Internet and Mobile Association of India

IAMAI Submission on Integration of E-commerce Companies Database with NATGRID

The Internet and Mobile Association of India ("IAMAI") is a not-for-profit industry body and we play a key role in ensuring the growth and sustainability of the digital industry.

National Intelligence Grid (NATGRID) has proposed connecting databases from various Providing Organizations (POs) and leverage Information Technology to access, collate, analyse, correlate, predict and provide speedy dissemination of information to Law Enforcement and Intelligence agencies.

The Department for Promotion of Industry and Internal Trade (DPIIT) organised a consultation on 13th April 2021 with e-commerce companies to discuss the integration of e-commerce platforms database with the National Intelligence Grid (NATGRID). We would like to thank DPIIT for inviting IAMAI for the consultation. Meeting focused on the data needs of Law Enforcement and Intelligence Agencies from e-Commerce platforms, requirement of NATGRID from the e-Commerce Platforms in the capacity of Providing Organizations (POs) and modalities on data sharing.

NATGRID has recently shared a note defining the nature of requests, process of integration and legal part with our members.

Members are fully committed to support the government initiative to strengthen national security. However, they have few queries and concerns regarding this initiative. They have approached IAMAI with their concerns on operational, legal, and technical aspects of the integration. IAMAI on behalf of its members would like to share key concerns and queries for the e-commerce industry on the proposed integration of the e-commerce database with the NATGRID.

IAMAI Submission

Nature of e-commerce data

E-commerce platforms, being multi-sided platforms involve data generation of multiple parties - buyers, sellers, logistics providers and the platform itself. Generally, e-commerce data, (data pertaining to business activities of sale, marketing, distribution of goods or provision of services through the Internet or other information networks) is not sensitive data which can have an impact on national security. Sharing of consumer-specific data without the explicit consent of the consumers (outside the ambit of applicable law) is likely to run contrary to the privacy rights of the consumers. The overarching objective of NATGRID is to combat terrorism and internal security threats.[1] While e-commerce entities are committed to assist the government in relation to matters relating to national security, the likelihood of need for data sharing is minimal, which in any event these entities are carrying out under applicable law, such as in relation to sale of dangerous substances.

[1] https://www.mha.gov.in/MHA1/Par2017/pdfs/par2013-pdfs/ls-260213/352.pdf

Additionally, the data on purchasing trends, user patterns, etc, is an extremely valuable trade secret and are proprietary to several e-commerce entities. The operation and maintenance of the technological platform is extremely resource and cost – intensive and sharing of such data threatens the free market and the economic autonomy of the private businesses. The disclosure of database which in an event if misused/leaked would have very adverse consequences on the business of e-commerce entities and it may happen that it would allow the buyer and seller to bypass the e-commerce entity and directly conduct a transaction between each other in addition to the risks posed from access of such data by the competitors. Currently, members lack clarity on the specific safeguards by NATGRID on protecting the proprietary rights and commercial value of such data.

Legal basis for data sharing with NATGRID

Historically, data sharing mechanisms (including in telecommunications, insurance and banking regulations) are rooted in regulations or mandatory license agreements which specify the data that is to be necessarily shared with the authorities. E-commerce entities are currently not licensed and therefore, no similar legal framework for data transfers exists for e-commerce entities. The e-commerce entities are subject to multiple laws and regulations (from the Consumer Protection Act, 2019 to the PDP Bill, CrPC, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021) which include data sharing obligations. E-commerce entities can only share data pursuant to provisions of the law that they are subject to and data sharing outside the statutory framework can be challenged before the courts. Further, the e-commerce entities are duty bound towards their customers and the obligations stemming from their privacy policies as well as their terms and conditions. Any request for data / information from NATGRID should be under the existing regulatory regime applicable to e-commerce entities.

NATGRID and IT Rules

The Information Technology Act, 2000 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (IT Rules) authorise specific Government agencies to intercept, monitor and decrypt information stored in a computer resource. The Government has **not** notified NATGRID as an agency authorised under the IT Rules. The Government has also told the Delhi High Court that no blanket permission has been granted to any agency for interception or monitoring or decryption of any messages or information under the NATGRID surveillance programmes.[2]

Moreover, the scope of data dealt with by NATGRID can be very wide and may include the data of European Union (**EU**) residents. Post the decision of the Court of Justice of the European Union in Schrems II, surveillance undertaken by NATGRID which lacks a legal framework and an oversight mechanism is likely to impact transfer of data to Indian processors and is likely to impact the outsourcing industry in India. To meet these requirements under EU laws, it will be necessary for regulatory access to data to be grounded in clear legislative backing and oversight.

[2] https://legal.economictimes.indiatimes.com/news/industry/no-blanket-permission-given-for-surveillance-under-netra-natgrid-centre-to-hc/80719875

Lack of clarity on the scope of the NATGRID framework

Under NATGRID MoUs private parties are required to provide data as per the framework of NATGRID, which has not been specified yet. This means that anyone entering into the MoU with NATGRID at this point of time will not have a clear understanding of the mechanisms under it. The e-commerce entities will not be aware of any safeguards within the NATGRID framework, and will not be able to undertake the efforts involved in relation to being part of the NATGRID framework.

Furthermore, additional details are required on what would be the nature of the safeguards adopted in the event such an integration with NATGRID does take place and which party would be responsible for the safety of the data being shared. Such data exchanges can become increasingly exposed to cyber-attacks and breaches and adequate safety protocols will need to be put in place to safeguard the proposed integration mechanism.

Limitation of Liability

Given the lack of statutory authority behind NATGRID's requests for data, e-commerce entities are currently unlikely to be able to provide the data required without incurring legal liability towards the data principals. There is a conflict with basic privacy laws that protect customer confidential information from unwanted / unjustified disclosure without a regulatory/judicial order. Further, any data requests will need to account for the liability incurred by the e-commerce entities and how that may be mitigated, until a regulatory framework is created in this regard. E-Commerce companies will be unable to justify the risk undertaken in assisting with data transfers without any statutory reasoning or some form of indemnity/limitation of liability (such that they are not held liable for data that has been transferred by NATGRID) being in place. The government should consider a legal mechanism which allows e-commerce entities to protect themselves legally while assisting with data transfers.

Queries:

1. Given the possible passing of the Personal Data Protection Bill, 2019, is there any statutory backing envisaged for the operations of NATGRID?
2. Kindly provide us with the copy of the MoU and the Standard Operating Procedure.
3. Will the request from User Agencies contain information regarding the authorization of the user agency to access the data requested? How will provider organization exercise control on information being pulled out and how would law of proportionality be applied?
4. If a nodal officer is required to be appointed to interface with NATGRID, which law will govern the obligations/liabilities of such nodal officer?
5. Will data of foreigners be treated differently from data of Indian nationals with regards to the data requests?
6. We assume that each request from an authorized User Agency will be backed by a valid legal mandate and the specifics of the legal mandate will be disclosed to us. Also, we have an obligation to respond only once we are satisfied that authorization is valid. Kindly confirm.
7. Will NATGRID issue a legal order/notification directing all e-commerce entities for such data sharing or will there be selected e-commerce entities? If latter, what will be the selection criteria?

8. Many large retailers are selling online and may have more data than some of the ecommerce companies approached by NATGRID. Are such retail companies that are also selling online approached for such integration? Moreover, FMCG or retail have similar customer data and transactions so will those be covered under this initiative?
9. How will the data provider be required to integrate their systems with the NATGRID framework? If this will be achieved through API integration, then kindly provide technical specifications.
10. Is there a requirement of keeping data in certain formats or using certain technological processes?
11. Will the query response feature of NATGRID IT framework work on a real-time basis? Will the data providers be provided an opportunity to review each request made by a User Agency? Will there be a distinct processes based on the sensitivity of the data?
12. What will be the pre-defined set of use cases for e-commerce providers for providing access to data? How will these be determined?
13. What are the security measures currently in place for storage of data? How will NATGRID protect the proprietary data which may be transmitted under the data transfer framework?
14. What will be NATGRID's data security protocols for the PII/SPDI that platforms are likely to share under this proposal?
15. In the event of a data breach or loss of commercially sensitive/personal data, what remedies are available to the data providers and the customers?
16. Will request for historical data be time bound and within a specific range?
17. We note that NATGRID is also developing capabilities to analyse the data. Will NATGRID be storing the data transmitted? Will this storage and analysis of data by NATGRID be reflected in the MoUs?
18. What remedies are available in case the data provider does not have a particular set of data? e.g. KYC information for buyers.
19. Can e-commerce entities revise/delete shared data especially if they do not have back-to-back right from customer to store the data forever? Customer can request e-commerce entity for data deletion – how will NATGRID handle this request?

We reiterate that we stand shoulder to shoulder with the Government of India on protecting the national security of the country. We are grateful for this opportunity to submit our views on the matter and we humbly request the Government to provide due consideration to our concerns and queries voiced in this submission.