# Technology Law Analysis

January 06, 2022

## PRIVACY AND DATA PROTECTION IN INDIA: 2021 WRAP

2021 was a blink-and-you-will-miss conveyor belt of activities on privacy and data protection in India. With the din of the absence of a comprehensive data protection law in India louder than ever, there was no lack of activity on the legislative and executive side. The Indian Government introduced significant changes such as liberalizing the archaic geospatial data regime, introducing industry standards for privacy assurance, and introducing tighter security measures in the digital payments sector. On the judicial side, there have been pronouncements on issues of anonymity, the right to be forgotten, and on state surveillance. The new draft of the proposed GDPR-inspired data protection law of course takes the cake, having been deliberated for two years since the last draft was floated.

We had anticipated an eventful year as predicted in our look-ahead to 2021, though our expectations have been well exceeded in terms of privacy and data protection developments. The roller-coaster ride of privacy and data protection law related legal developments from 2021 are elucidated below:

1. **Proposed data protection law**

   The Joint Parliamentary Committee on December 16, 2021 presented its report on the proposed data protection law, along with a revised version of the bill, the *Data Protection Bill, 2021* in the Parliament.[1] The draft bill is yet to be tabled as a draft law for consideration and passing by the Parliament. Subsequent to the draft bill being made public, there have also been calls from the industry for a fresh consultation since many of the provisions deviate from the previous version published two years ago.

   The draft bill, which has flavours of the GDPR, brings in a number of significant changes as compared to the earlier iterations of the proposed law, such as expanding the scope of the law to cover not only personal data, but *non-personal data* as well. Also introduced are stringent data breach reporting requirements (within seventy two hours), regulation of hardware manufacturers and enabling a certification mechanism for all digital and IoT devices to mitigate data breaches. The draft bill also provides for a phased implementation wherein the central government may notify different dates for enactment of different provisions.

   Our detailed analysis of the report of the Joint Parliamentary Committee and the draft bill is available here.

2. **New regime for geospatial data and map services**

   The Department of Science and Technology of the Government of India issued "*Guidelines for acquiring and producing geospatial data and geospatial data services including Maps*"[2] on February 15, 2021. Prior to the guidelines, there were numerous notifications and guidelines issued by various ministries/departments of the Government, including the Ministry of Defence, Survey of India, Ministry of Finance and Ministry of External Affairs regulating mapping data, most of which were either unclear or archaic, or both. Under the new guidelines, there is no restriction, nor requirement of any approval, clearance, license, etc. on the collection, generation, preparation, dissemination, storage, publication, updating and/or digitisation of geospatial data and maps within the territory of India, subject to a negative list of attributes for which there are restrictions. The new guidelines also restrict foreign entities from creating and/or owning, or hosting geospatial data finer than certain prescribed threshold values. They are also restricted from conducting terrestrial mobile mapping surveys, street view surveys and surveying in Indian territorial waters.

   Our analysis of the new geospatial data and maps guidelines are available here.

3. **Banking regulator clamps down on card data storage**

   The Reserve Bank of India (RBI) introduced "*Guidelines on Regulation of Payment Aggregators and Payment Gateways"* tolicense andregulate payment intermediaries facilitating and handling payments between users and merchants using electronic / online payment modes.[3] Under these guidelines, RBI introduced a restriction on payment aggregators and merchants from storing card and card related data. Subsequent clarifications were also issued in March 2021[4] reiterating the card data storage restrictions. On September 7, 2021, the RBI issued a circular mandating that, from January 1, 2022, (a) no entity other than card issuers or card networks is allowed to store card data, and (b) all such data previously stored should be purged.[5] As an exemption, the last 4 digits of the card number and the card issuer's name could be stored for transaction tracking and reconciliation purposes.

   Tokenization was suggested as a workable solution to comply with the card storage restrictions, whilst maintaining continuity in online payments. RBI widened the existing limited device-based tokenization framework to all devices and also permitted card-on-file tokenization. Based on multiple industry representations to the RBI,

## Research Papers

**FAQs on Setting Up of Offices in India**
December 13, 2024

**FAQs on Downstream Investment**
December 13, 2024

**Gaming Law 2024**
December 12, 2024

## Research Articles

**The Revolution Realized: Bitcoin's Triumph**
December 05, 2024

**The Bitcoin Effect**
November 14, 2024

**Acquirers Beware: Indian Merger Control Regime Revamped!**
September 15, 2024

## Audio

**Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice**
December 18, 2024

**Digital Lending - Part 1 - What's New with NBFC P2Ps**
November 19, 2024

**Renewable Roadmap: Budget 2024 and Beyond - Part I**
August 26, 2024

## NDA Connect

Connect with us at events, conferences and seminars.

## NDA Hotline

Click here to view Hotline archives.

## Video

**"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh**
October 31, 2024

**Analysing SEBI's Consultation Paper on Simplification of registration for FPIs**

the RBI on December 23, 2021 extended the timeline for compliance till June 30, 2022.[6]

Our article on these developments on card data storage is available here and our webinar with industry stakeholders can be viewed here.

4. **Data privacy standards issued**

The Bureau of Indian Standards, towards mid-2021, made available to the public its new standards for data privacy assurance i.e., the IS 17428 which was notified earlier.[7] The standard seeks to provide a privacy assurance framework for organizations to establish, implement, maintain and continually improve their data privacy management system. It comprises two parts - one being the prescriptive part where the requirements are to be mandatorily implemented by anyone applying the standard and the other part being the suggestive part with detailed best practices to aid in implementing the requirements of the prescriptive part.

It could be evaluated whether implementation of the IS 17428 by organizations could deem them compliant with the requirement under the *Information Technology (Reasonable securitypractices and procedures and sensitive personal data or information) Rules, 2011* to maintain reasonable security practices and procedures for sensitive personal data or information. However, these rules and the IS 17428 fall short of explicitly specifying that implementation of the prescriptive part of the IS 17428 is deemed compliance with the requirement to maintain reasonable security practices and procedures. Hence, the onus may be on the organizations to demonstrate that implementation of the prescriptive part of the IS 17428 meets such a requirement.

Under the upcoming data protection law, data fiduciaries and processors are required to implement security safeguards that use de-identification, encryption, steps to protection personal data integrity and to prevent misuse, unauthorized access, modification, disclosure or destruction of personal data. It should be evaluated and clarified whether the implementation of the IS 17428 can be demonstrated as compliance with these security obligations.

Our detailed analysis of the IS 17428 is available here.

5. **Large messaging apps required to introduce traceability features**

The Ministry of Electronics and Information Technology notified the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*[8] on February 25, 2021 replacing the *Information Technology (Intermediaries guidelines) Rules, 2011*. The new intermediary rules provide for certain due diligence requirements to be followed by internet 'intermediaries' including an obligation to retain information of all users collected upon registration for one hundred and eighty days even after any cancellation or withdrawal of such registration. The rules also went a step ahead by recognizing certain intermediaries as 'significant social media intermediaries' if the number of registered users cross a certain threshold (subsequently notified as 50,00,000 registered users[9]). One of the additional due diligence requirements to be complied with by significant social media intermediaries which provide messaging services primarily is to enable the identification of the first originator of the any information that is transmitted through such intermediary, if required to do so by a court or a government direction to intercept, monitor or decrypt the information. The new intermediary rules provide that the significant social media intermediary is required to disclose only the identification of the first originator of a message and not the contents of any electronic message or any information related to the first originator or other users.

This traceability requirement under the new intermediary rules has been challenged by WhatsApp before the Delhi High Court[10] on the grounds of unconstitutionality and violation of the fundamental rights to privacy and freedom of speech and expression of an individual. The case is pending before the Delhi High Court as on the date of this article.

6. **Judicial probe into the Pegasus spyware issue**

The Supreme Court of India delivered a significant judgment on October 27, 2021 following certain reports of a spyware called '*Pegasus'* (developed by an Israeli security firm i.e. the NSO Group) being deployed as a surveillance tool on Indian citizens.[11] The petitions prayed for an independent investigation to be conducted into the alleged deployment of Pegasus by certain foreign governments and Indian government agencies.

The Supreme Court noted that the impact of the alleged use of Pegasus on the right to privacy and freedom of speech need to be examined, while forming the three-member expert technical committee. The committee is directed to make recommendations on enactment or amendment to existing surveillance laws to ensure an "improved" right to privacy, improved cyber security and threat assessment measures. The recommendations of the committee are yet to be submitted.

7. **Antitrust concerns with WhatsApp's privacy policy update**

WhatsApp LLC, which operates the messaging platform WhatsApp updated its privacy policy and terms of service in January 2021. While previous updates to WhatsApp gave its users the choice to 'opt-in' to the data sharing with Facebook, this privacy policy update required users to agree to data sharing with Facebook in order for the user to continue using the WhatsApp service. In an order dated March 24, 2021, the Competition Commission of India, which is India's antitrust regulator initiated an investigation against WhatsApp, Inc. and Facebook, Inc. assessing the potential impact of the WhatsApp update on competition in the Indian market.[12] It noted that the unilateral requirement on users to accept the update to WhatsApp's privacy policy vitiates their voluntary agreement and primarily appears to be unfair and unreasonable for its users.

Facebook, Inc. and WhatsApp, Inc. in separate petitions before the Delhi High Court challenged the order of the Competition Commission of India initiating an investigation.[13] It was argued that the WhatsApp update does not negate the choice of users and is aimed at providing further transparency on WhatsApp data sharing practices with Facebook. The Delhi High Court dismissed these petitions and additionally, upheld the impleadment of Facebook, Inc. deeming it to be an integral part of the investigation.[14]

September 26, 2024

**Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996**

September 22, 2024

8. **(No) right to be forgotten**

   A single judge bench of the Madras High Court delivered a judgment on August 3, 2021 dismissing a petitioner seeking to have his name redacted from court orders by exercise of his right to be forgotten.[15] The petitioner was subjected to criminal proceedings in the trial court and in the Madras High Court but was ultimately acquitted. In the interest of his reputation, the petitioner prayed for his name to be redacted from the judgment of the Madras High Court. The Madras High Court reiterated an individual's right to privacy (and anonymity) as held by the Supreme Court in *K.S Puttaswamy v. Union of India*[16] while also pointing out that the Supreme Court held that the right to be forgotten cannot be exercised if the information is required for the performance of a task carried out in public interest. Without a precise framework or objective criteria for redaction of the name of an accused in India's criminal justice system, the court held that it would be more appropriate to await the enactment of India's new data protection law to exercise such rights and thus dismissed the petition.

   This follows along the same lines as previous judicial decisions by various high courts over the last few years emphasising the importance of the right to be forgotten and the need for legislative action in this regard. Interestingly the draft data protection bill recognizes an individual's right to be forgotten in a limited manner and extends it to include a restriction on 'processing',[17] exercisable with due procedure.

   Our analysis of such previous decisions on the right to be forgotten may be accessed here.

9. **National Strategy on blockchain recommends data localization**

   The Ministry of Electronics and Information Technology published its '*National Strategy on Blockchain*'[18] in December 2021 with the aim to provide an insight into strategies and recommendations for creating a trusted digital platform using blockchain that can facilitate trusted service delivery to citizens and businesses. Interestingly, the ministry has identified that many countries have introduced data localization restrictions and as a security/privacy measure recommends that data localization should be enabled for blockchain based systems in the country. It suggests that this localization requirement may be achieved by "*hosting the blockchain infrastructure, data and smart contracts within the country*". While this is still a policy consideration it remains to be seen how data localization measures would be implemented for decentralized technologies.

10. **Closer lens on digital lending platforms**

    In January 2021, the RBI had constituted a working group to study digital lending activities in light of increasing disruption by online lending apps. The Report of the Working Group on '*Digital Lending including Lending through Online Platforms and Mobile Apps'* was published on November 18, 2021.[19] It was observed that numerous lapses regarding privacy occurred across digital lending apps. Inadequate transparency, lack of choice of the user to manage or delete their data after a loan has been paid, non-disclosure of partner banks or non-banking financial companies (NBFCs), and misuse of borrowers' sensitive data to harass them and their family/friends were identified as some of the major concerns.

    Through this report, the working group of the RBI gave some recommendations related to technology including near term recommendations that data should be stored in servers locally in India and that data should only be collected "*from the borrower/ prospective borrower with prior information on the purpose, usage and implication of such data and with explicit consent of the borrower in an auditable way*". It was also recommended that standards on data and network security need to be prescribed for such apps and must be mandatorily reflected in the terms of service. The report was opened for public comments and the RBI stated that it will take a final view on the proposed regime.

11. **Parliamentary Standing Committee recommends permanent blocking of VPNs**

    The Parliamentary Standing Committee of Home Affairs presented its 233rd report on *Atrocities and Crimes against Women and Children*[20] on March 15, 2021 before the upper house Of Parliament. The report identified Virtual Private Network (VPN) services as a "technological challenge" that allow criminals to remain anonymous online and access the dark web to commit crimes bypassing security walls. It recommended that a coordination mechanism be developed with international agencies to ensure that these VPNs are blocked. Since VPNs are also used as security and privacy enhancing tools to maintain anonymity on the internet by users, such a recommendation would have to be seen under the lens of a person's right to remain anonymous which is a part of the fundamental right to privacy affirmed by the Supreme Court in *K.S Puttaswamy v. Union of India*[21]. Presently, there are no general legal restrictions which may specifically prohibit or regulate the use of VPNs by individuals.

12. **Bill on regulating DNA Technology**

    During the 2021 monsoon session of the Parliament, the *DNA Technology (Use and Application) Regulation Bill, 2019*[22] was listed for consideration and passing before the lower house. This bill seeks to regulate the use of DNA technology for identifying persons for specific purposes such as solving crimes, among others. It also prescribes DNA collection procedures, establishment of DNA data banks, a regulatory board, accreditation mechanisms, etc. The bill was however not taken up in the Lok Sabha.

    Since the bill allows for the collection of DNA samples without consent in certain circumstances (such as for offences with imprisonment terms of above 7 years), the interplay with one's right to privacy is a serious consideration which the law would have withstand.

## A DEFINING YEAR AHEAD

2022 may well be the landmark year that India sees its first comprehensive, general data protection law introduced. While there are still certain aspects that may need to be ironed out, it is possible that a draft law may be laid before the Indian Parliament in the budget session in February or the monsoon session thereafter, which typically happens across July and August. There may even be a fresh public consultation held on the draft law, which would be a welcome step.

As industry regulators also play a more proactive role of protecting data and consumers interests in their sectors, there have been numerous developments in terms of sector specific data regulation. Implementation of the incoming general data protection law in tandem with these sector specific regulations may raise some note-worthy issues, and may even prompt important questions to be considered by Indian courts. For instance, with increasing significance of new-age technologies such as AI/ML, IoT, blockchain and Web 3.0, it would be interesting to see how regulators blend traditional stances on data localization with these decentralized data sharing frameworks.

*Buckle up, sit tight and let's embrace a promising 2022!*

– Purushotham Kittane, Aaron Kamath & Gowree Gokhale

You can direct your queries or comments to the authors

[1] Available at 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 (last accessed December 31, 2021).

[2] Available at https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf (last accessed December 31, 2021).

[3] Available at https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0 (last accessed December 31, 2021).

[4] Available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12050&Mode=0 (last accessed December 31, 2021).

[5] Available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12159&Mode=0 (last accessed December 31, 2021).

[6] Available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12211&Mode=0 (last accessed December 31, 2021).

[7] See https://egazette.nic.in/WriteReadData/2020/223869.pdf (last accessed December 31, 2021).

[8] Available at https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf (last accessed December 31, 2021).

[9] See https://egazette.nic.in/WriteReadData/2021/225497.pdf (last accessed December 31, 2021).

[10] *WhatsApp v. Union of India* (W.P. (C) 7284/2021).

[11] *Manohar Lal Sharma v. UOI* (WP (Crl) 314 of 2021); available at https://main.sci.gov.in/supremecourt/2021/16884/16884_2021_1_1501_30827_Judgement_27-Oct-2021.pdf (last accessed December 31, 2021)

[12] See https://www.cci.gov.in/sites/default/files/SM01of2021_0.pdf (last accessed December 31, 2021).

[13] *WhatsApp v. CCI* (W.P.(C) 4378/2021 & CM 13336/2021) and *Facebook, Inc. v. CCI* (W.P.(C) 4407/2021 & CM 13490/2021).

[14] Available at http://164.100.69.66/jupload/dhc/NAC/judgement/24-04-2021/NAC22042021CW43782021_153656.pdf (last accessed December 31, 2021).

[15] *Karthick Theodre v. The Registrar General, Madras High Court* (W.P.(MD) No.12015 of 2021 and WMP (MD).No.9466 of 2021); available at https://www.mhc.tn.gov.in/judis/index.php/casestatus/viewpdf/783065 (last accessed December 31, 2021).

[16] WP (C) 494 of 2012; available at https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf (last accessed December 31, 2021).

[17] "processing" under section 3(36) of the draft data protection bill is defined as the following:

"*"processing" in relation to personal data, means anoperation or set of operations performed on personal data, and mayinclude operations such as collection, recording, organisation,structuring, storage, adaptation, alteration, retrieval, use, alignmentor combination, indexing, disclosure by transmission, dissemination*or otherwise making available, restriction, erasure or destruction."

[18] Available at https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf (last accessed December 31, 2021).

[19] Available at https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189 (last accessed December 31, 2021).

[20] Available at https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/15/143/230_2021_3_14.pdf (last accessed December 31, 2021).

[21] WP (C) 494 of 2012; available at https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf (last accessed December 31, 2021).

[22] Available at http://164.100.47.4/billstexts/lsbilltexts/asintroduced/128_%202019_LS_eng.pdf (last accessed December 31, 2021).

not substitute the need to refer to the original pronouncements.