INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

TDW (THE DATA WRAP)

Authors: Namita Viswanath | Shreya Suri | Naqeeb Ahmed | Nikhil Vijayanambi
Ruhi Kanakia | Srika Agarwal

MARCH 2023

INTRODUCTION

Change is the only constant. We live in a fast-paced society with limited time, as a result everyone's a big fan of a wrap (all ingredients mixed up and rolled in a piece of bread). We at IndusLaw through this piece are attempting to do the same with all things data, thus calling this **THE DATA WRAP!** (Wrap anyone?)

GOING BACKWARDS

NOVEMBER 2022

The government ended the year 2022 with a bang (if we may call it so) and on a positive note with the introduction of the draft Digital Personal Data Protection Bill ("**Data Protection Bill**"). The Data Protection Bill is the government's fourth attempt to create a wholesome and specific data privacy law. It is also the simplest and most succinct draft data protection law released by the government till date.

The Data Protection Bill is focussed on promoting the ease of doing business and sets out the (a) rights and duties of citizens (i.e., Digital Nagrik); and (b) obligations of data fiduciaries based on the data privacy principles, namely, (i) lawful, fair, and transparent usage of personal data; (ii) purpose limitation; (iii) data minimization; (iv) accuracy of personal data; (v) storage limitation; (vi) reasonable safeguards to ensure prevention of unauthorized collection or processing of personal data; and (vii) accountability for processing of personal data by the person deciding the purpose and means of processing.

That said, the Data Protection Bill fails to recognize the fundamental right to privacy of individuals, which is in contrast with the previous iterations of the bill – this is an irony, considering the fact that the Data Protection Bill is the outcome of an exercise undertaken to safeguard the right to privacy of individuals.

More onw the Data Protection Bill is available here.

OCTOBER 2022

After concluding public consultations which started in June 2022, the Ministry of Electronics and Information Technology ("**MeitY**") notified the amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**Intermediary Rules**").

The amended Intermediary Rules, among other things, (a) requires intermediaries to make reasonable efforts to cause users to not host, display, upload, modify, publish, transmit, store, update or share any misinformation and hate speech (which has not been specifically called out) along with other unlawful content on its platform; (b) establishes 'Grievance Appellate Committees' which have been effective from March 1, 2023, as an appellate mechanism from orders of grievance officers such appeals are to be resolved through an online dispute resolution format; and (c) requires intermediaries to provide a choice of language to its users vis-à-vis its policies, including its privacy policy and terms of use.

SEPTEMBER 2022

With the growth of innovative methods of designing and delivering credit products and their servicing through digital lending platforms, certain concerns emerged such as breach of data privacy, misuse of data, mis-selling, unfair lending and recovery practices, etc. The Reserve Bank of India ("**RBI**") sought to address these concerns that led to the RBI constituting a working group on digital lending including lending through online platforms and mobile apps on January 13, 2021 ("**Working Group**"). The report submitted by the Working Group[1] ("**Report**") invited feedback from diverse stakeholders and basis such feedback, the RBI announced by way of a press release ("**Press Release**"), a regulatory framework focused on the orderly growth and regulation of the digital lending ecosystem.[2]

The Press Release sets out the applicable recommendations from the Report which were intended to be implemented by the RBI in a phased manner through specific regulations issued by the RBI in this regard. As part of the Press Release, the RBI clarified that it would issue detailed instructions in relation to the Press Release separately. Pursuant to this, on September 2, 2022, the RBI released a circular titled 'Guidelines on Digital Lending' ("**Guidelines**") implementing the crucial recommendations identified in Annex I of the Press Release along with certain incremental provisions *(Press Release and Guidelines are collectively referred to as "**Framework**").*

The Framework is intended to be focused on RBI regulated entities that are permitted to carry out the business of lending ("**REs**") and Lending Service Providers ("**LSPs**")[3] engaged by such REs to extend various credit facilitation services. While applicable primarily to the REs as the regulated entities under the jurisdiction of the RBI, the Framework provides guidance for the REs, LSPs and the digital lending applications ("**DLAs**") of REs and LSPs, with the onus of implementation resting on the REs.

1. Press Release titled 'RBI releases the Report of the Working Group on digital lending including lending through online platforms and mobile apps' dated November 18, 2021, available at (https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52589)
2. Press Release titled 'Recommendations of the Working group on Digital Lending – Implementation' dated August 10, 2022, available at (https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=54187)
3. An agent of a Regulated Entity who carries out for a fee from the RE, one or more of lender's functions in customer acquisition, underwriting support, pricing support, disbursement, servicing, monitoring, collection, recovery of specific loan or loan portfolio.

SEPTEMBER 2022 (Continued)

Digital Lending Guidelines – A Data-Focussed Approach

The Guidelines prescribe certain specific requirements in relation to the collection, usage and storage of data with third parties, such as LSPs engaged by the REs. While some of the requirements stated therein are on similar lines as the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI Rules**"), which is the primary data protection rules framed under the Information Technology Act, 2000 ("**IT Act**")**,** these obligations are further detailed and have been tailored to specifically address the data specific concerns vis-à-vis digital lending activities of the REs undertaken with facilitation by LSPs.

In terms of setting minimum standards, the Guidelines have effectuated certain core principles on (a) consent mechanism, (b) purpose of collection of data, and (c) storage of data. In the digital payments ecosystem, the RE that engages an LSP is obligated to ensure that the minimum standards set out under the Guidelines are complied with by the LSP, and that the DLA *(of the RE and/or the LSP)*, reflects such compliance as well.

At the outset, the Guidelines provide for explicit and prior consent to be taken for collection of any data by the DLAs, and that such collection shall be need-based. The implication here is that data collection shall be limited to purposes for which such collection is absolutely necessary. Further, a restriction is also placed in terms of mobile resources including media and files, contact lists, and call logs, which the DLA shall desist from accessing. Additionally, collection and storage of biometric data has been explicitly prohibited unless the same is mandated in any extant statutory guidelines. That said, the Guidelines allow one-time access to resources like camera, microphone and location, with the explicit consent of the user, only for onboarding and KYC purposes. The intention of the RBI appears to be that data collection by LSPs should be minimal and solely restricted to the purposes for which they are required.

Furthermore, users' rights in terms of (a) denying and revoking consent; (b) requesting deletion of their data; and (c) restricting disclosure of their data to third parties, have been factored in the Guidelines. It has also been specifically highlighted that DLAs have to mention the purpose at every instance of data collection. Additionally, any act of sharing of data of users with third-parties would require the explicit consent of the user, with the exception being when such disclosure is mandated by law.

The Guidelines have also prescribed various measures pertaining to storage of users' data so as to ensure that DLAs store only minimal basic personal information of such users, which are necessarily required by such apps for undertaking their operations. Further, DLAs are required to have comprehensive policies in place pertaining to, among other things, (a) type of data that can be stored; (b) period for which such data can be stored; (c) restrictions on use of such data; (d) data destruction protocol; and (e) standards for addressing security breach. Additionally, the Guidelines provide for data localisation, and state that data collected shall only be stored in servers located in India. The Guidelines also prescribe that the principles set out by the RBI shall be captured comprehensively in the privacy policy of a DLA.

The foregoing requirements, while similar in intent to the SPDI Rules to a certain degree, certainly offer a greater protection than the SPDI Rules and the IT Act, given the extensive nature of financial information and sensitive personal data that LSPs are likely to process. The Guidelines will potentially warrant revisiting the user interface, terms of use and privacy policies of the DLAs and websites of the LSPs and the REs. The collective effect of these measures is that the users are in control of the processing of their personal data, thereby safeguarding users' interests and avoiding misuse of their data. This is especially relevant in light of recent instances of LSPs adopting unscrupulous means including misusing personal data of users to threaten them when collecting loan repayments. While the Guidelines have made a reasonable attempt at incorporating certain core principles of data protection, there still remains a need for a more robust data protection framework to capture the principles already covered in the Guidelines and more.

JULY 2022

The National Payments Corporation of India ("**NPCI**") issued a circular that required all Unified Payments Interface ("**UPI**") applications to obtain explicit consent from their users before collecting their location data. The circular was issued in response to growing concerns over the privacy and security of user data.

Location data can reveal a lot about a person's daily routines, travel patterns, and personal preferences. It is often collected by UPI applications to provide location-based services, such as finding nearby merchants or enabling transaction alerts based on the user's location.

However, the collection of location data without explicit consent has raised concerns about the potential misuse of this information by third-party entities. Accordingly, the NPCI has mandated that UPI applications must obtain a one-time consent from their users before collecting their location data. The consent must be obtained in a clear and unambiguous manner, and users must have the option to withdraw their consent at any time.

The circular is a significant step towards protecting the privacy of UPI users in India, particularly in the context of collection and processing of data that may not directly identify the user, but with other relevant factors can amount to being classified as personal data. By requiring explicit consent for the collection of location data, the NPCI has made it clear that user privacy is a high priority for UPI applications.

APRIL 2022

With data leaks, ransomware attacks and other cyber security incidents becoming increasingly rampant, the Indian Computer Emergency Response Team ("**CERT-In**") took charge of matters and issued 'Directions relating to information security practices, procedure, prevention, response, and reporting of cyber incidents' ("**CERT-In Direction**") and explanatory FAQs thereunder.

More on the CERT-In Direction is available here.

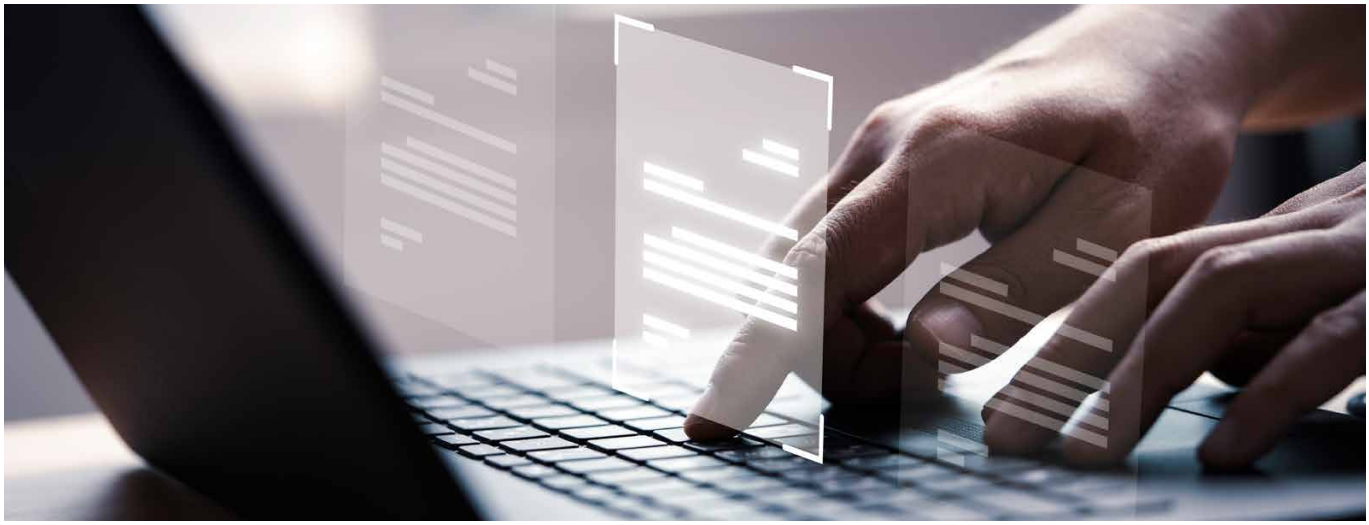
FEBRUARY 2022

The MeitY released the draft India Data Accessibility and Use Policy, 2022 ("**Policy**"). The Policy aims to facilitate data sharing across ministries and departments of the Government, thereby increasing access to, and the quality of non-personal data created, generated, collected, or archived by the Government.

The Policy plans to achieve this by (a) establishing the India Data Office ("**IDO**"); and (b) the India Data Council ("**IDC**"). The IDO will ensure monitoring, implementation, and enforcement of the Policy whereas, the IDC will coordinate data sharing across ministries, provide technical support and periodically evaluate their performance.

The Policy is in line with the Government's recognition of non-personal data as a valuable resource and the opportunities it provides for better governance, service delivery, and innovation in sectors critical for societal transformation. The Policy also notes that the nation's ambition to achieve a USD 5 (five) trillion economy is dependent on its ability to harness its data.

While the Policy provides for anonymisation of data and is only applicable to non-personal data or information processed by the Government, it would raise privacy concerns if such data were to be monetized by the government (particularly if the process of anonymisation can be reversed), and this would defeat the very purpose of having such a Policy (protecting the non-personal data) in place. The Policy must ideally address and curtail the potential of any misuse of citizens data and curb privacy violations. It has been a year since MeitY had released the draft Policy but any developments or revisions to the draft Policy are yet to be seen.



ON THE SIDE!!! LET'S NOT FORGET THE RIGHT TO BE FORGOTTEN

The culmination of 2022 witnessed yet another attempt by the MeitY to bring in a draft legislation to regulate the use and processing of personal data of data principals,[4] titled Data Protection Bill. The Data Protection Bill (along with its previous iterations) essentially found its genesis in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India and Ors*: Justice Chandrachud[5] ("**Puttaswamy I**"), as well as the resultant Justice BN Shri Krishna Committee report, and dives into myriad concepts surrounding the protection of digital personal data.

While MeitY has broken new ground on several aspects and delivered a simplified law that attempts to navigate competing interests, the Data Protection Bill does not seem to recognize the fundamental right to privacy of individuals, or the nuances related to the right, as was seen in the earlier iterations of the Data Protection Bill - one of the most prominent being the data principal's "right to be forgotten". The discussion surrounding this much-debated right flowed from Justice Sanjay Kishan Kaul's oral remarks in Puttaswamy I, wherein the Hon'ble judge noted that the right to be forgotten was an innate facet of the right to privacy and was necessitated in the digital era where any information available on the internet is seemingly permanent.

The bench in Puttaswamy I foresaw the "right to be forgotten" ("**RTBF**") to extend to the individual, the ability to limit, restrict, delink, or delete any personal data available with a data fiduciary, contingent to the personal data serving its requisite purpose. The right essentially allows individuals to control and determine the extent to which their personal data is communicated to others and is available for the general public's perusal. While acknowledging the existence of RTBF (and its inextricable link to the right to privacy), the Supreme Court of India also clarified that this right cannot be exercised where such data was necessary, was required for the compliance with legal obligations, or was required in public interest.

4. The Bill under section 2(6) defines data principals as *"the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child;.*
5. (2019) 1 SCC 1.

RTBF - A game of balance

The courts, in determining whether there is a reasonable expectation of privacy (and RTBF) in a given context, have attempted to implement an appropriate balance between the right to freedom of speech and expression (more specifically, the right to information) and the individual's right to privacy. This nexus, between RTBF and the right to information, and the case-by-case analysis that courts have undertaken to balance the two in a claim to RTBF, has led to various High Courts taking differential views on its application, as discussed below.

RTBF and right to information: The petitioner had sought the deletion of a judgment relating to a case from the internet, in which he was ultimately acquitted, contending that despite having a stellar academic record, he was unable to gain employment due to the presence of the judgment online. While noting that the issue requires an examination of the interplay between the petitioner's right to privacy and the public's right to information and maintenance of judicial records, the Delhi High Court granted *interim protection* to the petitioner due to the irreparable injury that may be caused, and also ordered the deletion of the judgment from Google, Indian Kanoon, etc.[6] Adopting a similar line of reasoning, while hearing a batch of petitions dealing with RTBF, the Karnataka High Court in late 2022 passed an *interim order* directing media houses (such as India Kanoon) to temporarily block the names of two acquitted persons who had invoked RTBF.[7] Very recently, a petitioner also sought the removal of articles from the internet regarding his conviction by the Leicester Crown Court on charges of fraud and blackmail from the Delhi High Court. While the Delhi High Court has issued notice to the Central Government, Google, Twitter and two media houses to respond to the petitioner's plea to delete such information, it is yet to be seen how the court sees RTBF in relation to charges of conviction.[8] In a contrasting opinion, however, the Kerala High Court in late 2022 orally observed that RTBF can't be claimed as an absolute right, and even if petitioners are acquitted, one may need to know the case registered against them and their details could be required for extraneous purposes. The court also stated that in the absence of a data protection law, it may be up to the particular online entity on what information was to be published and made available.[9]

RTBF and court records: In a petition claiming RTBF in an acquitted case, the Madras High Court *prima facie* observed that an acquitted person has a right to get his name redacted from court records. However, subsequently, the court also observed that the Indian criminal justice system has not reached a stage where courts can pass orders for redaction of the name of an accused person without any *"objective criteria prescribed by rules or regulations"*. It observed that RTBF cannot exist in the sphere of administration of justice, and it would be more appropriate to await the enactment of the data protection legislation and rules, which may provide such objective criterion. Additionally, it asserted that since the Madras High Court is a Court of Record under Article 215 of the Constitution of India, 1950 ("**Constitution**") it is entitled to preserve the original record in perpetuity. The court eventually dismissed the petition pointing out that unlike in Europe where regulation prescribes objective criteria which would guide a decision for redaction, no such judicially manageable standards exist in India. In the absence of that, redaction of information would lead to *"utter confusion"*.[10] Additionally, the Kerala High Court recently observed that a claim for the protection of personal data based on the right to privacy cannot co-exist in an open court justice system.[11]

RTBF and victims of crime: The Orissa High Court[12], Delhi High Court[13] and Madras High Court have individually acknowledged that RTBF *has no statutory genesis* and was therefore is not an absolute right. The courts, however, also recognized that the victims of criminal cases could be adversely impacted by objectionable content being made available in the public domain without their consent. Therefore, while recognizing that RTBF is an 'inherent aspect' of the right to privacy, they observed that the right to privacy of such a victim should be protected. The Karnataka High Court[14] recognized RTBF in a limited sense in a petitioner's request to remove his daughter's name from a judgment involving claims of marriage and forgery. It held that recognizing RTBF in such instances would parallel initiatives by 'western countries' which uphold this right when 'sensitive' cases concerning the 'modesty' or 'reputation' of people, especially women, were involved. Further, in a case before the Supreme Court of India, the court directed that personal data of a petitioner and a respondent in a sexual offence case be masked on the internet so that their details are not displayed by search engines.[15]

---

6. *Jorawar Singh Mundy v. Union of India & Ors.*, Writ Petition (C) No. 3918/2020.
7. *Neekunj Todi v. Union of India*, Writ Petition (C) No. 12596/2022.
8. *Mohammed Umar Ashrafi v. Union Of India*, Writ Petition (C) No. 12620/2021.
9. *Vysakh K.G. v. Union of India & Anr.*, Writ Petition (C) No. 26500/2020.
10. *Karthick Theodre v. Registrar General*, 2021 SCC OnLine Mad 2755.
11. *Virginia Shylu v. Union of India*, Writ Petition (C) No. 6687/2017.
12. *Subhranshu Rout alias Gugul v. State of Odisha*, 2021 (I) ILR - CUT- 687.
13. *X v. Youtube*, Civil Suit (OS) No. 392/2021.
14. *Sri Vasunathan v. The Registrar General*, Writ Petition (C) No. 62038/2016
15. XXXX *v. Kancherla Durga Prasad & Ors.* Special Leave Petition (Crl) No. 3211/2022.

Conclusion

Since the Indian legal system does not particularly carve out RTBF as a statutory right, the courts in India have viewed the same in light of the fundamental right to privacy as a recognized facet of Article 21 of the Constitution, owing to the potential harm to the reputation of not only the litigants, but also their families. This has led to varying lines of jurisprudence on RTBF, with different High Courts balancing RTBF with its contrasting rights in different ways. However, as seen in the cases discussed above, while recognizing the existence of the right, the lack of a statutory remedy has led to courts granting case-specific interim protection to the claimants, in the wait for the introduction of a new law that would clarify the recognition and grant of RTBF.

While clarity on RTBF was elusive at the time of the introduction of the 2021 iteration of the data protection law in India, the Data Protection Bill, surprisingly, does not directly recognize RTBF, and seeks to subsume this right under the right to erasure. With this right no longer part of the Data Protection Bill and bereft of set standards, it seems courts will have to continue to resort to balancing RTBF and its contrasting rights, with divergent approaches.

INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

www.induslaw.com

OUR OFFICES

BENGALURU
101, 1st Floor, "Embassy Classic"# 11
Vittal Mallya Road
Bengaluru 560 001
T: +91 80 4072 6600
F: +91 80 4072 6666
E: bangalore@induslaw.com

HYDERABAD
204, Ashoka Capitol, Road No. 2
Banjarahills
Hyderabad 500 034
T: +91 40 4026 4624
F: +91 40 4004 0979
E: hyderabad@induslaw.com

CHENNAI
#11, Venkatraman Street, T Nagar,
Chennai - 600017 India
T: +91 44 4354 6600
F: +91 44 4354 6600
E: chennai@induslaw.com

DELHI & NCR
2nd Floor, Block D
The MIRA, Mathura Road, Ishwar Nagar
New Delhi 110 065
T: +91 11 4782 1000
F: +91 11 4782 1097
E: delhi@induslaw.com

9th Floor, Block-B
DLF Cyber Park
Udyog Vihar Phase - 3
Sector - 20
Gurugram 122 008
T: +91 12 4673 1000
E: gurugram@induslaw.com

MUMBAI
1502B, 15th Floor
Tower – 1C, One Indiabulls Centre
Senapati Bapat Marg, Lower Parel
Mumbai – 400013
T: +91 22 4920 7200
F: +91 22 4920 7299
E: mumbai@induslaw.com

#81-83, 8th Floor
A Wing, Mittal Court
Jamnalal Bajaj Marg
Nariman Point
Mumbai – 400021
T: +91 22 4007 4400
E: mumbai@induslaw.com