The world is going digital, and the marketing function is at the forefront of this digital revolution. To be more effective, good marketing relies on detailed and accurate customer data for targeted campaigns. This approach is key to the marketing efforts of e-commerce companies, who deal with faceless customers. And companies, not surprisingly, are eager to collect vast troves of customer data. As organisations seek to leverage data generated using the Internet of things (IoT), artificial intelligence (AI) and predictive analytics, it is important that they consider the impact that the European Union’s General Data Protection Regulation (GDPR) or India’s Data Protection Bill on the envisioned returns to their investments.¹

For retailers, India is a highly aspirational consumer market as it represents a growing middle-class population and a large young population (the working age group of 15–59 years of age), i.e. approximately 62.5% of the total population.² This favourable demographic dividend – together with an increasing smartphone user base – is set to give a fresh stimulus to the adoption and growth of e-commerce in India. The increasing smartphone penetration not only supports enhanced and inexpensive data access, but also helps in achieving the Government of India’s vision of building a digital India.³

One essential enabler for the digital ecosystem to be sustainable, feasible and desirable is the use of personal data to customise each transaction or interaction with the consumer. Driven by the value that hyper-personalised shopping and marketing offers, many consumer-facing companies are focusing on gathering data and insights to gain a competitive edge.

³ https://www.pwc.in/assets/pdfs/industries/technology/techworld-may-2018.pdf
However, the approaches undertaken by organisations to gather, process and secure consumer data differ. Non-standardised methods of gathering data result in an increased number of cyberattacks and incidents, as highlighted by a report by the Indian Computer Emergency Response Team (CERT-In). The report found a significant rise of 292% in cyber incidents from 2017 to 2018. Cyber incidents result in organisations suffering from not only monetary losses, but regulatory fines and reputational damage as well. Growing incidence of cyberattacks and data breaches has resulted in consumers becoming increasingly concerned about undue usage of data without their consent or approval. Breaches and hacks are potential setbacks for big brands that might lead to loss of customers to their rivals.

The constant discussion around misuse of data, coupled with breach-related headlines in the media, has triggered a movement for the protection of consumer data privacy rights. This brings us to an important question – where and how should companies draw the line in order ensure they are being non-intrusive and are able to guarantee a desirable degree of customer privacy even as they enrich transactions and the customer experience?

India is seeking to address these privacy challenges through a new regulation, namely the Personal Data Protection Bill, 2019. The bill aims to ensure protection of personal data handled by organisations, including all e-commerce players. For Indian e-commerce giants, the bill will significantly transform the way personal information is collected, stored and processed.

Organisations collect various types of personal data from customers, both directly and indirectly. This includes personal, transactional and session details captured while making online transactions. Fitness trackers and watches collect data on customer health, made-to-measure apparel retailers collect data about body measurements, banks and insurance companies accumulate financial information, credit card issuers store voice patterns of customers – the list is endless. In such a business environment where data gathering is widespread, what initial steps should e-commerce companies take to ensure the safety of customer data?
First, a company should establish a data strategy and outline goals for data collection, management and use. A key step in the data privacy compliance journey for organisations is to have a clear and accurate understanding of personal data and maintain records of the end-to-end lifecycle of the data. Organisations must establish the purpose and objective of data collection, mechanism for data collection, identification of critical data and garbage data, storage and processing of personal data, and access management controls around data. These steps can help e-commerce organisations understand the personal data landscape and accordingly take necessary actions to safeguard the personal information collected from consumers. Organisations should identify and make a repository of the extent of personal data collected, stored or processed and update it on a periodic basis.

They should consider a risk-based approach to data privacy by creating a data privacy framework, which can be applied consistently across all functions and geographies to minimise complexity and maximise data protection. To effectively govern privacy exposure, management should seek to understand the possible consequences of a breach of data privacy for the organisation’s current position. Factoring in an organisation’s plans like the adoption of latest technologies, launch of new products, expansion into new markets and acquisition of other companies is critical for the executive team. But these activities might expose organisations to new and potential data privacy risks. The management needs to consider the privacy risks arising from such actions.

Such a risk-based approach would help organisations build and enforce the right checks and balances based on risk exposure, and in a flexible and agile manner. For an e-commerce organisation adopting the concept of big data, data protection and storage become key risks – which need to be highlighted and addressed accordingly. An e-commerce organisation’s risk assessment exercise must aim at breaking down and examining the risks to data during all the stages of data lifecycle (collection, usage, sharing, storage and deletion).

The business model of e-commerce companies is built upon the concept of profiling and target-based marketing to offer various products and schemes to individual customers. This necessitates the collection, analysis and use of large amounts of personal data of potential customers. Adequate protection of personal data becomes a must for such organisations. E-commerce organisations should implement appropriate technical- and enterprise-level safeguards to ensure that personal data is protected from any kind of threat, both from outside and inside. The board of directors should ask the management what the organisation is doing to comply with data privacy laws and whether they have a strong data privacy compliance programme in place to regularly monitor compliance. The board must ensure that the management has established legitimate procedures and controls to mitigate the risk to personal data.

In order to effectively manage and protect data, privacy must be built into the e-commerce platform and services by design and should be integrated into the software development lifecycle (SDLC). Only that personal information should be collected which is absolutely necessary for processing, providing seamless customer experience and minimising compliance risk.

In today’s highly digitalised world, third-party vendors offer organisations the opportunity to reduce product prices and delivery time. This allows businesses to offer excellent customer experiences and drive profits forward, but often at the cost of new risks. E-commerce players must display responsibility and accountability by showcasing strong and robust governance controls over third parties. Organisations must evaluate the security and privacy practices of all third parties, maintain inventories of all third parties with whom business- or customer-related information is shared, frequently review third-party management policies and processes, implement a robust third-party risk management programme, get visibility into third or nth parties with whom the organisation does not have a direct relationship, and get notifications from third parties when data is shared with nth parties.


3 | Controlling the privacy risks of online shopping
Conclusion

Data privacy is a burning issue for both customers and organisations. With each high-profile breach that makes headlines, consumers increasingly worry about whether their personal information is secure and being used properly. Organisations are also on edge as recent disclosures about government and corporate practices have pushed privacy to the forefront. By considering only what privacy safeguards can prevent – customer loss, brand damage, fines, litigation – business leaders miss out on what the right strategy can enable. Customer data is one of the most valuable assets. Companies that not only protect that data but also empower customers to have a say in its use build trust in their privacy programmes – and in their business.

In conclusion, e-commerce players must identify the extent of personal data collected and processed, assess the privacy risks associated with the same and integrate the necessary countermeasures into their existing enterprise risk management framework.