BREACH OF PERSONAL DATA HELD BY THE STATE: CRITICAL CONSIDERATIONS IN THE BREACH NOTIFICATION PROCESS UNDER INDIA'S UPCOMING DATA PROTECTION LAW

Written by ***Abishek Nippani***

2nd Year MPP student, National Law School of India University

INTRODUCTION

Instances such as government databases being left open without requiring password access, criminals selling access to government databases for 'sessions of 10 minutes' and botched procedures leaking data have made breach of personal data held with the State business as usual. A report by World Economic Forum (2019) stated that UIDAI – the principal Aadhaar implementing agency has had its database incessantly breached since inception, compromising sensitive personal data of over 1.1 billion Indians. A COVID-19 tracking app introduced by Madhya Pradesh was breached within days (Ranjan 2020). Recently, the CSC BHIM website was breached resulting in highly sensitive personal data of over 70 lakh people being compromised (Sengupta 2020). The breached data included, *inter alia*, scans of caste certificates, Aadhaar cards, residence, payment related data and PAN cards. The breach also compromised personal data of minors. The firm that identified this breach has stated that the same has occurred due to a misconfiguration which allowed public access to the database.

The WEF (2019) report mentioned earlier ranked the Aadhaar leak(s) as the biggest in the world, followed by the Marriott-Starwood breach, which put personal information of 500 million people at risk. However, the data protection authority of U.K. (the ICO) has decided to impose a fine of £99,200,396 on Marriott (Information Commissioner's Office 2019). Such a situation with the Aadhaar breach is unimaginable, despite attempts[i] to seek damages from the Government for the same.

Breach of personal information held by public institutions gives immense scope for fraud and misuse, and due to undeveloped breach remedy strategies, approaches have been deplorable. For example, the Jharkhand government had cancelled *en masse* ration cards that were not linked to Aadhaar cards in 2017 in a bid to fight fraud (Scroll.in 2020). The callousness with which public institutions deal with personal data can be understood from the fact that the Jharkhand government did not even notify the affected individuals about the deleted ration cards, and this act has resulted in hundreds of starvation deaths (ibid.).

Government of India has denied both the breaches – the claim with respect to CSC BHIM breach (Faisal 2020) (the entire website is inaccessible as on 15 June 2020) and the numerous Aadhaar breaches (Vidyut 2018).[ii]

Other incidents such as the chief of TRAI challenging people to hack him (Indian Express, 2018), though humorous, highlight the condition of technical dissonance even helms of technical regulators suffer from.

The question then is, what would be the scenario after the Personal Data Protection Bill, 2019, comes into force?

Citizen-State Relationship

The citizen-state relationship with respect to personal data is unique from other power relations. Firstly, the State can legitimately extract information from its citizens without giving them any scope for negotiation. Moreover, most services of the State are not substitutable. This unilateral, non-negotiable and monopolistic extraction of data must be met with heightened care during its handling and usage.

Secondly, under the PDPB 2019, which purports[iii] to "…*provide for protection of the privacy of individual…"* and "…*create a relationship of trust between persons and entities processing the personal data…"* mandates fostering of trust and active protection of personal data.

Taking the foregoing in conjunction, the element of trust between state-citizen is heightened, primarily due to non-consensual extraction of data. However, this moral duty does not translate well into accountability without corresponding enforcement mechanisms.

While the Bill requires[iv] public institutions to implement necessary security safeguards, gaps in the Bill indicate that breaches will continue to take place. To understand the rate of incidence of data breaches and measures for its rectification requires technical competence and research which the author of this paper lacks. Rather, focus has been placed on the next consideration, i.e., mitigation of damage to the principal's rights through notification.

DATA BREACH NOTIFICATION

Under the Bill, a personal data breach which is likely to cause harm to any data principal must be notified to the Data Protection Authority (DPA).[v] Thereafter, the DPA can direct the entity to carry out remedial measures, publicise breach on its website and, most importantly, notify the affected data principals.[vi]

Consideration of Key Terms

The trigger term, 'personal data breach', has been defined[vii] as "*any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal".* The wide ambit of this definition is commendable, and globally compatible. Public institutions will no longer be able to shirk responsibility as with the Aadhaar breaches. On the contrary, however, Indian government's weak support for personal data in the face of this wide definition could motivate framing of rules to dilute this standard.

The second decisive factor in the process of notification is whether the breach is *"likely to cause harm to any data principal".*[viii] The definition of harm within the legislation is too broad to arrive at predictable decisions as of now, and the fact that it can be further moulded not by the DPA but the Union Government raises its own concerns. Essentially, though most breaches of personal data held with the State *prima facie* result in harm construed as per the foregoing broad definitions, the considerations enlarge the discretion available to the entity.

Lastly, subsequent to being notified, the DPA, after *"…taking into account the severity of the harm…"*[ix] and seeing whether any corrective action is required by the principal, determines whether the breach ought to be notified to the affected principals. Underlying the process of

subsequent notification to the data principal is the fact that the data principal is at the centre of data privacy laws. Accordingly, a principal has a very strong right to know.

POLICY AND REGULATORY ISSUES

While procedural aspects with respect to data breaches are same for public and private sector, there are additional factors that are at play when public sector breaches take place. Essentially, data breach notification by the State is laden with concerns over discretion, DPA's autonomy, perverse incentive and lack of effective redressal.

Discretion

The element of discretion at play occurs at two distinct points. First, when an entity must notify of a personal data breach to the DPA (initial notification), and second, when the DPA makes an assessment whether the breach is notifiable to the principal (subsequent notification).

1. *Pruning discretion*

Under GDPR, initial notification must be made unless the breach is unlikely to pose a risk to the rights of the principals.[x] This is different from the PDPB 2019, which triggers the initial notification only if the breach results in a likely risk. The framing of the provision under GDPR in effect makes breach notification mandatory, which can only be deviated from if entities are sure that the breach will not adversely affect the principals. [xi] In India, the condition for notification is that the entity who has suffered a breach must only notify if it is certain that the same will pose a risk to the principal. It is safe to assume that private entities would err on the side of caution, however, the same may not hold true for public entities in India.

2. *Objectivity*

Under Australia's Privacy Act, 1988, entities must employ an objective 'reasonable person' test.[xii] For a country which has had data privacy laws since 1975 and consistently updated them, Greenleaf notes that '*…enactment of a data breach notification scheme in 2017 [has been the] only positive step…'* in a while (Greenleaf 2019, 2). U.S.A.'s HIPAA[xiii] mandates publication of data breaches if the breach affects more than 500 people.[xiv] In an unusual approach, South Korea requires every breach to be notified to data principals,[xv] and only if a breach affects more

than 10,000 people, the entity must notify the Ministry and DPA. South Korea introduced this through subsequent amendments with the aim of securing GDPR-adequacy.

DPA-State Relationship

The DPA-State relation affects both stages of notification and is influenced by the following (albeit non-exhaustive) factors.

1. *Independence and agency of DPA*

Firstly, PDPB will potentially produce a skewed DPA Board due to the Selection Committee comprising exclusively[xvi] of executive bureaucrats along with failure to expressly incorporate independent members in DPA, board, and selection committee. A report by AccessNow (2018) had marked the hailed Srikrishna committee report envisioned DPA as lacking due to lack of independence and power, which makes one think of the gross inadequacy of the DPA under PDPB. Secondly, the Central govt has subsumed integral regulatory powers of the DPA. The DPA cannot notify laws that ought to be passed at the level of an independent regulator, as against by MeitY, since they include the power to notify sensitive personal data and significant data fiduciaries, both calling for a distanced and technocratic approach[xvii] (Dvara Research 2020; Greenleaf 2020). Lastly, adjudication officers are also under the 'command' of the executive as the government notifies the important aspects associated with them, such as appointment and employment conditions.[xviii]

2. *Perverse incentives*

As aforementioned, though procedural requirements are the same for public and private entities, the nature of relationship involves different variables. This is aptly described by Konisky & Teodoro (2016, 572),

what matters most when governments regulate governments are not the carrots and sticks available to regulators, but rather the regulated entity's political costs of compliance and political prospects for appeal against the regulator, and the regulator's political costs of penalizing a fellow government agency. Two important implications of this perspective are that government agencies are less likely than similarly situated private firms to comply with regulations, and that regulators are less likely to punish violations when they occur at publicly owned facilities

Economic theory suggests that penalties, bad publicity, notification costs, etc. would persuade entities to employ stricter safeguards. However, for most functions of the State this is inapplicable, as profit motive is never an incentive. Public choice theory would suggest that government would want exemption and laxity in application as it reduces accountability. It is a matter worth considering whether the DPA and State would collude to conjunctly escape accountability.

In such a situation constitutional and other legal enforcement mechanisms assume greater importance.

Recourse

1. *Compensation under PDPB*

a. *Adequate standards*

PDPB requires[xix] concerned entities to maintain *necessary* security safeguards. These includes steps to prevent unauthorised access and disclosure, and to use encryption systems.[xx] A principal can seek redressal under this provision.

b. *Negligent behaviour*

The Bill also provides[xxi] for compensation where data processors have acted in a negligent manner.

Data breach laws of South Korea and California, prescribe payment of 'statutory damages' (example: USD 1,000) notwithstanding proof of actual damage suffered (which will mostly be impossible to prove) (Greenleaf 2020).

Figure 1: Fines on State entities under GDPR (GDPR Enforcement Tracker)

Country	Authority	Date	Fine [€]	Controller/Processor	Quoted Art.	Type	Summary	Infos
Filter	Filter			government		Filter	Filter	
SWEDEN	Data Protection Authority of Sweden	2020-04-29	18,700	National Government Service Centre (NGSC)	Art. 33 GDPR, Art. 34 GDPR	Insufficient fulfilment of data breach notification obligations	The DPA's decision shows that it took almost five months for the company to notify the data subjects of a data breach and almost three months for the DPA to receive a notification of a data breach concerning an security lack of IT systems of the company.	link

NORWAY	Norwegian Supervisory Authority (Datatilsynet)	2020-05-03	134,000	Telenor Norge AS	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Fines for security breaches in a voice mailbox function.	link

c. Constitutional measures

With Adjudicating Officers possibly fearing reprisal due to the control of executive over them, other avenues for recourse are important to cover. The Supreme Court of India in *Puttuswamy*[xxii] held that the right of privacy is a fundamental right, accordingly, data breaches can possibly be (and should be) seen as a deprivation of right to life and liberty, as it does not stem from a procedure established by law.

RECOMMENDATIONS

'Principal' based approach: Right to know must always be respected and catered to

Since it is unlikely that the State would be scrutinised by the DPA, accountability can be facilitated by ensuring that all data breaches (as opposed to notified breaches) are recorded[xxiii] and open to the public. Citizens' right over their data and the opacity with which government operates creates a disconnect which can be corrected by this, as some data breaches though notifiable to the DPA, might still go un-notified to the data principal.

Common portal to check breaches

Considering the incidence of digital illiteracy and information asymmetry in India, it may be practically prudent to create a common portal for data principals to check the breaches that might have affected them. This can help streamline breach notifications to principals as well.

Notification fatigue

In lesser than 2 years, data protection authorities in the 28 EU states have received 160,000 data breach notifications (DLA Piper 2020), which amounts to 262 notification/day. Bear in mind that the EU's total population is 446 million and contains roughly 28 data protection authorities (European Union), as against a single data protection authority for 905 million Indians who fall within the ages of 15-64. This helps one appreciate the magnitude underlying

a single task of the DPA (breach notification). It is thus important to think in terms of decentralising this function of the DPA, possibly by setting up state-level breach 'registrars'.

CONCLUSION

Personal data breaches of public sector disproportionately burden affected citizens. Though PDPB will help by negating the scope to wiggle out of responsibility for data breaches, the institutional factors at play will possibly result in status quo being maintained. In order to combat this, greater accountability can be facilitated by pursuing open governance – wherein all data breaches, irrespective of notification, are recorded and open to public. This is important as this may be the only consideration pressurising the government to clean its shoddy practices, and a good parallel to market forces present in a competitive market.

BIBLIOGRAPHY

- AccessNow. 2018. *Assessing India's Proposed Data Protection Framework: What the Srikrishna Committee Could Learn From Europe's Experience.* AccessNow.
- DLA Piper. 2020. *Newsroom.* January 20. Accessed June 14, 2020. https://www.dlapiper.com/en/global/news/2020/01/114-million-in-fines-have-been-imposed-by-european-authorities-under-gdpr/.
- Dvara Research. 2020. *Initial Comments of Dvara Research on the Personal Data Protection Bill 2019.* Initial Comments, Dvara Research.
- European Union. n.d. *Living in the EU.* Accessed June 13, 2020. https://europa.eu/european-union/about-eu/figures/living_en#:~:text=The%20EU%20covers%20over%204,population%20after%20China%20and%20India.
- Faisal, Mohammad. 2020. *The Indian Express.* June 2. Accessed June 14, 2020. https://indianexpress.com/article/technology/tech-news-technology/govt-denies-data-breach-of-7-million-bhim-users-cybersecurity-firm-maintains-its-claim-6437656/.
- Froomkin, A. Michael. 2009. "Government Data Breaches." *Berkeley Technology Law Journal Vol. 24, No. 3* 1019-1059.
- n.d. *GDPR Enforcement Tracker.* Accessed June 14, 2020. https://www.enforcementtracker.com/.
- Greenleaf, Graham. 2019. "Australia Debates Tougher Privacy Regulation of Digital Platforms." *161 Privacy Laws & Business International Report* 17-19.
- Greenleaf, Graham. 2020. "India's Personal Data Protection Bill, 2019 Needs Closer Adherence To Global Standards." Submission to the Joint Parliamentary Committee .
- Greenleaf, Graham. 2018. "Submission to MeitY on Srikrishna Report and Bill."
- Indian Express. 2018. *The New Indian Express.* July 30. Accessed June 15, 2020. https://www.newindianexpress.com/nation/2018/jul/28/trai-chiefs-personal-details-leaked-after-he-shares-aadhaar-number-in-challenge-to-hackers-1850002.html.

- Information Commissioner's Office. 2019. *Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach.* July 9. Accessed June 13, 2020. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.
- Konisky, David M., and Manuel P. Teodoro. 2016. "When Governments Regulate Governments." *American Journal of Political Science, Vol. 60, No. 3 (J)* 559-574.
- Ranjan. 2020. *Madhya Pradesh app to track patients leaks personal data, taken offline.* May 11. Accessed June 12, 2020. https://www.hindustantimes.com/india-news/mp-app-to-track-patients-leaks-personal-data-taken-offline/story-WO7ATpaxOMDTsmUxSKduUO.html.
- Scroll.in. 2020. February 20. https://scroll.in/latest/953768/jharkhand-almost-90-of-deleted-ration-cards-belonged-to-real-households-finds-study.
- Sengupta, Abhik. 2020. *Gadgets360.* June 1. https://gadgets.ndtv.com/apps/news/bhim-site-data-breach-exposes-70-lakh-indian-aadhaar-bank-pan-information-vpnmentor-report-2238851.
- Vidyut. 2018. *Medianama.* April 13. Accessed June 10, 2020. https://www.medianama.com/2018/04/223-government-denies-data-breaches-and-leaks-describes-security-of-aadhaar-database/.
- World Economic Forum. 2019. *The Global Risks Report 2019: 14th Edition.* Insight Report, World Economic Forum.

REFERENCES

[i] *Shamnad Basheer vs. UIDAI and Ors*. W.P.(C) 5405/2018
[ii] Both of these breaches have resulted from technical incompetence, lax oversight and sheer recklessness.
[iii] Preamble, Personal Data Protection Bill, 2019
[iv] *Ibid*., §24
[v] *Ibid*. §25(1)
[vi] *Ibid*. §25(6)
[vii] *Ibid*. §2(29)
[viii] *Ibid*. §3(20)
[ix] *Ibid*. §§25(5)
[x] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, art 33(1)
[xi] Article 29 Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (WP250rev.01, 6 February 2018)
[xii] Privacy Act 1988 (AU), s. 26WGd
[xiii] Health Insurance Portability and Accountability Act (US)
[xiv] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402, 123 Stat 115 (2009)
[xv] Personal Information Protection Act, 2011 (KR), s. 34
[xvi] *Supra* note 3, §42(2)
[xvii] It is important to note that this may not pass the three-prong test laid down in *Justice K.S. Puttaswamy Vs. Union of India* (2017) 10 SCC 1
[xviii] *Supra* note 3, §62(2)
[xix] *Ibid.*, §24
[xx] Considering how easy it is so encrypting data, failure to do should attract severe punitive measures.
[xxi] *Supra* note 3, §64(1)
[xxii] *Justice K.S. Puttaswamy Vs. Union of India* (2017) 10 SCC 1
[xxiii] This is an express requirement under Article 35(5) of the GDPR. Working Party 29 recommends recording the reasoning for decisions taken in response to a breach.