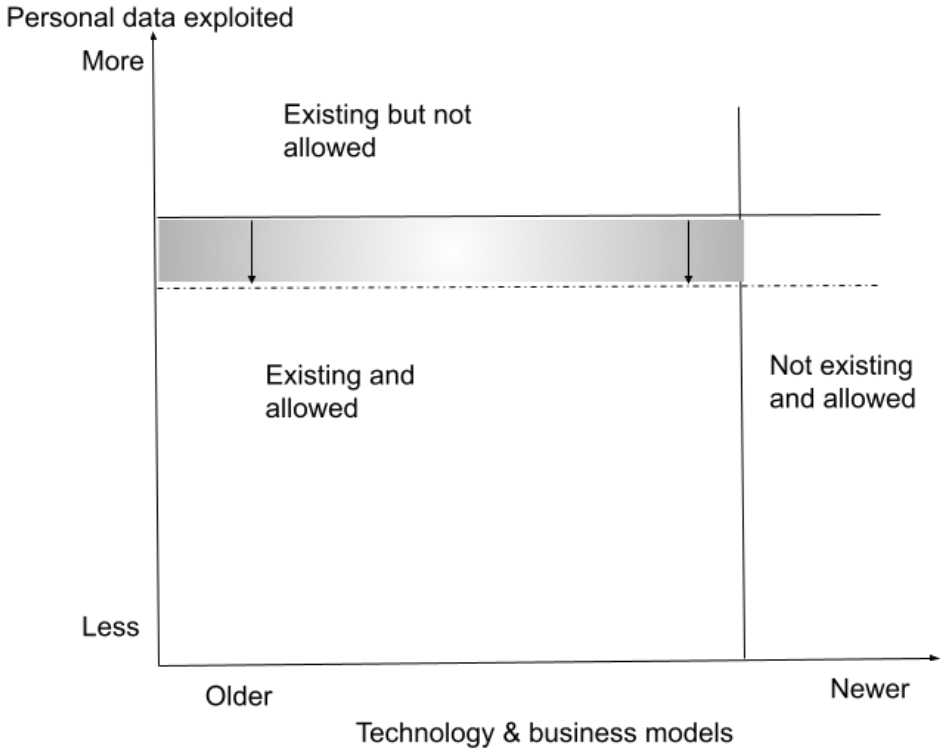


Figure 3: Immediate impact of tightening data protection

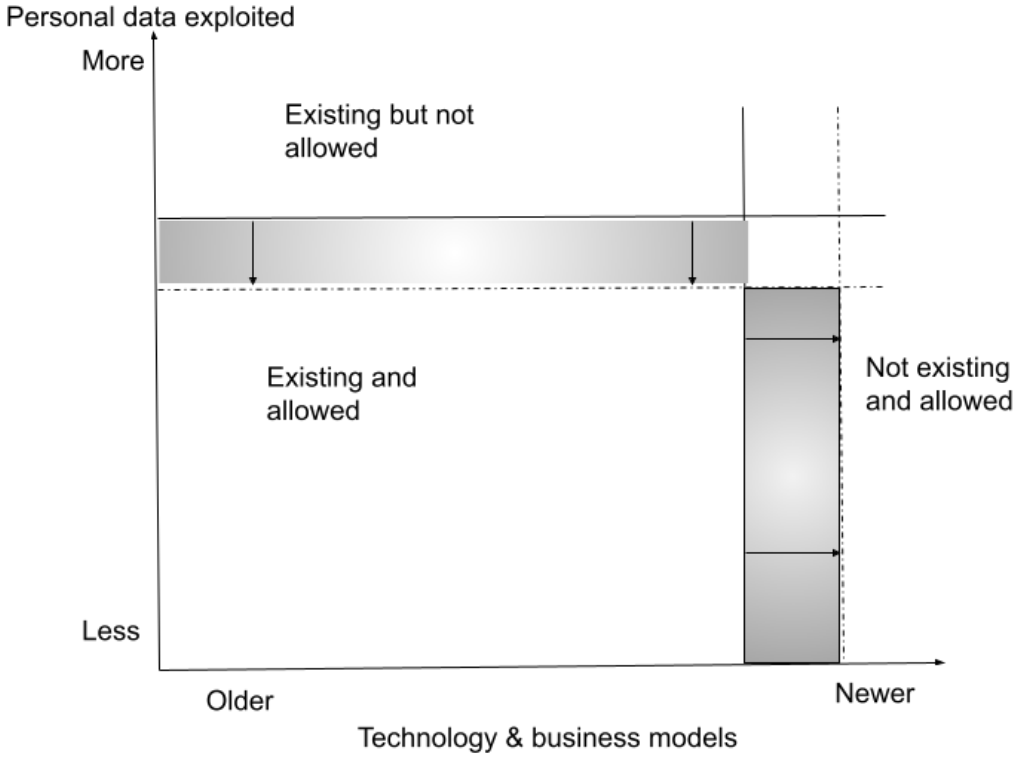


Figure 4: Long term impact of data protection- moving out of the technology frontier

Evidence from environmental regulation – which has an older history than data protection supports the idea of this differential impact in the short vs. the long run.

Blind et al. (2004) [4] find that the EU's strict regulation of genetically modified organisms amounted to a virtual "moratorium on their commercialization", prompting a substantial reduction in innovation activity. Whereas, Blind (2012) [5] finds that stricter product and environmental regulation has a significant positive effect on patenting intensity, confirming earlier findings by Rennings and Rammer (2011) [6], who also reveal that regulation-driven innovations are as successful in the market as other innovations.

3.3 Incumbents vs. start-ups – who will be impacted more?

The impact of the DP Bill can be different for start-ups and incumbents for two reasons –

1. The incidence of the bill itself is different across larger incumbents and smaller start-ups
2. While the incidence is similar, the ability of the two types of companies to respond to the incidence is different

We can expect both of the above to be true to an extent. Start-ups have fewer customers, and lesser data when compared to incumbents. They also have data models that are not matured yet. This means that certain provisions in the bill – such as purpose limitation (discussed in detail in a later section) – can have differential impact for start-ups vs. incumbents.

Start-ups also have costlier access to financial resources to meet compliance costs or redesign business processes. Thus their ability to comply with the DP Bill provisions may also be lower than that of incumbents.

While it is too early to answer this question for India, as we discuss in the next section, early evidence from EU suggests that Data Protection Regulation does impact start-ups more – at least in the short run.

4.0 Impact of GDPR on start-ups

The guiding principle of GDPR is data minimization, where GDPR accords data rights to EU residents and requires firms to encrypt and anonymize personal data. Further, firms are required to notify the regulator and affected individuals after a data breach. Though GDPR is a harmonized law within the EU, its enforcement varies by country as enforcement is split between a central EU supervisory and authorities in each EU country. Among other laws around jurisdictions, the Data Protection Bill 2021 is heavily influenced by the GDPR.

While the GDPR is a European law designed primarily to protect European consumers, given the nature of the digital economy its scope extends beyond EU's borders, since any firm with customers in EU has to adhere to it. Given the interconnectedness of world economies firms outside Europe has customers in Europe, so they must reallocate firm resources to comply with the law along with firms based in Europe.

Certain industry and business reports suggest that companies have incurred costs of over 10 million dollars to comply with the law [7]. It has also been argued that GDPR has asymmetrically impacted smaller companies and led to increased market concentration of more established companies [8]. In the e-commerce space it is estimated that loss of revenue for small firms is nearly double of big firms. And in AI space GDPR led to reduction in the number of smaller web technologies and has increased market share for established

companies, thus raising concerns over possible negative externalities to market competition [8].

The rest of this section discusses in detail papers that exclusively study the impact of the GDPR on start-ups and innovative activity by start-ups.

Artificial Intelligence (AI) has the potential to boost human productivity and economic growth. AI (or rather Machine Learning, the technology that provides 'AI') relies critically on availability of data, and often includes data on individuals to train and tune algorithms such as neural network and ensemble learning algorithms. The GDPR while increasing regulation to protect consumers' privacy, negatively impacts firms that need data to develop AI products [9]. This is more likely to be the case for start-ups who have not already collected the data they want to work with [10]. Larger companies may be able to access data more easily from already established relationships and could benefit from complementary business models which provide data as by-product.

To assess the impact of GDPR and data regulation on AI start-ups and to examine the importance of data to AI product development, Bessen et. al. [11] administered a survey to 131 companies.

In the survey, companies have a median size of less than 50 employees. The study finds that to access additional training data, around 50% of startups retain secondary reuse rights to their customer's data. Most firms that have secondary reuse rights to customer data report adhering to a data retention policy.

69% of firms reported creating a new position to handle GDPR-related issues and 63% firms had to reallocate resources due to impact of GDPR regulation such as limits to types of data that can be stored. AI firms place high value on use and access to training data. 75% of firms surveyed reported having deleted data due to GDPR regulations and responded that this could impact the ability to innovate and dampen AI advancement.

Even though smaller firms with less than one million dollars in revenue are exempt from GDPR, the smaller firms are more impacted by GDPR than larger firms. The differences between smaller and larger companies are both in terms of access to financial resources and access to trained staff and divertible resources.

It is difficult even for high-growth potential start-ups to raise capital [12] whereas larger firms have additional capital to hire required skilled labour. They also have slack resources such as excess computing capabilities to run valuable experiments and are more likely to reallocate resources which help them manage customer and personally identifiable data [13] and thus having lower impact than start-ups.

Digital firms represent 4% of EU's economy and 10% of retail sales. As advertising and e-commerce sales are the main sources of revenue for such firms, limiting the use of personal data may have unintended consequence of harming the existing business models of online firms. From the perspective of carrying out an empirical study privacy regulation creates an inference problem where data protection regulation can obscure the real economic impact from the effect on recording of data – for example, privacy regulation can reduce page visits by customers but may not have much impact on revenues – the real economic outcome.

So, to distinguish between GDPR's impact on real economic activity and the process of recording economic outcomes, a study [14] was conducted using data from web analytics

companies. Web analytics companies provide technology for websites to track users and browse sales. The dashboards from web analytics reveal revenue performance overtime and broken down by various categories like user country of residence etc. The study considers weekly panel data of 1084 analytics dashboards (firms) for 32 weeks in each of 2017 and 2018. The primary outcomes of interest for the study are page views and revenue. Only dashboards with at least 500 weekly visits form EU prior to GDPR's enforcement to ensure EU-relevant data and to avoid any noisy data outcome due to low traffic. And dropping more dashboards which are for testing purposes, frequent outages, etc. gives a sample of 353 e-commerce dashboards.

The companies considered in the study have long right tails in distribution for both page views and revenue. The primary empirical approach applies panel difference estimator (resembles difference-in-difference approach), where the control group consists of 2017 outcomes from set of dashboards as treatment group. The point estimates indicate a 11.7% drop in recorded page views and 13.3% drop in recorded revenue. The strictness of GDPR is not uniform across countries. So, a normalized index is constructed that ranges from -1.64 to 1.49 to examine the role of regulatory strictness. It was found that one standard deviation increase in regulatory strictness reduces recorded page views by 2.1% and recorded revenue by 4.5%.

The effect of GDPR on business activity can be explained by three principle mechanisms namely consent, marketing and privacy frictions.

During the sample period most websites relied on de facto opt-out consent. Previous research has demonstrated that when given a choice users choose the default option with a higher probability. Thus for websites relying on de-facto opt out consent, this approach ensures high consent rates and platforms in the study reported consent rates of more than 90%. Whereas sites that followed a strict opt-in approach have lower consent rates. Sites reported consent rates less than 10% where strict opt-in was followed [15] (UK and Netherlands).

The GDPR has also raised the legal risk and logistical cost associated with personal data processing. In another study it was found that only 64% of consumers provided consent even when offered incentives [16].

The quantity and efficiency of firm's marketing could also be reduced by GDPR. Companies in the study reported high costs of complying with GDPR and had todivert funds from discretionary expenses like marketing. The study also found that e-mails precede 3.9% page views and 7.9% revenue while display ads precede 1.3% page views and 0.4% of revenue. Thus, GDPR could affect firm's revenues by adversely affecting firms marketing channels.

Privacy frictions interrupt user's browsing and deters users from continuing to browse and leads to decrease in real outcomes. To see if this is indeed the case the above study on e-commerce performs a simple empirical test on user bounces (browses a single page and leaves). Bounces should ideally increase if there is increase in privacy frictions. The pre-GDPR bounce rate was found to be 37% in e-commerce sample. Post-GDPR there is not much change in bounce rate, and this is due to the fact that most firms used opt-out consent mechanism. Number of firms with opt-in consent is low in the sample considered but for the sample of firms with opt-in consent bounce rates decreased by more than 20% but recorded page views reduced by more than 50%. Using panel difference model

estimating bounce rates shows 0.275% fall for all sites and 0.354% fall for e-commerce sites. So, the privacy frictions do not contribute to GDPR effect in firms.

The study concludes that consent accounts for at least 7% of the recorded page views and 29% of the recorder revenue estimates, whereas marketing effect alone represents 9.4% of recorded page view and 7.6% of recorded revenue estimate. The study was conducted in 2018 during which there is limited regulatory enforcement and website compliance efforts are inadequate. From study it was further observed that larger firms may benefit from GDPR as they obtain consent more easily and could benefit from economies of scale. Whereas smaller firms couldn't obtain the same. It was observed that decline in revenue for small firms is 17.4% whereas for small firms is 8.9%. This disparate effect on small firms could create concentration in market.

5.0 Impact of specific provisions in the DP Bill on start-up activity: Analysis of various provisions

In this section we provide a detailed discussion of various provisions of the DP Bill that can impact the start-up ecosystem. This includes the relevant clauses. We also discuss the possible nature of the impact of these provisions, positive or negative. The highlights are presented first, followed by a detailed discussion.

Highlights

- Relevant provisions that can impose business process redesign costs include those relating to notice and consent, purpose limitation, collection limitation, data localisation, data categorisation, and data portability
- There are also provisions that will impose purely monetary and certain costs such as reporting of data breaches within 72 hours
- The consent framework can increase the price of goods and services since these limitations place a constraint on the business model that companies can follow. The impact for start-ups could be higher since they foreclose certain avenues of monetisation in the future for start-ups who do not have yet have matured business models. And seeking consent repeatedly can impose costs on both consumers and companies without improving privacy outcomes significantly.
- Data localisation may not be as onerous in the long run, if the local data storage and processing sector grows rapidly.
- Data portability can level the playing field between start-ups and incumbents by allowing consumers to move to newer companies without losing the value of their data.

Notice and consent

The provisions related to notice and consent ensure that data is collected from the user with informed consent. The clauses which contain these provisions are

Clause 7 – Every data fiduciary shall give to the data principal, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as is reasonable practice, a notice containing the information specified

Clause 11 – The consent given by the data principal is valid if the consent taken is free, informed, specific, and clear and data principle is capable of withdrawing such consent.

Clause 34 – Data fiduciary shall take explicit consent from data principal when sensitive personal information is transferred outside India, given that authority has approved for such transaction.

These set of provisions imply that firms need to seek consent from customers whenever they visit the website or use the application. Such consent is typically obtained through a privacy pop-up box. This effectively standardizes the consent mechanism to an opt-in mechanism for all companies, which could lead to decrease in number of visits to website – known as consent fatigue or privacy frictions.

A big part of services in the digital world is creation of consumer types or profiles. These profiles can be used by the company to provide better services to the consumer and/or monetise this information, say through targeted advertising. Profiling may require collection of data categories that are not directly related to the provision of service and informed consent may decrease the user's willingness to provide such data.

This could affect those companies which require tracking data (generally done through cookies). As these companies need personalisation data to determine the consumer preferences (ex: e-commerce). While on the other hand if firms don't require much tracking or additional data for personalisation, they are likely to be less affected by this clause.

For start-ups the specific impact of these provisions – especially clause 34 – will be to slow down the pace of data collection. And given that the marginal benefit of data collected is highest in the earlier stages of AI/ML models this could have negative impact on their outcomes.

Repeated requirement of consent may likely introduce fatigue and make consumers less likely to experiment with newer services, again adversely affecting start-ups more.

Collection limitation

The DP Bill makes it mandatory for companies to only collect that data which is strictly necessary to provide the particular service. Provisions related to collection limitation in DP bill draft are contained in

Clause 6 – The personal data shall only collected to the extent that is necessary for the purpose of processing personal data

Clause 9 - Personal data shall not be retained beyond the period necessary to satisfy the purpose for which it is processed, and the personal data shall be deleted at the end of such period

Suppose that in the absence of any regulation the company collects a set $\boldsymbol{n}$ of personal data categories and uses a set $\boldsymbol{m}$ of non-personal data categories to provide a service $\boldsymbol{S}$. Note that it is possible that given its business model the company collects more data than is strictly necessary to provide the service per se.

After the introduction of the DP regulation it may be restricted to collect $\boldsymbol{n}'$ personal data categories, where $\boldsymbol{n}' \subset \boldsymbol{n}$ (i.e. n' is a proper subset of n). Now if personal data and non-personal data are substitutes in the design of the data model, then the company could collect $\boldsymbol{m}'$ non-personal data categories (instead of $\boldsymbol{m}$, $\boldsymbol{m} \subset \boldsymbol{m}'$) to make up for some of the disadvantage from the restriction.

So, if collection limitation is binding, then companies adopt to $\boldsymbol{m}'$ non-personal data variables such that $\boldsymbol{f}(\boldsymbol{n}', \boldsymbol{m}') \to \boldsymbol{f}(\boldsymbol{n}, \boldsymbol{m})$ as $\boldsymbol{n}' \to \boldsymbol{n}$ and $\boldsymbol{m}' \to \boldsymbol{m}$,[2] where $f(.)$ is the value created to company from data.[3] That is the firm, will be required to change its algorithms

[2] Formally, there is a sequence of sets $n_1, n_2, \ldots, n_k$ such that $n_1 \subset n_2 \subset \cdots \subset n_k$ and $n_k = n$ as $k \to \infty$. Similarly for the set of non-personal data m.

[3] More accurately if the collection limitation is binding then $f(n, m) > f(n', m') > f(n', m)$

and business models such that it can make up for the loss of personal data with non-personal data. This will generally result in loss of economic value generated.

A second possibility is that companies switch to a different business model and technology such that the value from it which we denote $\boldsymbol{g}(\boldsymbol{n}', \boldsymbol{m}')$, using data collected with restrictions is equal to or greater than $\boldsymbol{f}(\boldsymbol{n}', \boldsymbol{m}')$**.** That is, there is innovation in the market.

The company may collect additional data points, i.e. $\boldsymbol{l}$ such that, $\boldsymbol{n}' \subset \boldsymbol{l} \subset \boldsymbol{n}$, but it would need to seek separate consent for this and cannot deny the original service to the user if she refuses to share additional data. Early evidence from the EU suggests that consumers are unwilling to part with data when there is no new service being offered. In effect making collection limitation binding.

Though collection limitation could increase the privacy of the customers, collection limitation could also potentially increase the processing costs and, depending on market structure, some of these increased costs could be passed onto customers. This increase in price of the goods could reduce the number of users/customers in a given industry (as **n'** could vary from one industry to another industry).

Specifically for start-ups this could also impact experimentation to come up with the mature product since they cannot collect additional data to fine tune their models. On the flip side though collection limitation could encourage the entry of start-ups with technologies and business models that allow the provision of service with limited data sources, because it levels the playing field between business models that use data extensively vs. those which do not.

On the other hand, collection limitation may also level the playing field between start-ups and incumbents. A stricter data retention policy decreases the relative advantage that incumbents have over start-ups, thus decreasing the switching costs from incumbent firms to start-ups.

Purpose limitation

Data may be only be used for the purpose which it was collected for by giving notice to the user. Purpose limitation in data protection bill is given by

Clause 5 – Every person processing personal data of a data principal shall process such personal data in a fair and reasonable manner and ensure the privacy of data principal, and only for the purposes consented by the data principal.

Clause 20 – The data principal shall have the right to restrict or prevent the continuing disclosure or processing of his personal data by the data fiduciary where such disclosure or processing has served the purpose for which it was collected, consent of the data principal has been withdrawn, or made contrary to provisions of the Act.

Clause 31 – The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.

Let **A** be the purposes for which personal data is collected with consent. Then this data can be used for connected purposes **A'** such as archiving, research, census etc. But it cannot be used for any other purpose **B** which could come at later stage or in a segment which is different from what initially the data is consented for.

Note that for purpose limitation to have a bite it must be the case that at the time then firm is seeking consent it does not know what all purposes it will use the data for in the

future. Given the economies of scope in data and rapid advances in digital technologies this is quite common.

Another possibility is that the company does indeed know what it will use the data for at a later date. But seeking detailed consent may signal or even provide information about the company's data processing process to competitors and therefore the company does not wish to provide this information.

As stated before this clause limits the economies of scope. Take the example of an e-commerce platform that with data collected over time can identify customers who are tourists and can provide other services like travel insurance, sightseeing tours, etc., to them. By leveraging these economies of scope the company can reduce its costs and can also reduce overall prices to users. But if the firm needs to seek fresh consent these economies would not be exploited.

Purpose limitation can be especially onerous in those industries where input data is always a by-product from another industry. For example, in insurance sector it is difficult for entrant to get data to provide insurance related products. The firms must rely on products in other industries and then use that data in insurance sector. But with purpose limitation this may not happen.

Clause 31 is non-controversial in that it is important to have transparency and clarity in data markets. If the firms don't follow standard practice in first place, then this clause could drastically increase the costs and further leading to closure

Some clauses which give exemptions to purpose limitation through connected purposes are

Clause 38 – Exemptions for research, archiving and statistical purposes [But these exemptions will need more guidance]

Where processing such personal data is necessary for research, archiving, or statistical purposes, and Authority is satisfied that data fiduciary has followed anonymisation procedures.

Clause 39 – Exemptions for non-automated processing by small entities.

Clause 40 – The authority may, for the purposes of encouraging innovation in artificial intelligence, machine learning or any other emerging technology in public interest, create a sandbox.

These three provisions – notice and consent, collection limitation and purpose limitation - taken together constitute the consent framework in the DP Bill. And together they can increase the price of goods and services since these limitations place a constraint on the business model that companies can follow. These limitations can be especially constraining for start-ups since they foreclose certain avenues of monetisation in the future for start-ups who do not have yet have matured business models. Purpose limitation can curtail their ability to grow and pivot at later stages. And seeking consent repeatedly can impose costs on both consumers and companies without improving privacy outcomes significantly.

Data localisation

Data localisation refers to provisions in the bill which require certain types of data to be held only in India and not transferred outside its jurisdictions or where a copy of the data is required to be held in India. The clauses containing these proposals are

Clause 33 – The sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India. The critical personal data shall only be processed in India.

Clause 34- The sensitive personal data may only be transferred outside India for the purposes of processing, when explicit consent is given by the data principal for such transfer.

These of course impose compliance costs on firms since they may currently be holding data in jurisdictions that are more efficient economically, but also has effect on business in short term.

Data will be located outside India to reduce costs of holding and processing data when such costs are lower elsewhere compared to India. The immediate impact of the data localisation clause will be to increase costs of operation, especially if domestic capacity to store and process data is limited.

Data localisation is akin to import substitution. If India develops capacity and capability we could see these costs coming down over time. If instead costs are not reduced then this could have effect on start-ups. Start-ups depend on third parties for data processing (especially during initial phases). These higher data processing costs could pass on to start-ups and could adversely affect them.

Data portability

Clause 8 – Data fiduciary shall take necessary steps to ensure personal data is complete, accurate, updated and not misleading

Clause 10 – Data principal shall have regard for which his personal data is being processed and shall ask for correction and updating of data, completion of incomplete data.

Clause 19 – If processing is done through automatic means, then data principal shall have rights to receive data in standard readable format and have such data transferred to other data fiduciary. This will not be applicable to processing where it is necessary for the functions of state or on any judgement or quasi-judgement related areas.

Presently companies do not have the incentives to keep data in formats and structures which make it more amenable to transfer. But with these clauses in place, it makes it easier for users to move between companies for services without having to worry about loss of value from the new company not having any data on them.

This could effectively reduce market concentration (where few firms which hold vast amount of data in unreadable formats) and could improve start-up ecosystem and spur innovation. This would encourage firms to compete for the source of the data – the consumer, rather than depending on any advantage built through data.

Data categorisation

Clause 15 – The central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of the personal data as "sensitive personal data", having regard to risk of significant harm that may be caused to data principal, expectation of confidentiality attached and whether a significantly discernible class of data principals may suffer significant harm from processing of such category of personal data.

Clause 27 – Where a significant data fiduciary intends to undertake any processing involving new technologies or large-scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing shall not be commenced unless

the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions given.

Data categorisation can potentially increase compliance costs and thus increase entry costs in sectors that deal directly with such data. But these costs can be internalised as long as the categorisation of data is certain. So while there can be some compliance costs upfront, as long as there is certainty about the categories of data this clause should not impact companies adversely.

Pure compliance burden

The provisions discussed so far can have impact on the business models of the companies, also impacting entry of companies. Complying with them may require business process redesign including redesigning data processes and algorithms. Thus their costs may not be purely financial but also in terms of hiring staff and innovating new processes.

There are also certain clauses/provisions in the Bill that impose a pure compliance cost on the companies. These costs are pure financial costs on the company – often a onetime cost and do not require too much reorganisation. The following clauses are some of the more prominent ones in this aspect.

Clause 17 – The data principle shall have the right to obtain their data from the fiduciary. The data provided by data fiduciary should be clear and understandable by the customer. And data principal shall have right to access in one place the identities of data fiduciaries and the categories shared by a given data fiduciary.

Clause 21 – The data principal, for exercising any right, shall make a request in writing to the data fiduciary either directly or through a Consent Manager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period specified by the regulations.

This requires the company to create a system to share this information with the data principal.

Clause 22 – every data fiduciary shall prepare privacy policy containing various points notified by the bill (like organisation/ business practices, technology used, protection of privacy etc.)

Clause 23 – Every data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make the information available in such form and manner as may be specified by regulations.

Clause 24 – Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards.

Clause 29 – The significant data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor.

Clause 32 – Every data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner

These clauses could be time consuming for a small entrant but will also lead to better data practices and more trust in the digital economy.

Clause 25 – Every data fiduciary shall by notice report to the Authority about the breach of any personal data processed by such data fiduciary within 72 hours of such breach.

This clause increases the data security costs to companies – including costs such as those for cyber insurance. There by increasing the price of product offered to customers. These are compliance burdens likely to be proportionately higher for start-ups but on the other hand this should increase the security of data. Even without fines, reporting norms may enhance data security if the firm cares about its reputation in the market. And better data security may have an overall positive impact on the digital economy.

Overall this analysis suggests a mixed impact of the provisions of the DP bill on start-ups. Certain measures – those concerning purpose limitation and collection limitation can have significant negative implications for smaller companies. Others, like compliance costs which are certain, may not have any significant impact. Still others – such as data portability – may in the long run have positive implications for start-up entry.

We conducted an online survey of start-ups to elicit their beliefs about the impact on the DP Bill on their operations. The results are presented in the next section.

6.0 Survey results

CDF conducted a survey to determine start-ups' perception of the impact of the DP Bill 2021 on their business operations. The survey contains two sections. The first section asks questions about the start-up's business models, sectors of operation, year of incorporation, etc. In the second section, questions on different clauses and their specific impact on start-ups were asked. The questions in the second section are of multiple-choice type with options being agreed, disagree, no significant impact and unable to answer. Questions were framed in as neutral a way as possible to prevent signalling any researcher bias. The surveys were conducted online and a total of 26 responses were recorded in the last week of May and first week of June.

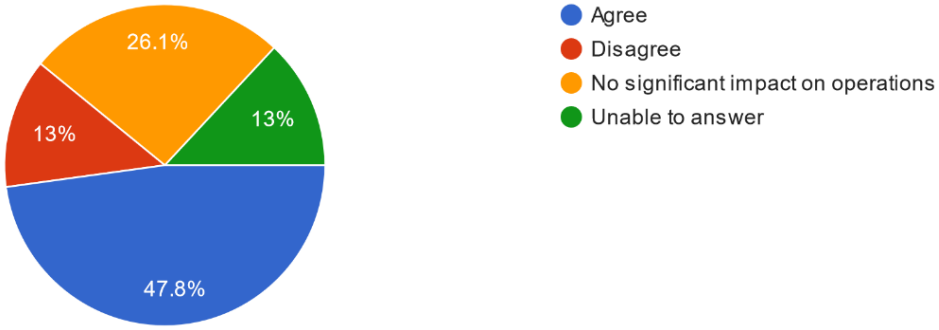
The incorporation year ranges from 2012 to 2022, where 17 start-ups incorporated in or after 2019. The area of business is varied. The e-commerce sector has the most firms, with a number equal to seven. More than half of the firms responded have less than 1000 customers, a quarter of responded have up to 10,000 consumers and the remaining firms have users above 10,000. We also recorded the 2021-22 financial year revenue. About 87% of firms have revenue less than 1 crore, 8.7% of firms have revenue between 1 and 10 crores and the remaining firms have revenue between 10 and 100 crores.

In the rest of the section we present the detailed results of the second part of the survey – on the impact of the DP Bill.

The impact of DP Bill clauses on business operations

Consent mechanism as proposed in the Data Protection Bill, 2021 will adversely impact our business.

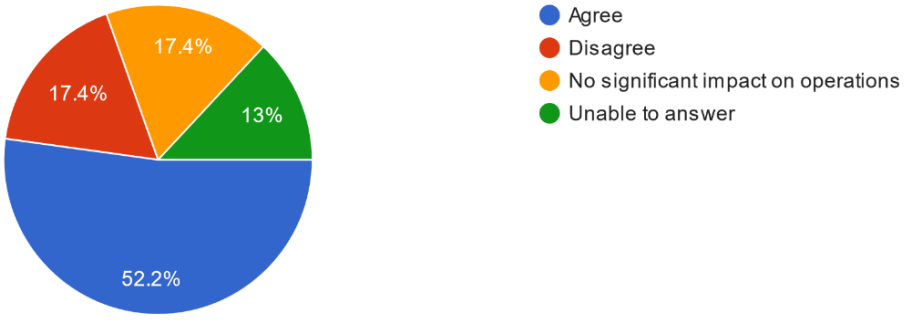
23 responses



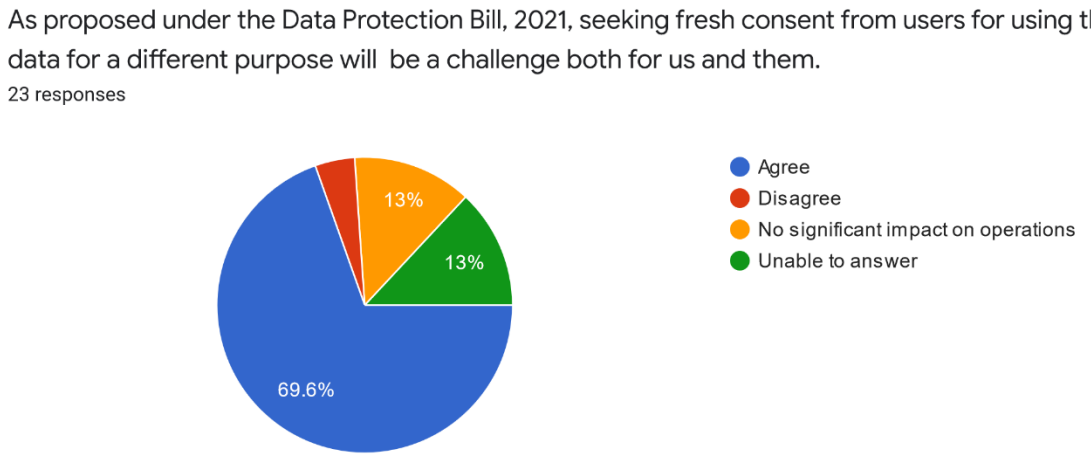
The Data Protection Bill, 2021 has clauses for consent that data fiduciaries need to obtain from data principals. When asked about the adverse impact of the consent mechanism on business, nearly half of the start-ups (47.8%) responded that the proposed consent mechanism will adversely affect their business. 13% of firms disagreed with the statement that the consent mechanism would adversely affect their operations. 26.1% felt that there would be no significant impact either way while 13% were unable to answer the question.

Purpose limitation as mentioned in the Data Protection Bill, 2021 will adversely impact monetizing users' data.

23 responses

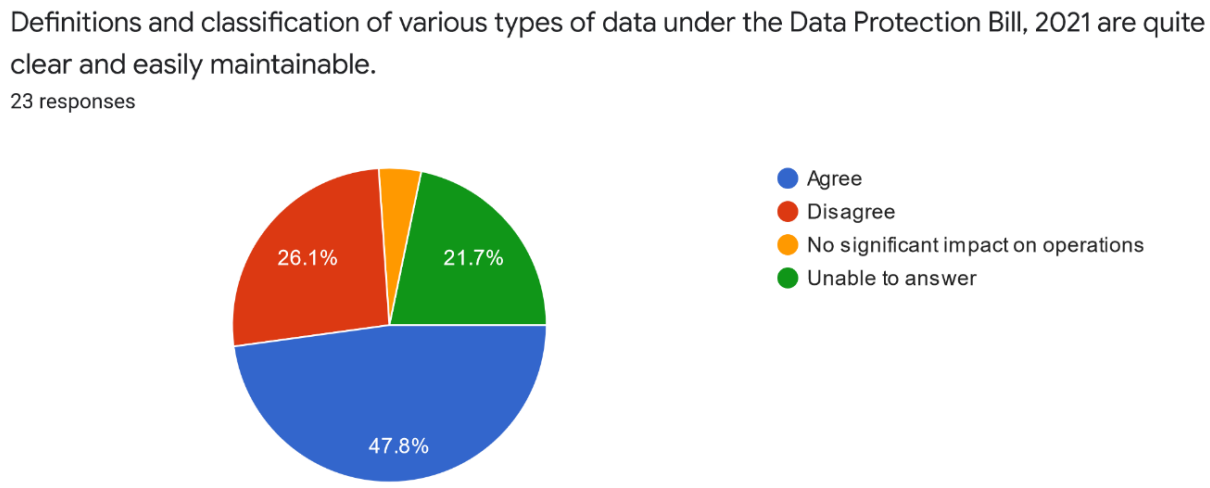


The Bill restricts the use of personal data to only those purposes for which explicit consent has been sought from the user while collecting the data. Also, there are restrictions on processing of personal data by a third party. As discussed in previous sections, these can all significantly affect start-ups. When we asked start-ups about adverse impact of purpose limitation on monetizing users' data, more than half agreed (52.2%), 17% disagreed with the statement, 17% felt that there would be no significant effect on their business and the remaining 13% were unable to answer.



When a start-up wants to use data for a different purpose, a fresh consent needs to be obtained. Earlier research studies – studying the impact of the GDPR in Europe - have found that getting consent for different purpose is very difficult even when users are paid. And, getting fresh consent without providing a new service has even lower response rates. This resonates with the findings of our survey. When asked about the challenge posed by seeking fresh consent for different purpose, overwhelmingly, 70% felt it would be difficult for them as well as for customers. And only 4% of the start-ups disagreed with the statement.

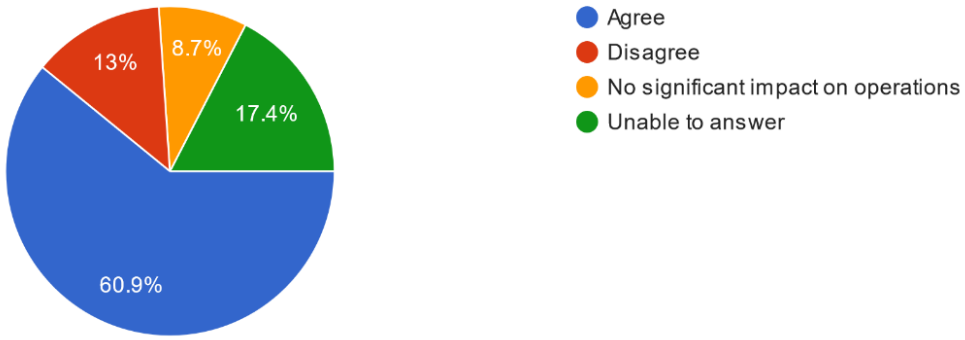
When start-ups were asked about clarity of definitions and classification of various data types in the DP Bill, there was a mixed response. Nearly half (47.8%) felt that the classifications were clear whereas 26.1% disagreed and 27.1% were not able to answer.



While the DP Bill deals mostly with personal data and doesn't layout any detailed provisions about non-personal data, it does bring NPD under the ambit of the Bill and the Data Protection Authority. When asked whether inclusion of non-personal data will help business or not. Most (61%) start-ups felt it would help their business.

Inclusion of non-personal data within the Data Protection Bill, 2021 will help our business

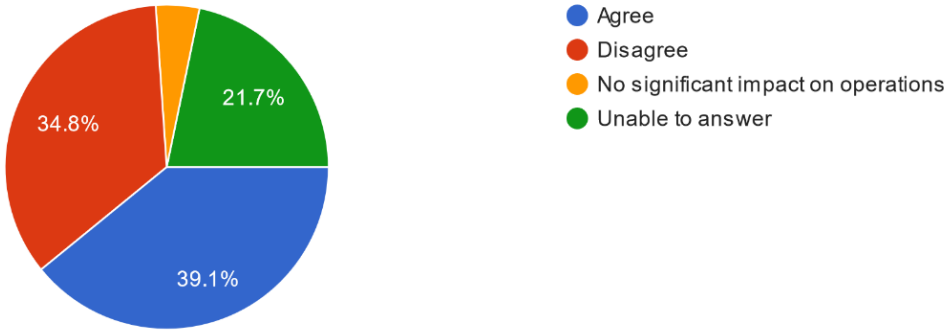
23 responses



The Data Protection Bill requires firms to store certain categories of personal data in India. Even if processing is done abroad, a copy of data needs to be stored in India for some categories. This may affect start-ups through increased compliance costs – storing and processing of data in India may not be cost effective. There was a mixed response from start-ups surveyed on the impact on business of relocating legacy data with 39% agreeing that this would be a significant challenge and 35% saying that it would not be.

Relocating legacy data (currently stored abroad) to India as required under the Data Protection Bill, 2021 is a major challenge for our business.

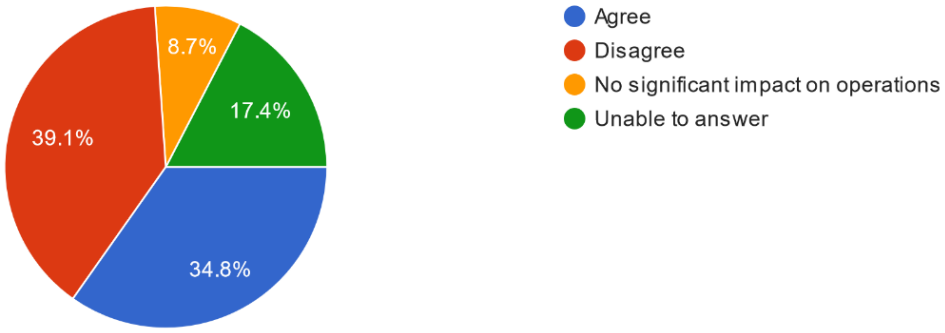
23 responses



When the regulation comes becomes an act, there may be increased costs of compliance and firms would need time and resources to manage. The response to the question of whether the start-up would be able to manage the cost of compliance was mixed with 35% saying that the costs will be easily managed and 40% disagreeing.

Costs of compliance with the provisions of the Data Protection Bill, 2021 will be easily managed by our company.

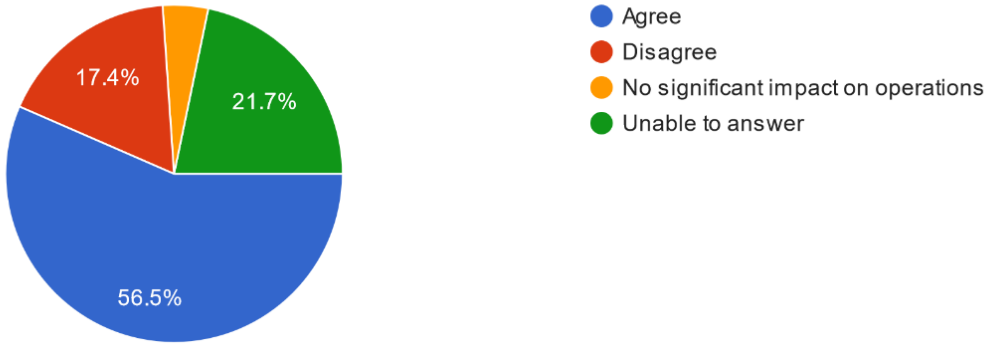
23 responses



Currently there is no standard format for collecting and storing personal data. The format differs from company to company, which makes it difficult for start-ups to use and for the users to know what data categories were collected by the company. The bill has provisions for standardisation of data and, further, requires data fiduciaries to provide data in a commonly read format. Data portability along with consent could reduce switching costs, which could benefit the start-ups. So, when asked start-ups on the impact of data portability on business, 57% responded that it would have a positive impact and 17% disagreed. And 22% were not able to answer.

Will the provision related to data portability have positive impact on your business

23 responses



Based on this sample of responses two main points emerge. The start-ups perceive that the impact of the DP Bill will be mixed

3. The issue of purpose limitation and seeking fresh consent from the users at a later point in time is the most vexing for start-ups. This should not be surprising given the discussion already presented in the previous section.
4. The inclusion of NPD and data-portability can increase the access of the start-ups to data that has already been collected. This may make up to some extent for increased cost of collecting new data. Start-ups overwhelmingly consider this to be a positive move.

7.0 Conclusion and recommendations

The objective of this study was to understand the possible impact of the DP Bill 2021 on start-ups in India. Both our theoretical analysis and the results of an online survey conducted by us suggest a mixed impact. Certain provisions will have a negative impact on start-ups' business models, imposing business process redesign costs on them. Some others – like the inclusion of the data portability provision may have positive impacts.

The online survey was designed to validate our theoretical analysis of the Bill. Based on the sample of responses two main points emerge. As discussed the start-ups perceive that the impact of the DP Bill will be mixed

1. The issue of purpose limitation and seeking fresh consent from the users at a later point in time is the most vexing for start-ups with almost 70% start-ups agreeing that seeking fresh consent will adversely impact their business operations.
2. The inclusion of Non- Personal Data (NPD) and data-portability may increase the access of start-ups to data. This may make up to some extent for increased cost of collecting new data. Start-ups consider this to be a positive move. About 60% of the respondents say that NPD inclusion and data portability will positively impact their business operations.

A final point about the impact of the Bill is in order. The costs imposed by the Bill are immediate. They will impact start-up activity and start-up entry as soon as the Bill becomes law. The benefits that start-ups may derive from having access to already collected datasets (NPD) and data portability will only be realised in time, once these proposals and how to implement them without hurting the incentives to generate data have been worked out. This feature – of immediate costs but later realisation of benefits - needs to be acknowledged while the design of the DP regulation is finalised.

The need for certainty in personal data regulation in India cannot be denied. At a more fundamental level, Indian society's desire to safeguard people's personal data and hence informational privacy online, as also expressed in the Supreme Court judgments, also demands a policy intervention. This report has attempted to understand the impact of the DP Bill 2021 on Indian start-ups. We find the affect to be mixed.

The question before us now is whether the consent framework, which can have significant negative impact on start-up activity, provide commensurate protection online to individuals? Or can we come up with a different form of regulation which improves on both – real safety online for India's population and less onerous on start-ups?

8.0 References

[1] https://www.startupindia.gov.in/content/sih/en/international/go-to-market-guide/indian-startup-ecosystem.html

[2] https://s3.amazonaws.com/document.issuu.com/210604105808-596456930d959ee95816ee83dc1c5fa2/original.file?AWSAccessKeyId=AKIATDDRE5J7VVA66JW6&Expires=1656480579&Signature=Gw3LMkTqiEDSQMsC%2Fjy6faaRWzY%3D

[3] Viscusi, W. K., Harrington Jr, J. E., & Sappington, D. E. (2018). Economics of regulation and antitrust. MIT press.

[4] Blind, K., Bührlen, B., Menrad, K., Hafner, S., Walz, R., & Kotz, C. (2004). New products and services: Analysis of Regulations shaping new markets. Fraunhofer Institute for Systems and Innovation Research, Karlsruhe.

[5] Blind, K. (2012). The influence of regulations on innovation: A quantitative assessment for OECD countries. *Research policy*, *41*(2), 391-400.

[6] Rennings, K., & Rammer, C. (2011). The impact of regulation-driven environmental innovation on innovation success and firm performance. *Industry and Innovation*, *18*(03), 255-283.

[7] PricewaterhouseCoopers (2018). Pulse survey: GDPR budgets top $10 million for 40% of surveyed companies.https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html

[8] Johnson, G., Shriver, S., and Goldberg, S. (2021). Privacy & market concentration: Intended & unintended consequences of the GDPR. Available at SSRN 3477686.

[9] Jia, J., Jin, G. Z., and Wagman, L. (2018). The short-run effects of GDPR on technology venture investment. Technical report, National Bureau of Economic Research.

[10] Martin N, Matt C, Niebel C, Blind K. How data protection regulation affects start-up innovation. Information systems frontiers. 2019 Dec;21(6):1307-24.

[11] Bessen, J. E., Impink, S. M., Reichensperger, L., and Seamans, R. (2020). GDPR and the importance of data to AI start-ups. NYU Stern School of Business.

[12] Nanda, R. (2016). Financing high-potential entrepreneurship. IZA World of Labor.05530

[13] Athey, S., & Luca, M. (2019). Economists (and Economics) in Tech Companies. Journal of Economic Perspectives, 33(1), 209-30

[14] Goldberg, S., Johnson, G., and Shriver, S. (2019). Regulating privacy online: An economic evaluation of the GDPR. Available at SSRN 3421731.

[15] Snelders, E., L. Worp, and S. Song (2020). A future without advertising cookies? It's possible! Technical report, Ster

[16] Susser, D. (2019). Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't. Journal of Information Policy, 9(1), 148-173.

[17] De Matos, M. G. and I. Adjerid (2019). Consumer behavior and firm targeting after GDPR: The case of a telecom provider in Europe. Working paper

About Centre for The Digital Future

Centre for The Digital Future (CDF) was launched on October 30, 2019 with a vision to conduct actionable research on the impact of digitisation on the economy and society. The inquiries are analytical, without any pre-determined bias, multi-dimensional and evidence-based, and provide policy and regulatory insights that enable the transition to an optimal digital economy and society.

The Centre has been established and incubated as an entity by the **India Development Foundation (IDF)**, a private non-profit research organisation set up as a Trust in 2003.

For more information, please visit https://cdfresearch.org or https://idfresearch.org.