MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

The Protection of Private Data in Japan under Duress

Arnab Dasgupta and Rohit Kumar Sharma

April 08, 2024

Summary

Japan's data protection framework faces significant challenges emerging from corporate structures as well as inadequate defences against human actors within the chain of data custody. Indian regulators can study and learn from the Japanese experience on the creation of a legal framework that takes due consideration of the norms of free enterprise while ensuring the safety and sanctity of personal data.

Introduction

Personal data is the next great key resource shaping the future of human evolution, as epitomised by the phrase 'data is the new oil'.[1] This understanding has driven countries and societies to begin thinking deeply about the implications of handing over private data to a corporation, government or other entity. Japan's status as a key United States ally as well as a developed economy makes it a strong player in the digital economy.

Recent string of incidents in the corporate domain have highlighted that Japan does not necessarily possess the strong safeguards seen elsewhere in the world to prevent data leakage from taking place. The Brief examines Japan's existing legal and policy frameworks and assesses the implications for the future of data security and private data protection in the country. It will be argued that Japan's data protection framework faces significant challenges emerging from corporate structures as well as inadequate defences against human actors within the chain of data custody.

The LINE-NAVER Data Breach

On 5 March 2024, the Ministry of Internal Affairs and Telecommunications issued administrative guidance (*gyōsei shidō*) to social media entity LINE Yahoo! Corporation after it discovered a breach in the cloud services it had been subcontracting from Korean social media entity NAVER Korea.[2] NAVER's servers, containing LINE's data on Japanese consumers, were found to be inadequately protected against unauthorised access, and a malware infection in one of NAVER's subcontractors' servers allowed external actors to access Japanese consumers' data. The investigation found that 'external actors' had been able to access NAVER Cloud's servers, which in turn gave them access to LINE's data.

It is pertinent to observe here that LINE Yahoo! has been involved in a string of unauthorised data leakages in the past as well. In 2021, a Chinese subcontractor of the company was able to access user data in Japan and in August 2023, the company was found to be sharing user location information to NAVER, which in turn was giving its subcontractors access to its data. As a result, the Minister for Internal Affairs in a press conference reported that the ministry has placed LINE! Yahoo under a year-long watch list, after which further actions would be considered if no improvements were observed.[3]

---

[1] **"The World's Most Valuable Resource is No Longer Oil, But Data"**, *The Economist*, 6 May 2017.

[2] **"LINE ヤフー株式会社に対する通信の秘密の保護及びサイバーセキュリティの確保に係る措置（指導）" [Measures (Guidance) for Protecting the Confidentiality of Communications and Ensuring Cybersecurity for LINE Yahoo! Corporation]**, 総務省 (Ministry of Internal Affairs and Telecommunications), 5 March 2024. Also see **"Japan Ministry Urges Line App Operator to Bolster Data Protection"**, *Kyodo News*, 5 March 2024.

[3] **"松本総務大臣閣議後記者会見の概要" (Summary of Minister of Internal Affairs and Communications Matsumoto's Post-Cabinet Press Conference)**, 総務省 (Ministry of Internal Affairs and Communications), 5 March 2024.

NTT West Data Leakage

Nippon Telegraph and Telephone (NTT) Corporation West, the branch of the semi-private national carrier handling operations in Western Japan, also came under the scanner after a former temporary worker at the company was arrested in January 2024. The staffer had reportedly copied over 9 million pieces of customer data onto a USB stick from another subsidiary using his access to NTT West's internal network. The subsidiary targeted by the former employee handled call centre operations for NTT Corporation, and the data allegedly taken covered over 10 years of names, telephone numbers and addresses.

Once again, this was not the first time NTT West has been hit by cases linked to unauthorised access of data. In April 2022, a client of the telecom giant reportedly warned of a suspected leak of information at NTT's end. However, NTT West apparently conducted a shoddy investigation after which it declared the matter settled, only to be outed in October 2023 after the client company approached the police to request an investigation. As the January incident came to light, NTT West's president Masaaki Moribayashi announced that he would step down from his post to take moral responsibility. The company has committed to spend over 10 billion Japanese yen in the following three years in order to boost its network security and detect irregularities.[4]

Legal Frameworks for Data Protection

In both instances, the unauthorised access to user's personal data is under scrutiny, leading to questions being raised about whether the affected parties have any legal recourse under current Japanese law. Also, what obligations do businesses have under the law to safeguard such data?

In Japan, the Act on the Protection of Personal Information (APPI), 2003 is the principal data protection law. After its adoption, it has undergone periodic amendments, the latest one being in 2020. One of the key steps under the APPI was the establishment of the Personal Information Protection Commission (PPC) as the primary regulator responsible for the implementation of the legislation. Under the law, the PPC is entrusted with the following responsibilities:[5]

- Promotion of basic policy
- Supervision
- Mediation of complaints

[4] **"NTT West: Be Aware of Responsibility for Handling Personal Information"**, Editorial, *The Japan News by the Yomiuri Shimbun*, 6 March 2024.

[5] **"Roles and Responsibilities"**, Personal Information Protection Commission, Japan.

- Public relations
- International cooperation
- Reporting to Diet

Given the wide range of responsibilities, the PPC plays a vital role in ensuring robust privacy security frameworks across businesses along with sectoral regulators, if any. For the purpose of the law, businesses dealing with personal data are called personal information controllers (PIC), while the individuals or the customers are referred to as data subject. The act also outlines the broader duties and obligations of PICs and the rights of data subjects.

LINE/NAVER Korea Data Leakage

To examine the applicability of the APPI in this case, it is important to determine the nature of cooperation between the LINE and NAVER. According to the administrative guidance, factors that contributed to the incident included strong dependence of the LINE on NAVER regarding system and network configuration, as well as inefficient safety control measures. The ministry also advised the Japanese entity to improve its operations by reviewing its capital partnership with NAVER as it is under "considerable influence" from the South Korea-based entity.[6] As reported, NAVER's cloud has "extensive access" to LINE's environment, making it easy to access data stored using NAVER's network.[7] On this, the ministry underlined the need for both services to implement their own authentication tool instead of relying on the shared directory.

These operational arrangements position NAVER as a data processor in the case, entrusting the entities with certain obligations under the law. According to the law, LINE has a legal obligation to conduct appropriate and necessary supervision over NAVER, which is a data processor.[8] In fact, the PPC guidelines also emphasise the importance of measures that involve visibility and supervising the processing of personal data by the outsourcing provider.[9] However, neither the APPI nor any related regulations impose direct obligations on data processors.

There is also a need to evaluate whether such operational arrangements were serving any of the key principles of any data protection regime, such as purpose limitation and data minimisation. These principles are at the heart of the General Data Protection Regulation (GDPR), which has partially, if not completely, inspired the

[6] **"Japan Ministry Urges Line App Operator to Bolster Data Protection"**, no. 2.

[7] Simon Sharwood, **"Japan Orders Local Giants LINE and NAVER to Disentangle their Tech Stacks"**, *The Register,* 6 March 2024.

[8] **"A Guide to Data Protection in Japan"**, Atsumi & Sakai, September 2020.

[9] Hiroyuki Tanaka, Noboru Kitayama and Ryoko Matsumoto, **"Japan: Data Privacy Comparative Guide"**, *mondaq*, 14 March 2023.

data protection regime in Japan. Purpose limitation entails the collection of personal data for 'specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes'.[10] Similarly, data minimisation means the collection of personal data that is 'adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed'.[11] Clearly, these principles were not adhered to in the present case, as LINE user credentials serve no purpose to NAVER's infrastructure. Furthermore, administrative guidelines also noted that LINE entrusted security management to NAVER, amounting to the breach of duty under the law.

NTT West Data Leakage

In this case, the leak is believed to have taken place over a decade, and the management ignored warnings on multiple occasions.[12] The threat actor in the case, a former employee of the company, sold the leaked data to a third party, which included information such as addresses, names and phone numbers of customers. Furthermore, the leaked data also contained credit card information in some cases. The fact that a temporary employee had access to such data raises concerns about the company's data security framework, which clearly failed to prevent data breaches. It also prompts questions about data security practices, such as implementing stringent controls over user credentials and access privileges to prevent unauthorised access and safeguard sensitive information. Following the widespread publicity of the breach, the communications ministry has also ordered NTT West to revise its contracts with employment agencies.

As far as legal remedies for victims are concerned, despite no evidence of secondary harm to users resulting from the leak, courts in Japan now recognise the private right of action for a data breach involving personal information.[13] In fact, the Supreme Court of Japan acknowledges that the plaintiff's mental distress stemming from the data breach constitutes compensable harm. On multiple occasions, it has been observed that PICs have often voluntarily offered compensation to affected parties to forestall any proceedings. Though no claimants have come forward thus far in the current case, it is not a sign of mature business practice to prefer paying compensation over strengthening data protection rules.

Many sector-specific regulations authorise relevant regulators to enforce rules by notifying business improvement orders following a cyber incident or, in the worst

[10] **"Article 5- Principles Relating to Processing of Personal Data"**, GDPR.

[11] Ibid.

[12] Laura Dobberstein, **"NTT Boss Takes Early Retirement to Atone for Data Leak"**, *The Register,* 1 March 2024.

[13] Andrew M. Pardieck, **"Privacy Matters: Data Breach Litigation in Japan"**, *Washington International Law Journal,* Vol. 33, No. 1, pp. 1–43.

case, render business suspension orders. Following a breach, the PPC is also authorised to issue advice for improvement. If the PIC fails to comply with such advice, the PPC may escalate by issuing an order of improvement. Failure to comply with an order for improvement could also be grounds for criminal imprisonment.[14] As NTT West has been served with an order for improvement, it is too early to say how conditions will improve in the future.

To ensure that appropriate data protection measures are in place, the PICs are also required to remain vigilant of malicious insider threats, as exemplified in the case of NTT West. User behaviour monitoring is critical to look for an anomaly to pre-emptively identify an insider threat. However, it is equally important to strike a balance between these practices and privacy concerns. To enable a better understanding of data management, the PPC released a data mapping toolkit for private entities.[15] The toolkit can also help the PICs with regulatory compliance, data governance and security initiatives within the organisation, though it is unknown whether NTT West applies the toolkit in its internal systems.

Conclusion

In an age where the free flow of data is at the root of global commerce, even a state with high capacity like Japan needs to wrestle with the creation of a legal framework that takes due consideration of norms of free enterprise while ensuring the safety and sanctity of the data shared by its 127 million citizens. The cases discussed above throw up interesting—and complicated—questions about Japan's struggle to implement the same.

As the Diet enters into discussions on the amendment to the Designated Secrets Protection Law 2014 which will seek to protect economic secrets behind a firewall of security clearances,[16] it is an opportune moment for it to also consider how it can best protect the private data of Japanese citizens from a range of threats emerging from within and outside its economic actors. It is also a good opportunity for India, currently in the throes of devising its own legislation on data protection, to learn from Japan's struggle, particularly concerning delineation of wider obligations for data processors and enactment of stringent penalties in the event of a data breach involving sensitive personal data.

[14] **"A Guide to Data Protection in Japan"**, no. 8, p.15.

[15] **"Japan's PIPC Introduces Data Mapping Tool"**, International Association of Privacy Professional (IAPP), 18 October 2022.

[16] **"2nd Half of Diet Session: It Is Time to Deliver Results to Dispel Distrust in Politics"**, Editorial, *The Japan News by the Yomiuri Shimbun*, 30 March 2024.

About the Author

Dr. Arnab Dasgupta is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses