Risk based approach to data privacy
"Risk based approach to data privacy can help businesses manage global data privacy risks, apply, calibrate and enforce controls based on the risk exposure, in a manner that is flexible and more agile."

Personal information has huge potential to create economic and social value for both the customers and the organizations who serve them. The ability of the organizations to acquire and use personal information to launch new products, services and enhancing customer experience has increased immensely with innovative use of technology; however, it also increases the risk to the privacy of personal information.

Ensuring data privacy through every stage of information life cycle (collection, storage, processing, retention, sharing and disposal) has become very critical for organizations to stay relevant. Evidently there is a need for organizations to take a risk based approach to data privacy and protect personal information to maintain business competitive edge. Risk based approach to privacy is a process that allows organizations to identify potential high risks and focus their efforts towards high risk areas. This white paper explores a risk based approach to privacy with the intention of helping the organizations to manage data privacy effectively.

New horizons – new risks

Technology is growing in a rapid manner to enable business growth and the amount of data is proliferating at an exponential rate. The risks to privacy of personal information has been and will continue to be affected by automation and adoption of new technologies in every industry and every geography and across all functions.
The key trends that are altering the threat landscape include adoption of Cloud, expanding usage of mobile applications, social media, location based services, machine to machine communications, Internet of Things, mobile advertising, wearable devices, etc. With the privacy regulations enforcing principles like ‘Right to be forgotten’, ‘Privacy by Design’, ‘Data Portability’, etc., a checkbox approach to data privacy is not sustainable. A paradigm shift in privacy mindset is necessary to mitigate these risks arising due to usage of these disruptive technologies.

| **Big Data Analytics** | • Customer data is used for analytics to provide high quality customer experience and to anticipate increases in revenues & profits.  
• Data privacy concerns around data analytics and processing of customer data for analytics as the potential for abuse of data is significant. |
|------------------------|--------------------------------------------------------------------------------------------------|
| **Cloud Adoption**     | • Organizations are moving the customer information beyond the secure perimeter of the organization and accessing it via diverse devices and locations.  
• This introduces compliance issues due to cross border data privacy regulations. |
| **Smart Metering**     | • Smart meters offer significant benefits to consumers by giving them more information and control over their energy usage.  
• Secondary use of energy consumption data results in intrusion of personal behavior patterns. |
| **Mobility**           | • Organizations are adopting mobile technology to provide convenience to its customers.  
• Lack of data privacy controls to protect privacy and client data confidentiality shall result in data breach and violation of the data privacy regulations. |
| **Location Data**      | • Location based services provide great value to consumers and businesses like targeted advertising, etc.  
• Intrusive identification of behaviour patterns, aggregation, distribution or selling of individual’s location or location profile derived from location data. |
| **Internet of Things (IoT)** | • IoT is a network of interconnected everyday objects like mobile phones, wearable devices, washing machines, coffee makers, etc., for data processing to enable a smart environment to improve interaction.  
• Objects can reveal information about individuals. |

Figure 1: New Technology Adoption & New Business Models Bring Privacy Risks
Data privacy challenges

All the data privacy acts provide only guidelines for privacy compliance and do not contain any control framework or standards for ensuring compliance. The privacy laws are based on principles; hence, they are subject to interpretation, leaving it both to organizations to decide on how to implement these principles, and to regulators on how to interpret and impose the law.

Challenges in Data Processing
- Can the data collected for specified purpose be used subsequently for creating economic and social value?
- How to gain new insights and make better decisions, and to do so in a manner that protects individual privacy?

Data - New Currency of Global Economy
- 2.5 quintillion bytes of data are created each day
- 6 billion people in the world population have mobile phones that generate trillions of transactions every day

Challengers in Data Collection
- How to notify individuals when data is passively collected from machine to machine transactions?
- How to provide individuals with new ways to exercise choice and control, especially where data uses most affect them?

Challengers in Data Storage
- Is there a process to limit the personal information storage?
- How to implement controls based on criticality of risk when there is lack of guidance from regulators?
- What mechanisms can be employed to control the proliferation of personal information?

Figure 2: Current State of Data Privacy in a Hyper Connected Ecosystem
Data privacy challenges

Today there is no standard methodology to implement privacy controls and comply with the privacy principles obligations that are imposed by the regulators. To comply with the privacy principles, each organization has to derive their own methodology for achieving compliance. The privacy compliance becomes complicated when an organization services customers across multiple geographies where multiple country regulations come into the picture.

Risk based approach would bridge the gap between the privacy principles on one hand, and privacy controls on the other, using a methodology that would help organizations to apply, calibrate and implement privacy requirements appropriately and effectively. A risk based approach to data privacy can help organizations enforce controls based on the risk exposure, in a manner that is flexible and more agile.

Proactive approach to data privacy

Organizations must take a proactive approach to data privacy by creating a data privacy standard and privacy control framework, which can be applied consistently across all functions and geographies to minimize complexity and maximize data protection. Such a framework must provide guidance on what constitutes personal data, what are the requirements for personal data collection, process of managing consent, rules for accessing and using personal data, how to classify and protect personal data, implement the right set of processes and controls based on the risk. This should be followed by creating a data privacy strategy that would help the organizations to manage the privacy of data life cycle right from data collection, storage to disposal.
Identify the assets, business processes, type of PII being collected, stored, processed & transferred by the organization. Develop a detailed threat profile by considering the various threat actors, threat vectors and the threat impacts to calculate the risk level.

Assess your privacy risk posture

Conduct a PIA for new projects, new application development, existing critical applications that stores or process PII & also to changes to business processes. Automate PIA using GRC tools.

Ongoing privacy impact assessment

Embed privacy as a central element of value proposition. Build a privacyware organization by conducting privacy trainings, awareness campaigns, and by conducting data privacy events.

Build a privacy aware culture

Privacy must be built into products and services by design and by default. Integrate privacy into SDLC lifecycle. Collect data only that which is absolutely needed for processing, to minimize compliance risk and increase customer trust in the product and services. Provide notice, choice and transparency to customer.

Build product and services with privacy mind

Look for opportunities to drive value from privacy. Bring economic and social value to customers by enabling optimal use for personal information.

Embrace privacy as a core business value

Organizations that respect the customer privacy, and promote trust and transparency are most successful in the industry. Use privacy as a differentiator to gain competitive edge in the industry.

Make privacy a brand differentiator

Figure 3: Data Privacy Strategy
The road ahead

Data is becoming a fundamental asset in the digital transformation of economies. The increasing use of disruptive technologies has created an unprecedented flow of personal information. Data subjects are becoming increasingly aware of their privacy rights and are rightfully demanding more control over how their personal information is used, shared, and assurances that the privacy of their personal data will be protected.

Organizations across industries and geographies continue to be challenged by disruptive technologies. The boundaries of the digital world are not fully established. The data breaches continue to make headlines and data privacy has become a focal point of discussions in boardroom. Data breaches can do irreparable harm to the organizations brand equity, credibility, trust and customer relationship. It is apparent that there is no one-size-fits-all solution that is available to comply with the ever evolving data privacy regulations. There is a need for organizations to take a comprehensive risk based approach to privacy where globally defined privacy risks are identified and countermeasures are built. This would be far more effective and more likely to respond to cross-border requirements.

About the author

Ramkumar Narayanan is a Senior Practice Manager for Wipro’s Cybersecurity & Risk Services (CRS) business. He heads the data privacy and data security governance practice within CRS, and is currently responsible for making Wipro’s customers succeed in their data privacy and security journey.

He can be reached at ramkumar.narayanan@wipro.com
Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have a dedicated workforce of over 170,000, serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at info@wipro.com