Comments on the draft Digital Data Protection Bill, 2022

Urvashi Aneja Rishab Bailey Aman Nair K Shashidhar
Karthik Suresh*

2 January 2023

Abstract

On 18 November 2022 the Ministry of Electronics and Information Technology published a draft Digital Data Protection Bill, 2022, for public comments.

In our response to the Ministry, we point that many of the safeguards based on the concepts of necessity and proportionality that were laid down by the Supreme Court in the Puttaswamy decision have, in practice, been diluted or removed from this draft Bill. The grounds for processing personal data have been widened, the concept of "deemed consent" has been used to expand on the exceptions from consent, and the state and its instrumentalities have been granted broad and far-reaching exemptions from complying with the draft Bill. The age of consent should be re-framed to prevent onerous compliance. The draft Bill is also overly prescriptive and it takes many ex-ante functions away from the ambit of the Data Protection Board of India.

JEL Codes: H11, H80, L86, O38

*Urvashi Aneja is the Executive Director of Digital Futures Lab. Aman Nair and K Shashidhar are Research Associates with Digital Futures Lab. Rishab Bailey is a Visiting Research Fellow with XKDR Forum. Karthik Suresh is a Research Associate with XKDR Forum. All views are personal.

Contents

1 Preliminary

1.1 Chapter as a whole

The preamble of the Personal Data Protection Bill, 2019 (PDP, 2019) stated that its objective was to protect the privacy of individuals in a manner rooted in a rights-based approach. However, the current Bill seeks to focus on the *right of individuals to protect themselves* rather than an institutional-level approach to privacy. This change of tone is concerning since it disregards the principles that have been already identified in India in the field of the right to privacy.

1.2 Definitions

The concept of "sensitive personal data" has been excluded from the Bill. While sensitivity depends more on the context rather than the type of data, there should nevertheless be some regulations specific to sensitive personal data with the consequence of stricter requirements.The identification of sensitive personal data should be based on the expectations of likely harm that may arise in case of a breach. While the Bill uses the term "personal data" to convey all data which an individual is identified by or in relation with, the term "sensitive" connotes a higher duty of care. The scope of a higher duty of care has been removed in this Bill. Removing this higher standard of care will mean that data fiduciaries would not treat sensitive personal data (especially biometric information) with stricter standards of security from less-valuable personal data. The misuse of sensitive personal data has the potential for more harmful consequences for the data principal than non-sensitive personal data.

The definition of "harm" is exclusive to four types of harm i.e., bodily harm, distortion/theft of identity, harassment, and prevention of gain/ causation of loss. Many other important forms of harm such as loss of confidentiality, the possibility of psychological manipulation (e.g., "dark patterns"), unlawful surveillance, restrictions on speech, loss of goodwill/reputation etc. have not been covered. It also does not cover non-quantifiable harm. For a concept like harm, an inclusive definition is necessary. We suggest that a risk-based approach be adopted towards defining harm. All harms that arise out of privacy violations should be covered – including harms arising out of unauthorized state access. For example, a distinction could be drawn between reversible and irreversible harm, etc.

The definition of "children" should also be amended – the Srikrishna Committee had noted that the age of 18 was "too high". Article 5 of the UN Convention on the Rights of the Child requires parties (which includes India) to provide appropriate guidance for parental consent *in a manner consistent with the evolving capacities of the child.* A graded list of age-appropriate content could be created with carve-outs allowed for specific purposes. Even within the Indian context, laws like the Juvenile Justice Act, 2000 already lower the age of consent to 16 in most cases.

'Anonymisation' has not been defined. A risk-based framework should guide the rules on data anonymisation.

1.3 Application of the act

Clause 4 of this Bill draws a distinction between digitised and non-digitised forms of data. It is unclear why the law is restricting itself to consent taken for processing non-digitised offline data. For such data, no safeguards are in place. Further, the term "digitised" has not been defined anywhere. This could lead to uncertainty on applicability. For example, if an agency conducts a house-to-house market survey by collecting data on pen and paper, then "digitize" their findings by entering data on a local Microsoft Excel file, and only later publish "online" a portion of their findings. It is unclear when and where the Bill's provisions apply in such a case. We suggest that the Bill should cover offline processing of data as well as non-digitised collection. The scope of the Bill could be limited to avoid onerous compliance requirements but such limitations should be *purpose*-based and not *form*-based.

2 Obligations of a data fiduciary

2.1 Chapter as a whole

Data fiduciaries should incorporate privacy-by-design principles in their systems while collecting and processing personal data. However, not only does this Bill omit privacy by design requirements, but also removes principles like purpose limitation, data minimisation and storage limitation from its ambit. This is concerning because, rather than envisaging institutional systems to protect privacy, it reduces the responsibilities of the data fiduciary. We strongly suggest that the principles of purpose limitation, privacy-by-design and data minimisation be hard-coded into future versions of this Bill.

The grounds for processing personal data are poorly-defined and the scope of personal data collection is capable of being grossly expanded through the Deemed Consent clauses.

The Deemed Consent clauses expand the scope for data collection which is not proportional and necessary and will appropriate citizens' personal data. The larger concern for data collected through the Deemed Consent clauses is that data principals will not have a clear way of recourse as data fiduciaries are not required to give notice to them. Another serious lapse is that this Bill does not give guidance on how data fiduciaries need to give notice to data principals who have already processed data or provide options to opt out from the services of a data fiduciary.

2.2 Grounds for processing digital personal data

This Bill defines "lawful purpose" as any purpose which is not expressly forbidden by law. This phrase has a very broad meaning and the scope of processing should be defined more clearly.

2.3 Notice

The purpose of an effective notice is to operationalise effective consent that is free, specific, informed and unambiguous. However, under the current provisions, there are no details on

what the notice should contain. Some details that the notice should contain are: (i) specific information on the third party data processors, (ii) duration for which the data is retained by the data fiduciary, (iii) details of the data protection officer, (iv) details on how to withdraw consent, etc. There should also be some protection against a unilateral amendment of notice by the data fiduciary e.g. requiring fresh consent with a specific description of the change from the previous notice.

2.4 Consent

The parameters of consent should be better defined – purpose and storage limitation should be defined clearly.

Clause 7(5) pertains to how data fiduciaries must stop processing personal data of a principal when they have withdrawn consent "within a reasonable time" unless processing without the data principal's consent is required or authorised under the provisions of any other law. Templates for withdrawal of consent notices from other jurisdictions like the European Union's GDPR and Singapore's Personal Data Protection Act stress on inclusion of the time period within which a data principal's withdrawal of consent will take effect. Given this context, this Bill should clarify what is considered a reasonable time. Further, data principals should also be given notice if the withdrawal of consent is denied with sufficient explanation for the denial.

Clause 7(7) states that a consent manager will be a data fiduciary that will act on behalf of the data principal and be registered with the data protection board. It adds that it will be subject to "technical, operational, financial and other conditions as may be prescribed." Consent managers are a relatively new concept and the nature of how they will be operationalised is unclear. There should be greater detail given on their role and the standards they are required to follow especially when they are handling sensitive information.

2.5 Deemed consent

The term "deemed" has not been defined. Exemptions from consent have been defined clearly in previous iterations of data privacy bills which have been significantly expanded through this clause. The clause also does not have safeguards and does not carry the qualifiers of necessity and proportionality as laid down in the Supreme Court's decision in *Puttaswamy*.

The requirement of providing notice is absent from the provisions on deemed consent. This may be valid for situations like medical emergencies and epidemics but not for the performance of functions like the issuance of certificates/ licenses by the State.

The definition of the term 'public interest' has no bearing on many of the sub-clauses included in clause 8(8) of the Bill. In other words, the relationship between issues of sovereignty and integrity of India, security, maintenance of foreign relations, public order and dissemination of false statements of fact – and issues like credit scoring, debt recovery and corporate restructuring transactions – has not been given clearly.

There is a clear need to identify limits to what kind of data processing can be done by data

fiduciaries through their use of deemed consent. For example, the Bill's framing of clause 8(2) as having the data principal deem consent for "*for the performance of any function under any law*" is very broad. The clause should carry the twin tests of necessity and proportionality.

The bill must also stipulate notice be provided in a reasonable time to data principals when data is collected or processed under the conditions of deemed consent. At present, there is no provision to ensure that the user is retroactively informed that they have provided consent and no procedure for a person to withdraw their consent in cases where consent was deemed to have been provided.

Processing of "publicly available personal data" under clause 8(8)(f) should be qualified because many people may have shared personal data that would have been protected by consent-dependent processing had there been a data privacy law from an earlier date.

The state has the power to include additional grounds under clause 8(9). However, this clause is not drafted to convey clarity and leaves room for a lot of ambiguity.

We suggest a redrafting of the entire clause on deemed consent to introduce requirements of proportionality, necessity and clear notice procedures. Only data shared voluntarily by the data principal and data shared under a procedure established by law should be exempt from prior notice and consent. Even with these two exemptions, the tests of necessity and proportionality of collection and usage of data must apply.

2.6 General obligations of data fiduciary

The obligations under this clause are vague and unclear. To begin with, there is no principles-based approach to these obligations. The concept of privacy-by-design, which could have been hard-coded into clause 9(3), is not included.

There should have been a principles-based approach to the data fiduciary's obligations. For example, it should have been mentioned that the processing of data should be fair in such a way that it does not cause harm to the data principal even after they gave consent.

Clause 9(6) of the bill describes the ability of the data fiduciary to retain data that is no longer being utilised for its intended purpose provided that there exists a necessary legal or business purpose. While legal obligations to retain data in specific cases can be clearly identified and outlined, determining whether or not a data fiduciary possesses a necessary "business interest" is a far more difficult and amorphous question to answer.

Clause 9(7) requires the appointment of a data protection officer "where applicable". But clause 11(2) requires only significant data fiduciaries to appoint a data protection officer. This inconsistency in compliance requirements should be clarified.

The clause is also silent on when and how data should be anonymised. The Bill in its current form does not provide for any rule-making powers on anonymisation.

Clause 9 also does not carry the language of transparency and accountability e.g., periodic assessments and audits, privacy scoring etc. There are no requirements for disclosure of the data fiduciary's privacy policies in this clause. There are also no details on the quality of

safeguards that the data fiduciary should adopt e.g., proportionality to the risks involved in the data being processed, etc. We suggest that these be added based on previous iterations of data privacy bills in India.

2.7 Additional obligations in relation to the processing of personal data of children

Clause 10 of the Bill outlines the obligations of data fiduciaries with respect to children, which includes a requirement to obtain parental (or lawful guardian) consent, abstaining from tracking and targeted advertising of children, and avoiding data processing that could harm a child. The clear logical conclusion of such a provision is that data fiduciaries will be required to undertake age verification through a KYC process. These provisions raise serious concerns over access to the internet for children. Firstly, the widespread adoption of a KYC procedure would functionally exclude all those children without verifiable proof of age. Secondly, the mandating of blanket consent requirements from parents or guardians could have severely negative effects on a child's access to information and could curtail their right to education and freedom. For example, a child may be unable to access information regarding topics such as menstruation or sexuality due to their parent's decision to withhold consent. Further, the requirement for parental consent and age verification can also encourage increased surveillance of a child's online activities by their parents; in direct violation of their privacy rights.

2.8 Additional obligations of Significant Data Fiduciary

Significant Data Fiduciaries have been defined as those who are selected on the basis of factors such as "potential impact on the sovereignty and integrity of India", "risk to electoral democracy", "security of the State", and "public order".

Across the world, while there are regulations which impose additional obligations on significant data fiduciaries, these are based on the size, function and number of users handled by that data fiduciary. The factors mentioned in the Bill have no bearing on data protection at all. Moreover, they are unhelpful for a firm to reasonably predict whether it may be chosen to follow an increased set of obligations. Further, it is unclear why the government has to *designate* any individual firm as a significant data fiduciary. The concern is that this process could be used arbitrarily. The government has not published any of its rationales in the past as to the selection of specific firms for heightened obligations.

We have already seen that the ministry choosing individual firms for heightened obligations has failed the purpose for which they were created. Section 70 of the Information Technology Act, 2000 (IT Act, 2000) allows the Union and state governments to choose specific firms operating critical information infrastructure to be "protected systems". Only five firms were chosen, only some and not all firms in a specific sector were chosen, and the firms and systems chosen were not even the largest or most vulnerable in their respective sector. The outcome is that a large set of firms operating critical information infrastructure did not fall under the ambit of NCIIPC's directions.

We suggest that objective criteria based on factors such as the number of users, functions served, etc. be chosen to categorise a firm as a significant data fiduciary.

3 Rights and duties of a data principal

3.1 Right to information about personal data

Clause 12(3) notes that data principals will have the right to obtain data relating to "the identities of all the Data Fiduciaries with whom the personal data has been shared." It is unclear why this clause does not also include the right for data principals to be made aware of the data processors with whom their data is shared. Given the bill's provisions legitimising the transmission of data between data fiduciaries and processors, and even data transfers between two or more data processors, the current framing would leave the data principal unaware as to exactly which entities had access to their data. We suggest that this clause be extended to include information about data processors.

3.2 Right to correction and erasure of personal data

Two major omissions in this Bill are the "right to be forgotten" and the "right to data portability". The "right to be forgotten" refers to the scope of the right to seek discontinuation of the processing of personal data. Clause 13(2) of this Bill restricts the right to be forgotten by adding an exception for "legal purpose". The phrase "legal purpose" has not been defined in the Bill which can lead to ambiguity and denial of requests to delete data. Only a court order should be able to restrict a data principal from having their data erased by the data fiduciary.

The omission of the right to data portability is a glaring error. Data portability allows data principals to move their data across different service providers which can reduce costs associated with switching providers and effectively create a "marketplace for privacy" where consumers can switch their services to data fiduciaries with more privacy-friendly policies. We suggest the inclusion of this right in broad terms in the Bill.

3.3 Right of grievance redressal

While the right of grievance redress has been mentioned in the clause, no effective method of enforcement has been suggested at all. The Bill should provide more details on how such a right would be operationalised, the form of complaints, etc.

3.4 Right to nominate

The form of the right to nominate should be specified. Whether such a nominee is nominated by a will, a court order, or under another arrangement recognized by family law should be clearly specified.

3.5 Duties of a data principal

The requirement of "under no circumstances ... furnish any false particulars" which attracts a fine of INR 10,000, is onerous and does not take into account the majority of cases where incorrect information is entered by mistake. It is a common occurrence that a person's name is entered incorrectly by some staff on an official document and a correction needs to be made. A provision that imposes costs on information that is not "verifiably authentic" attracts an onerous burden in a country with low levels of documentation. The phrase "verifiably authentic" is also not defined by this Bill. In any case, existing laws like IT Act, 2000 already cover cases of fraud and misrepresentation. We suggest that this provision be removed in its entirety.

4 Special provisions

4.1 Transfer of personal data outside of India

The Bill has not outlined the metrics by which the government can deem a foreign jurisdiction to be a trusted one. For example, the GDPR requires that in order for personal data to be transferred to a foreign jurisdiction, it must possess equivalent data protections to those present in the EU. Given the lack of any clarity on similar requirements in the Indian context, the personal data of citizens is converted into a tool of Indian foreign policy without any link with the levels of privacy being afforded to the data of Indians.

We suggest that the bill place clearly defined criteria against which the assessment conducted by the government can be measured. We suggest that a minimum requirement of 'equivalent data protection frameworks' be applied when assessing those states that can function as trusted nations.

4.2 Exemptions

The exemptions provided to the state and its instrumentalities under this clause (especially clause 18(2)) are disproportionate. The clause fails to account for the dicta of the Supreme Court in the *Puttaswamy* judgement by doing away with the requirements of necessity and proportionality. The absence of these protections raises concerns over the ability of the state to misuse personal data, including for purposes such as illegal surveillance. The government's blanket powers to exempt itself and its instrumentalities effectively allow it to not be subject to the entirety of this Bill. We suggest that clause 18(2) of the Bill be redrafted to expressly mention that requirements of legality, necessity and proportionality must be fulfilled in order for the government to exempt an entity from the provisions of this bill.

Clause 18(4) allows for the state and its instrumentalities to retain any data collected regardless of whether the purpose of such data collection or processing has been achieved. Such a broad exemption to the state defeats the purpose of the Bill to safeguard the privacy of people and gives rise to uncertainty.

The phrase "instrumentality of the state" has been used extensively in this Bill but has not

been defined at all. It comes from the Hon'ble Supreme Court's decision in *Ajay Hasia* v. *Khalid Mujib* AIR 1981 SC 487 where it said that the phrase "instrumentality of the state" refers to an entity which meets the following criteria:

1. The entity has the entire or a majority of its share capital or funding from the central or state government, or has *deep and pervasive state control*, or
2. The entity enjoys monopoly status conferred or protected by the government, or
3. The entity performs functions of public importance and is closely related to governmental functions.

The Court created this phrase to expand the ambit of Article 12 to cover entities which are not formally part of the state but are closely linked to it. The purpose was to enhance the accountability of "instrumentalities of the state" by ensuring that the Fundamental Rights apply to them. However, this Bill has subverted the meaning of the phrase and used it incorrectly to exempt any entity that is linked to the state from following any of the provisions of this Bill.

Further, the exclusion of "instrumentalities of the state" from following data processing laws is inconsistent with the Competition Act, 2002. Under this Act, only entities which are "performing a sovereign function" may be exempt from its application. To take an example, State Bank of India according to this Bill is exempt from the provisions but its competitor banks in the private sector would have to follow them. Since SBI does not provide a sovereign function, the application of this Bill frustrates the existing framework on fair competition. For these reasons, we suggest that any references to "instrumentality of the state" be removed from the Bill.

The Bill has also failed to consider exemptions allowed for certain end uses such as journalistic, artistic and literary purposes. These exemptions are recognized in other countries and they were also present in clause 36(e) of the PDP, 2019. This exemption is analogous to the fair use exemption that is already contemplated by this Bill for research and archiving.

5 Compliance framework

5.1 Chapter as a whole

The Data Protection Board of India (DPBI), as envisaged by this Bill, only has some powers of adjudication. It does not have the power to issue its own regulations or conduct its own investigations. The absence of an investigating agency that investigates and prosecutes offences under the law will embolden data fiduciaries and processors to exploit the information asymmetry between them and private complainants.

Further, the Bill should consider giving the DPBI some role in the adjudication over the *likelihood of harm* as opposed to only covering provable harms. In most cases, the harm may not be quantifiable or provable and the quasi-judicial mechanism may need to ascertain some function of penalty for practices that, while not immediately responsible for a breach or loss, nevertheless carry a risk so high that a penalty may be justified.

5.2 Data Protection Board of India

The Supreme Court in *Union of India* v. *R. Gandhi* 2010 (11) SCC 1 noted:

> "Tribunals should possess the independence, security and capacity associated with courts ... if a Tribunal is packed with members who are drawn from the civil services and who continue to be employees of different Ministries or Government Departments by maintaining lien over their respective posts, it would amount to transferring judicial functions to the executive which would go against the doctrine of separation of power and independence of judiciary."

The DPBI's function is to receive and adjudicate complaints and impose penalties and other remedies. However, its composition consists entirely of members appointed by the Union Government. It does not have any judicial members. The strength, composition, qualifications of members, process of selection, terms and conditions of appointment and service, disciplinary action etc. are not laid down in the Bill. They are left to delegated legislation. This raises questions on the separation of powers between an adjudicatory body like DPBI and the Union government which, as the executive, makes decisions on all facets of the DPBI.

We suggest that the DPBI's membership be chosen by a committee with equal representation by the executive and judiciary to be mentioned in the Bill. The selection of members should be done on the basis of some objective criteria which are mentioned in the Bill e.g. technical persons to be persons with qualifications and experience in the field of data protection and privacy, judicial members to be persons qualified to become a judge, etc.

5.3 Functions of the Board

The DPBI has powers only to receive complaints, conduct hearings and pronounce decisions. This will seriously undermine the state's ability to prosecute and even seek information on actions which could be potential violations of the Bill. We suggest that the DPBI be made a full regulator with powers of investigation, search and seizure, and regulation in addition to adjudication to ensure the protection of user rights. The design of DPBI should be in accordance with the decisions of the Supreme Court on the separation of powers.

5.4 Process to be followed by the Board to ensure compliance with the provisions of the Act

The process by which the Board determines which complaints are "devoid of merit" is unclear and this provision should not stand in the first place. Only complaints of a *frivolous* or *vexatious* nature should face any adverse action. A common person cannot be expected to understand the technicalities of the law and they should be guided to approach the correct forum instead of being threatened with costs. No other court or statute has any such provision for penal action against a petitioner. Such open-ended language could be used by any large data fiduciary against a petitioner and frustrate the ends of justice. We suggest that clause 21(12) be removed in its entirety.

Clause 21(11) notes the ability of the board to dismiss those instances wherein non-compliance

is "not significant." This framing creates a situation wherein the required standard is raised - that is to say it is no longer sufficient that there has been a violation of the provisions of this bill but rather it is now required that this violation be significant for the board to take action. Moreover, It is unclear how this determination of significance will be made by the board, particularly in those cases wherein the data rights of a data principal are violated.

The bill therefore clearly denotes the data rights of principals as protected only beyond a certain threshold of significance. We suggest that "non-significant" non-compliance should be removed.

5.5 Review and appeal

If a person is aggrieved with the outcome of a complaint filed before the DPBI, they have the right to file an appeal with the High Court. This means that the High Court is the first *judicial* authority to hear cases since there are no judicial members in the DPBI. If there are judicial members present in the DPBI, the quality of orders will improve which will limit the propensity of the High Courts to admit appeals. We suggest that the DPBI have an equal proportion of technical and judicial members in adjudicatory roles.

5.6 Voluntary Undertaking

Clause 24 outlines the ability of the board to accept a voluntary undertaking from any entity that submits to either carry out or refrain from carrying out a specified action. Acceptance of this voluntary undertaking by the board would lead to a bar on any proceedings against that entity for the specified action or inaction.

While such voluntary undertakings can make dispute resolution more effective and reduce compliance costs, their use in situations wherein the rights of data principles have been violated must be limited. In such situations, providing a hearing to the aggrieved data principal must be mandated in order to ensure fairness. Furthermore, the process of acceptance of a voluntary undertaking must be transparent and reasoned. The introduction of such processes serves to prevent the misuse of such undertakings.

Clause 24(4) notes that in instances where the data fiduciary does not comply with the voluntary undertaking, the DPBI "*may, after giving such person, a reasonable opportunity of being heard, proceed in accordance with section 25 of this Act.*" The use of the word "may" implies that DPBI will have the option to determine whether or not a fine is imposed following the non compliance of a voluntary undertaking. While this can be useful in cases wherein there is no violation of the rights of data principals, it is necessary to prevent its misuse in cases where such a rights violation does take place. We suggest that in cases where a voluntary undertaking by a data fiduciary relating to the rights of a data principal is violated, the board will be required to impose a financial penalty under clause 25.

We suggest that this clause be redrafted to ensure that an opportunity of a hearing be provided to affected stakeholders in case of a voluntary undertaking in respect of a breach that affects their rights. Further, the government must provide for a transparent process

to accept a voluntary undertaking as well as clearly defined and mandatory penalties for failures to abide by voluntary undertakings.

6 Miscellaneous

6.1 Power to make rules

The power to make rules should be laid down in a specific way. A general power to make rules "to carry out the purposes of the Act" could result in the government making rules which extend beyond the powers contemplated by the statute. This would lead to increased chances of litigation and uncertainty among all stakeholders. We suggest that specific powers to make rules be laid out in a manner similar to section 87 of the IT Act, 2000.

6.2 Amendments

Section 43A of the IT Act has been removed. But section 43A is dependent on many other provisions in the IT Act e.g. sections 46, 47, 48 etc. that provide for an adjudication mechanism that will continue to operate. This will conflict with the DPBI's adjudication mechanism unless it is made clear that the DPBI will adjudicate only those matters that relate to section 43A of the IT Act i.e. compensation in case of compensation to protect data. Some provisions like section 70A should also be amended to make DPBI and not CERT-in the agency that imposes reporting requirements on data fiduciaries in case of cybersecurity incidents involving the compromise of personal data. If section 70A of the IT Act is not amended by this Bill, firms will have to make the same reporting to two separate agencies which is onerous.

The amendment to the Right to Information Act, 2005 (RTI Act, 2005) is ill-advised since it gives a very strong ground for Public Information Officers to reject RTI applications. After this amendment, the exemption from provision of information will simply read, "information which relates to personal information". Virtually any request for information which has an element of personal information could be denied. The amendment to the RTI Act has no bearing on the data entered online by an individual. It is unclear if the text of the amendment covers only personal data shared online to a data fiduciary by a user. The RTI Act should be amended directly in this case. We suggest this amendment be removed from the Bill entirely.

7 Miscellaneous

More than half of all provisions in this Bill allow for the government, specifically the Union government, to make rules and prescriptions. Excessive delegated legislation leads to arbitrariness, regulatory uncertainty and the lack of parliamentary scrutiny. The lack of clarity in these provisions should be addressed at the stage of drafting of the Bill itself.