White Paper

Centre for
The Digital Future

3P's of Data Protection Law

Principled - Permissive - Pragmatic

Deepak Maheshwari
Senior Fellow

July 2022

Executive Summary

Consent-centric framework proposed within the **Data Protection Bill, 2021** would place significant compliance burden on the data fiduciaries without commensurately enhancing digital privacy of individuals.

Instead, the proposed law for Data Protection in India must address ground realities of India, be principles-based, drive growth of the digital economy and foster innovation while ensuring digital privacy of individuals.

Accordingly, the following propositions should be duly considered and incorporated in the law:

1. ***A set of foundational principles must be enunciated within the law, equally applicable for all data fiduciaries including government entities and body corporates. This will enable courts to deal effectively with litigation where understanding the legislative intent is important.***

2. ***The law must factor in India's political economy and social context.***

3. ***The consent framework burdens the data principal with maintaining control over their data. There are good reasons to believe this will not result in any substantial improvements in privacy for users. Instead, data fiduciaries should be asked to comply with threshold privacy norms that are non-negotiable.***

    a. ***The norms can be evolved through public consultation, or by self-regulatory organisations or even through standards and indeed could be sector specific. The norms must:***
        i. ***Be clear, concise and easily comprehendible***
        ii. ***Be communicated in a transparent manner***
        iii. ***Clearly spell out accountability.***

    b. ***This approach is especially relevant for:***
        i. Providers of quintessential government services
        ii. Significant intermediaries
        iii. Systematically important entities
        iv. Pervasive deployment, often without a text screen; e.g. in Smart City.

4. ***Data fiduciaries must be mandated not to deny access to any service as long as a data principal agrees to provide certain minimum set of necessary data.***

5. ***The undertone of the law must be permissive, allowing innovation rather than restrictive via unreasonable restrictions on collection, retention or use of data.***

6. ***Purpose limiting collected data can significantly reduce experimentation and innovation in the digital economy.***

   An alternative could be to allow data fiduciaries to use personal data that they themselves have collected for any purpose without seeking fresh consent. However, they must still seek fresh consent before disclosing or sharing the same with a third party. Such restrictions on disclosure or sharing must extend to government agencies, not just to the private ones.

7. ***Exemptions from law must be carved out only for government agencies responsible for national security, intelligence, and law enforcement based on specific approvals as in the case of interception of telecommunications rather than at an agency-wide level. Such exemptions need to be subject to judicial or legislative oversight to mitigate potential abuse or misuse.***

8. ***The law must provide sufficient guidance to resolve extant or potential conflict across various laws, rules or regulations. These could be across central and state level; or, across data protection and sector-specific vertical ones.***

1. Introduction

Two years after the **Personal Data Protection Bill, 2019 (PDP Bill, 2019)**[1] was referred to the **Joint Parliamentary Committee (JPC)**[2], in December 2021 it recommended a revised draft of the proposed law in the form of **Data Protection Bill, 2021 (DP Bill, 2021)**[3].

Deletion of the prefix **'Personal'** in the title, however, is more than cosmetic. Amongst the wide swathe of recommendations, the most important and far-reaching is to include the **Non-Personal Data (NPD)**[4] within the ambit of the law.

Considering the ever-increasing role of data in all aspects of life, it is imperative to ensure that not only the data protection law has cogent objectives and priorities but enshrine within and align with a set of fundamental principles.

As per the preamble, the objectives of the proposed law include but are not limited to the following:

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

2. Scope of the White Paper

This white paper attempts to assess the **DP Bill, 2021** with respect to the adherence to a set of principles, albeit considering the perspective of practical considerations.

The objective of this whitepaper is to assess if, how and to what extent the **DP Bill, 2021** enshrines within and adheres to, a mutually exclusive yet collectively exhaustive set of inter-dependent principles and analyse impact thereof within the Indian context on the following dimensions:

a. **Privacy of individuals**, considering that privacy is a fundamental right within the Indian constitution.

---

[1] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
[2] http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1
[3] http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf
[4] Incidentally, another expert committee constituted by the government had recommended in December 2020 a separate regulatory framework for non-personal data (NPD), distinct from that for personal data (PD)

b. **Growth of the digital economy.** considering the rapid pace of digitisation and digitalisation across every aspect of society and economy.
c. **Innovation, especially by start-ups** considering emergence, proliferation, and adoption of innovations and growth of start-ups.
d. **Powers of the government by way of exceptions and exemptions**, considering that a set of checks and balances are necessary in a democracy like India.

3. The Indian Context

Any policy instrument like a law must be context-specific. It must factor in the political economy of the country as well as the social realities. At the same time, it must be based on what the country aspires for and how it plans to navigate that path.

India is full of diversity and paradoxes, challenges and opportunities. For example, there are 22 languages listed within the constitution, not even counting English, which are written in more than 10 scripts.

A significant proportion of the population is not yet functionally literate, leave aside being digitally literate or familiar with English, the language in which most privacy policies are published. Yet, even many an illiterate street vendors has adopted digital payments, relying on the voice notifications.

Role of start-ups has been and would continue to be seminal in this endeavour of offering innovative solutions that work within the Indian context and are scalable. Hence, the regulatory framework – including that for data protection, must ensure that the start-ups not only have a fair chance to survive but even thrive, while ensuring that the individuals' data is indeed protected.

The constitution of India has built-in checks and balances to ensure that none of the branches of the state behave in an arbitrary and unaccountable manner. However, there is still a need to be on the constant vigil to ensure that untrammelled power is not misused or even perceived to be prone to abuse.

4. Foundational Principles

In 2012, a group of experts chaired by **Justice AP Shah** had recommended a set of nine foundational principles for privacy law in India[5]. These are - **Notice; Choice and Consent; Collection Limitation; Purpose Limitation; Access and Correction; Disclosure of Information; Security; Openness; and Accountability**.

While specific terminology does vary somewhat and admittedly there are certain additions and omissions on the edges, these principles seem to enjoy universal support globally. Similar provisions are seen elsewhere too across frameworks and regulations as diverse as **Organisation for Economic Co-operation and Development (OECD) Privacy Framework[6], California Consumer**

[5] https://niti.gov.in/planningcommission.gov.in/docs/reports/genrep/rep_privacy.pdf
[6] OECD Privacy Guidelines of 1980 were last updated in 2013 https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Protection Act (CCPA)[7], European Union's General Data Protection Regulation (GDPR)[8] and **Council of Europe's Convention 108+[9]**. Indeed, most of these principles were drawn from global best practices.

Last updated in April 2022, **Global Comprehensive Privacy Law Mapping Chart[10],** published by **The International Association of Privacy Professionals (IAPP)[11]** has a more granular analysis across four clusters - individual rights; business obligations; scope; and enforcement across 20 jurisdictions with UK and India being notable exceptions.

It would only be appropriate that a set of mutually exclusive yet collectively exhaustive set of guiding principles must be enunciated within the law. Moreover, these must be equally applicable for all data fiduciaries including government entities.

5. Impact of DP Bill, 2021 on Privacy of individuals

In 2017, the Supreme Court of India upheld privacy as fundamental right under the Constitution of India[12]. Considering that the primary objective of the proposed law is to protect digital privacy of individuals or the data principals, it is crucial to ensure that not only they are aware of their rights but also have the agency and opportunity, cognitive capacity and access to requisite resources and processes. In addition, there must be a speedy, effective, and affordable mechanism for breach or grievance redressal.

At the same time, due care and caution are warranted against provisions that deter usage of digital products and services or retard the innovation ecosystem that keeps churning out new offerings and solutions for the benefit of individuals.

The legislative intent seems to empower the data principals with agency over their personal data through its lifecycle, primarily through an elaborate yet rather complex consent framework. However, to exercise such agency one must have the ability to understand and appreciate the implications of providing the data in the first place and thereafter, a realistic probability of exercising that informed and dynamic consent where the data fiduciaries define, if not dictate, the terms.

Even when disagreeing with certain provisions within the privacy policy notified by a data fiduciary, it is well-nigh impossible for a data principal to even initiate a negotiation, leave alone concluding the same. Such asymmetric bargaining power of a data principal vis-à-vis a data fiduciary implies that in most situations, the choice with the data principal would be binary – either accept the terms offered almost blindly and use the product or the service, or else, just

[7] https://oag.ca.gov/privacy/ccpa
[8] https://gdpr.eu
[9] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
[10] https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf
[11] https://iapp.org
[12] https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

decline and be deprived of the very access and usage of the product or service on offer.

DP Bill, 2021 proposes that a fresh consent must be obtained by the data fiduciary every time the data has to be used for a purpose different from the purpose for which it was collected with consent in the first place.

If a data principal is inundated with detailed choices in terms of what type of data is being collected through lengthy notices by way of privacy policy or terms and conditions, it may prompt the data principal either to refrain from the service or succumb to 'accept all cookies / tracking' just to ride over the friction in the usage. In both cases, this may be an unintended but more importantly, undesirable consequence. Incidentally, both GDPR and CCPA allow use of data for adjacent purposes or for purposes that are not materially different from the original purpose for which the data was collected.

In any case, an 'informed consent' is a chimera[13] and in India, it is even more challenging on account of illiteracy, linguistic diversity, and inadequate digital literacy. Likewise, parental consent for use by their children may also be meaningless if the parents do not use or understand the service or service terms.

However, the challenge pertaining to consent is further exacerbated with vital, essential or crucial services without any pragmatic alternatives. This is often so with government services like Aadhaar, Income Tax, GSTN, MyGov and IRCTC. However, this may also extend to certain private sector activities and entities, for example, educational institutions and healthcare providers, as has been amply demonstrated during the Covid pandemic where one had to willy-nilly accept the terms offered by the respective providers with no meaningful choice.

Clearly, over-reliance on a framework construct centred around consent is impractical and cumbersome. Hence, rather than placing overt and unnecessary burden on the data principal through the proposed consent framework, alternative approaches must be explored.

These could include commitment to comply with threshold privacy norms by the data fiduciaries through clear, concise and comprehendible communication in a transparent manner, coupled with accountability to comply by the same. Such norms could be evolved either through public dialogue or via a self-regulatory organization or even through standards.

In addition, data fiduciaries must be mandated not to deny access to their offerings as long as a data principal agrees to provide certain minimum set of data that is absolutely necessary and sufficient for provision of the said service[14].

[13] https://www.livemint.com/opinion/columns/can-data-protection-framework-uphold-an-individual-s-right-to-privacy-11648399118667.html

[14] Admittedly, clause 11 (4) states that the provision of the service shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

Such provisions must apply to quintessential government services such as taxation and law enforcement as well as to significant intermediaries and systemically important entities as determined under the extant laws, rules or regulations.

6. Impact of DP Bill, 2021 on Digital Economy

It is clear that reasonable, proportionate and pragmatic data protection norms would foster and sustain trust amongst all the stakeholders within the digital ecosystem. From this perspective, data protection legislation is expected to have a positive impact as it would encourage data fiduciaries to self-discipline their behaviours, foster innovation and provide assurance to data principals to beneficially use digital products and services with confidence, knowing that they have recourse to institutional safeguards and effective grievance redressal mechanism provided within and by the law in case they suffer from harm by way of irresponsible or illegal collection, storage, processing, disclosure or use of their data.

All the same, it is important to appreciate that no two products or services are perfect substitutes of each other and there is always some differentiation. Accordingly, what is 'necessary' data for two services may and would likely differ even if these may have similar functionality.

For example, WhatsApp, Signal and Telegram are the three most popular instant messaging services on mobile phones. These three messaging services differentiate from one another notwithstanding their seemingly similar functionality. Telegram may offer more features than the average messenger, Signal scores well on security while WhatsApp has the largest user base[15] This is why some users use two of these or even all the three while some may choose none of these or even no such service at all.

Obviously, placing unreasonable restrictions on data collection would severely restrict the ability of data fiduciary to innovate and differentiate. Worse, it would deprive the data principals and the economy at large from benefitting from such innovations.

Hence, the proposal to mandate data fiduciaries to offer notice, choice and consent as well as strict limitations on data collection and purpose for which it may be used, can be counter-productive. Moreover, seeking fresh consent for using data for any other purpose different and distinct from the original one is both unnecessary and undesirable. As a result of such boundaries, the data principals may also be worse off, having been deprived from innovative offerings with immense benefits. Likewise, publishing 'privacy by design' policy may lead to additional burden on the data fiduciary but also create unnecessary friction for the data principals.

The real challenge is to ascertain what data is 'necessary' for the specified 'purpose(s)'. In fact, data fiduciaries may not even envisage, leave aside know what all data they might need and for what purpose. This is particularly true for start-ups.

[15] https://beebom.com/whatsapp-vs-telegram-vs-signal/

For example, digital payments do not necessarily need location data of the data payer. However, by tracking the location of the device from where a particular payment is initiated, the payment operators and networks detect any anomaly or unusual pattern, they may alert the payer, the partners or even the regulators about potential fraud or illegal transactions.

The idea of 'right to erasure' is rather utopian and also bereft of similarity in the physical world. If one walks into a retail store and does not buy anything, the store may still record the person's movement, time of entry and exit, and even facial biometrics, if only for the purpose of security. However, it may notice that the person scanned products and prices on a particular shelf. The store may also record data on items which the shopper picked up and returned, or even use eye-tracking technology to determine which items caught the eye of the shopper, or items the shopper looked at for some time but did not ultimately pick up. Such data can be used to determine consumer shopping behavior, provide targeted incentives, optimize for placement of goods and inventory. Presumably, all this would be happening without any explicit consent *per se*. It is also noteworthy that in the real world, even if X agrees not to disclose certain information about Y, it does not by itself imply that such information has been permanently erased from X's own memory and that X would not be able to use the same.

It is worth thinking about whether such data collection should be considered as "necessary" for the purpose of shopping by a consumer. In a digital environment, an e-commerce platform or a travel booking site might be collecting data likewise in terms of visitor's IP address, device, Operating System, browser, location, etc. However, these could be used to enhance user experience through suitable rendering of the webpage or layout of a particular step in the respective app or even to suggest possible options via helpful suggestions.

In case a batch of data sets is being lawfully processed either internally or by one or more third-parties, withdrawal of consent may require halting of such operations midway and starting afresh. This may become impractical *ipso facto* and undesirable overall. There could also be a situation where data fiduciary 'A' may stop processing data after the consent given to it has been withdrawn, but processing of data by 'B' may continue to whom such data may have been lawfully disclosed by 'A'. It is also plausible that a data fiduciary may create a shell / front entity and disclose data to the same and the latter may continue to process the data even after the consent has been withdrawn.

Proposed regulatory restrictions on collection, purpose and retention may also at times conflict with other extant requirements. For example, VPN service providers don not retain customer logs and most cloud service providers collect minimum personally identifiable information (PII) pertaining to their customers. One of the propositions of a VPN service is to proffer anonymity and confidentiality while in case of cloud service providers it is often an issue of convenience but also the realization that they need not collect such personally identifiable information (PII) in the first place. These are conscious choices to minimize data collection may come in conflict with the April 2022 directions issued by the Indian Computer Emergency Response Team (CERT-In is a

statutory authority under the Information Technology Act, 2000) mandating retention of VPN customer logs for five years and extended KYC validation of cloud computing customers[16]. Commenting on the merits of direction issued by CERT-In is beyond the scope of this paper but sometimes, such limits or mandates on data collection may not be practicable.

All the same, certain practices and instances of data collection may be totally unnecessary *ab initio*. For example, Indian Railway Catering and Tourism Corporation (IRCTC), a public sector unit under the Ministry of Railways, asks the registrant to declare whether one is 'married' or 'unmarried' at the time of creating login credentials. Incidentally, such information is not sought when one fills up a physical paper form at the railway reservation counters. Likewise, it may be unnecessary for a flashlight app on the mobile to have access to the location, address book or text messages.

It is easier said than done to make withdrawal of consent as easy as providing the consent in the first. place. As an analogy, it is easier and faster to deposit cash at a bank branch than to withdraw the same.

Reasonable security practices commensurate with the type of activity and personal data are necessary to instill trust amongst users. However, adoption of specific standards mandated under specific regulations under the **DP Bill 2021** may lead to over-burdening data fiduciaries.

In 2017, Zomato disclosed that personal data of 17 million users was leaked in a security breach that had begun in 2015[17]. It turned out that the company was hashing passwords using MD-5, a rather obsolete encryption algorithm. Secondly, it had not even deployed two-factor authentication that provides greater protection against fraudulent transactions using the personal data disclosed even as it does little to directly mitigate privacy concerns. On the other hand, with time any encryption methodology may become obsolete and hence, newer methods or algorithms may be needed.

Rather than mandating use of a particular encryption, in such a case the regulator should focus on the resultant harms and potential risks from poor data security. The reason is that while certain encryption method could be better than others, it also can be compromised and may lose its potency over time with increasing computing prowess that allows brute-forcing and other workarounds. Moreover, it is not just about the technology itself but also about the people and processes. For example, sharing of decryption key with unauthorized personnel would make even the strongest and the most complex encryption mechanism ineffective just like the duplicate key of a strong physical lock.

Accordingly, the following steps should be considered.

A data fiduciary may be allowed to use personal data for any legitimate without seeking fresh consent of the data principal. However, fresh consent must be sought before disclosure or sharing of the same with a third party.

[16] https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[17] https://www.zomato.com/blog/security-update-what-really-happened-and-what

Application of right to erasure must be extremely narrowly crafted, for example, to cull out the menace of child pornography.

The law must also provide sufficient guidance in terms of applicable hierarchy for decision-making in case there is obvious conflict across various laws, rules or regulations whether central or state or across horizontal laws like data protection and norms for the respective vertical sectors, usually through sector-specific regulators.

7. Impact of DP Bill, 2021 on Innovation by Start-ups

Most of the innovations in the digital space originate within or from the start-ups who take a different approach to problem solving or address an entirely new problem or new segment of users. True, most of the start-ups fail and many are often acquired by the so-called Big Tech companies.

However, many of the conditions described in the previous section can be debilitating for the start-ups. Not only such requirements may retard the formation of new start-ups these also may chill the innovation ecosystem. On the other hand, heavy compliances may lead to extremely high entry barriers raising the spectre of challenges on account of severely restricted competition as well.

As described in the previous section, mandating specific technologies can also place undesirable burden on data fiduciaries, especially the start-ups.

In the early phase, a start-up might focus on solving a particular problem and consider monetization options only later. It is also possible that the startup may pivot to or add a new line of business, a new business model, or even a new use case. In several cases, an individual Y's personal data may be provided by another individual X and in such situations, notifying and obtaining consent from Y would be well, nigh impossible.

Truecaller[18] is a good example for both such situations. A subscriber X may allow access to its contact list on mobile that contains X's phone number and name, even an alias. In the process, another individual Y's personal data are also shared with Truecaller even as Y oneself has not given explicit consent to Truecaller for such collection. However, without processing X's personal data, a crowd-sourced caller ID service like Truecaller just cannot function. Similar would be the case with services like Ancestry[19] that help people construct family trees and trace their lineage.

Within India, One 97 Communications began as a provider of Value Added Services (VAS) and later pivoted to mobile payments under the brand Paytm. Still later, it diversified into E-Commerce with Paytm mall. Obviously, the data that they would have collected as VAS provider would have been likely used also for subsequent offerings.

[18] https://www.truecaller.com
[19] https://www.ancestry.com

Incidentally, notwithstanding the specific authorizations under which a Law Enforcement Agency (LEA) may intercept communication of a particular target A they would inadvertently invade privacy of B to the extent that they may communicate with A. In such a situation, privacy of B is breached even when there is no specific authorization to intercept communication of B *per se.*

Mergers, acquisitions, and other forms of combinations and partnerships are par for the course across the start-up ecosystem. Such transactions can suffer significant uncertainty, friction or delay if there are severe restrictions on using the data for another purpose by the entity that collects it.

As explained in the preceding section, unreasonable restrictions on collection, retention, use and reuse of personal data by an entity through the elaborate consent framework can severely retard and disincentivize innovations. Moreover, it may not provide any commensurate benefit to the data principals in terms of privacy or data protection.

All the same, it seems reasonable to mandate seeking fresh consent before disclosing or sharing data with a third party.

8. Impact of Powers with the Government for Exceptions and Exemptions

Having been upheld by the Supreme Court of India as a fundamental right under the Constitution of India, privacy is first and foremost justiciable against incursions by the state. Any invasion of privacy by the state must pass the triple test of:

a. Legality (existence of statutory law)
b. Legitimate State aim or necessity
c. Proportionality (rational nexus between the objects and the means adopted to achieve them)

A government agency collects data from individuals essentially in two different ways, mandatory and voluntary.

Firstly, a government agency can use the statutory powers vested with itself to mandate that individuals are duty bound to provide certain type of data, e.g., under the Census Act. There are consequences in case one fails to provide the requisite data and an individual has the legitimate expectation that such data would be used for specific purpose and shall not be shared with any third party, even another government entity. Though aggregate reports are published, even unit-level data is not.

Secondly, a government agency can seek data on voluntary basis. For example, one has the agency to choose out of volition not to participate in a survey by the National Sample Survey Office (NSSO). However, if one does participate, NSSO can share even unit-level data with researchers, albeit after masking the individual identity. Such data can also be used more broadly.

It is noteworthy that data protection laws such in most of the mature democracies do not discriminate between the obligations between a government entity and a private entity. Rather than treating the whole of government as a

monolithic entity, each government entity needs fresh consent before sharing personal data with another one under EU GDPR and such like.

In fact, Ireland's Data Protection Commission (DPC) recommends that all data sharing arrangements within the public sector should generally[20]:

- Have a basis in primary legislation;
- Have a clear justification for each data sharing activity;
- Make clear to individuals that their data may be shared and for what purpose;
- Be proportionate in terms of their application and the objective(s) to be achieved;
- Share the minimum amount of data to achieve the stated public service objective;
- Have strict access and security controls; and
- Ensure secure disposal of shared data.

However, data may be shared across the government agencies in India with few restrictions. For example, in 2020 the government formally allowed income tax authorities to share data with Goods and Services Tax Network (GSTN), the company (a body corporate) that processes Goods and Services Tax (GST) returns[21]. Similar concerns have been raised in the realm of sharing data using the digital health ID under the National Digital Health Mission[22].

Against this backdrop, there are two specific provisions of the **DP Bill, 2021** that warrant closer scrutiny and analysis with respect to the powers proposed to be vested with the government.

Firstly, the clause 12 (b) obviates the need to seek consent of the data principal for carrying out any function authorized by any central or state law. Without any checks and balances in terms of interpretation, such unbridled power is prone to misuse. Even when such cases may ultimately may not be maintainable, the long-drawn and arduous process itself becomes the punishment. One way to mitigate misuse could be to replace the word 'including' with 'only' in the clause 12 (a).

Secondly, Clause 35 (ii) empowers the central government to exempt any agency of the government engaged in processing of personal data from any or all the provisions of the proposed law. The grounds for the same includes but are not limited to "security of the state", a ground that has been often interpreted extraordinarily widely.

Even more troublesome aspect of this provision is that any agency can be exempted. This goes against the principle that the exceptions / exemptions under any laws for interception are case and context specific and it is not befitting to grant blanket exemption(s) to any agency.

---

[20] https://www.dataprotection.ie/sites/default/files/uploads/2019-05/190418%20Guidance%20on%20Data%20Sharing%20in%20the%20Public%20Sector.pdf

[21] The purported purpose is to enhance scrutiny and checking tax evasion https://www.livemint.com/politics/policy/i-t-dept-to-soon-share-turnover-itr-data-of-biz-with-gstn-1556635028370.html

[22] https://www.reuters.com/article/india-health-tech-idUKL8N2G536U

After all, in a democratic set-up, no agency can or should be granted an unfettered "License to Kill" or similar powers without adequate checks and balances in terms of accountability and transparency notwithstanding such depiction in the James Bond franchise.

Hence, exemptions must be carved out only for agencies responsible for national security, intelligence, and law enforcement. In addition, there must be an effective and accountable oversight mechanism to mitigate potential abuse or misuse. In fact, the government should become the exemplar role model in the realm of data protection for private sector to emulate.

9. Summary of Recommendations

Underlying philosophy of the data protection law must be permissive rather than restrictive. While ensuring protection of personal data, it should allow its usage to foster innovation.

For example, road accidents can be totally obviated if nobody drives or walks on the road, or if there were no roads at all but that may not be desirable at all. Instead, we need are rules of the road that are understood and followed by drivers and pedestrians alike, safety standards, reasonably good road infrastructure, lanes and traffic lights; and, yes, enforcement mechanism to deal with violations.

Likewise, data protection norms should be reasonable and proportionate to the risks posed. Accordingly, the following propositions are worth consideration, deliberation and incorporation in the DP Bill, 2021.

1. ***A set of foundational principles must be enunciated within the law, equally applicable for all data fiduciaries including government entities and body corporates. This will enable courts to deal effectively with litigation where understanding the legislative intent is important.***

2. ***The law must factor in India's political economy and social context.***

3. ***The consent framework burdens the data principal with maintaining control over their data. There are good reasons to believe this will not result in any substantial improvements in privacy for users. Instead, data fiduciaries should be asked to comply with threshold privacy norms that are non-negotiable.***

    a. ***The norms can be evolved through public consultation, or by self-regulatory organisations or even through standards and indeed could be sector specific. The norms must:***
        i. ***Be clear, concise and easily comprehendible;***
        ii. ***Be communicated in a transparent manner; and,***
        iii. ***Clearly spell out accountability***

    b. ***This approach is especially relevant for:***
        i. ***Providers of quintessential government service***

ii. ***Significant intermediaries***
iii. ***Systematically important entities***
iv. ***Pervasive deployment, often without a text screen; e.g. in a Smart City scenario***

4. ***Data fiduciaries must be mandated not to deny access to any service as long as a data principal agrees to provide certain minimum set of necessary data.***

5. ***The undertone of the law must be permissive, allowing innovation rather than restrictive via unreasonable restrictions on collection, retention or use of data.***

6. ***Purpose limiting collected data can significantly reduce experimentation and innovation in the digital economy.***

   An alternative could be to allow data fiduciaries to use personal data that they themselves have collected for any purpose without seeking fresh consent. However, they must still seek fresh consent before disclosing or sharing the same with a third party. Such restrictions on disclosure or sharing must extend to government agencies, not just to the private ones.

7. ***Exemptions from law must be carved out only for government agencies responsible for national security, intelligence, and law enforcement based on specific approvals as in the case of interception of telecommunications rather than at an agency-wide level. Such exemptions need to be subject to judicial or legislative oversight to mitigate potential abuse or misuse.***

8. ***The law must provide sufficient guidance to resolve extant or potential conflict across various laws, rules or regulations. These could be across central and state level; or, across data protection and sector-specific vertical ones.***

10. The Way Forward

While being protective of the personal data, the proposed legal framework must be principled, permissive, and pragmatic, within the Indian context. Hence, the **Data Protection Bill, 2021** must be revisited for a thorough review leading to requisite revision. The objective must be to improve, improvise and strengthen the institutional framework for ensuring privacy of individuals while also fostering innovation and growth of digital economy[23].

23 https://cdfresearch.org/uploads/projects/1649929821_Legal%20Framework%20for%20Privacy%20in%20India%20-%20Revisit%20-%20Reframe%20-%20Revise.pdf

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.