WIPRO
Applying Thought

Privacy is for Safekeeping

Accuracy, Storage and Disclosure of Personal Data

Manohar Ganshani
Head Governance Risk & Compliance Practice
Wipro Consulting Services

Table of Contents

Accuracy, Storage and Disclosure of Personal Data

Telcos across markets are called upon to strengthen their privacy protection standards in the wake of increasing legal compliance burden and customer awareness.

In most developed nations, privacy – both information and data are regulated by law. Many countries have specific privacy acts that regulate how government and private organizations collect, use/process and disclose personal information. These laws also provide individuals with the right to access the information about them that is stored by organizations and the right to request that any erroneous information be corrected.

Unlawful storage of personal data, storage of inaccurate personal data and the abuse or unauthorized disclosure of such data is considered a violation of privacy in some European countries and the United States. User awareness around privacy is very high in these countries. In 2010 Google had to turn in/off Wi-Fi data collected by its Street View cars after privacy concerns were raised in Germany and some other countries. While it is considered perfectly normal in some countries like India for someone to ask for another person's salary, date of birth and other such personal information, such questions would be completely outside the boundaries of propriety, and the law, in many Western countries.

This paper dwells upon some fundamental issues around privacy and takes a look at the telecom sector as a specific case. However, the essence of the discussion here applies to most other sectors.

Personal information or personally identifiable information (PII) is something that helps to identify an individual or directly points to a person's attributes. This 'something' may be a telephone number or an email address or anything apart from the obvious name of the individual. So, first and foremost, it is necessary to define what constitutes the PII of an individual - a consumer, an employee, a contractor associated with your organization, or anyone else.

Next, privacy requirements should cover information and data. Information and data are frequently used interchangeably. Information denotes processed data and hence is more clear, useful and contextual. Data is the raw element lying in the technology system (it could be anywhere) which requires crunching to make it more meaningful and actionable. Therefore, an information privacy program would cover the entire information management system and communication channels, with data protection treatment within the technology ecosystem. As a matter of fact, we often see that organizations have multiple policies – information security policy, information privacy policy and online privacy policy – to cover all possible avenues of privacy treatment.

Privacy vs. Confidentiality

There are two schools of thought here. First, privacy is covered under the confidentiality aspect of the security triad and is governed by the classification of information. This makes confidentiality a bigger umbrella under which privacy requirements are addressed and remains the responsibility of the chief security officer.

The second school of thought suggests that confidentiality is an extension of privacy. This school argues for protecting identifiable private information by making its access and disclosure strictly governed by an agreement with the person whose information is involved. In other words, privacy concerns people (right to personal information) and confidentiality concerns data (the way secrecy of personal information is managed). Thus, in some organizations a separate position is established for dealing with privacy – to supervise the application of the privacy policy against a continuously changing regulatory landscape.

Indian Telecom Scenario

The Indian telecom industry is being discussed here as it has been the fastest growing industry in India over the last decade, and has attained maturity, alignment with global practices and regulatory compliance very quickly.

Take a look at the telecom regulatory landscape below:

- ## IT Act (Amendment) 2008:
  - Section 43 A of the ITA 2008 necessitates that corporate bodies protect all personal data and information they possess, deal with or handle in a computer resource. If an enterprise is negligent in implementing a reasonable information security procedure, it is liable to pay damages to the affected party.
  - Section 72 A of the ITA 2008 now explicitly provides recourse against dissemination of personal information obtained through an intermediary or under a services contract, without the individual's consent, with intent to cause wrongful loss or wrongful gain.
- ## Telecom License (UASL) Requirements
  - UASL License Requirements Part VI Security Conditions – Various clauses such as 39.1, 39.2, 39.3, 40.4, 40.5, 41.4, 41.14, 41.19 (iv) mandate the licensee (telecom operator) to ensure confidentiality and privacy of customer information.
- ## The Telecom Unsolicited Commercial Communications Regulations, 2007
  - Mandates requirements for setting up a National Do Not Call Registry, with implicit requirements for ensuring customer privacy.

It is important to understand the essence of these regulatory requirements and to draw the right interpretations. One also has to keep a tab on the amendments to the existing regulatory requirements to ensure that the control measures are designed to meet specific requirements. M&A further unfolds external mandates that demand more stringent regulatory requirements on privacy.

Where and how do these rules and regulations impact an organization the most? The response to this question lies in executing a top-down approach of privacy impact assessment since privacy too is a risk-management issue. Such an assessment needs to look at all the processes in the customer service delivery function – order handling, sales & service, billing, call center, subscriber data management – going further down within CRM, to retention & loyalty and other processes. In a nutshell, it should cover all processes within fulfillment, assurance, billing & revenue management as well as fraud management. Internal systems such as ERP, email and employee portals should not be overlooked either.

The privacy as a matter of concern is not only restricted to business sensitive information for telecom customers, but also expand its scope to employee life cycle, an another area that needs equal attention. The reasons for the same are multi-fold, which include: first, because employees' personal information demands protection, and secondly, because employees are the custodians of customer sensitive information, hence they should also maintain confidentiality.

Let's look at two processes that go through various stages where privacy or, more specifically PII data is involved.

a) Customer Life Cycle Management

The process depicted in Figure 1 shows the five steps a telecom service provider follows for customer life cycle management. Within each of these steps, there are touch points where PII is originated, handled and managed. These touch points cover both the physical records (the customer application form that contains most of the personal information along with the payment options) as well as the data in the business and operations support systems applications.

For example, in customer acquisition – part of the fulfillment vertical process, while selling or order handling through outlets or online subscription or through a third-party arrangement, personal details are sought in the customer application form. Likewise, PII is sought in all of the remaining four steps. Once the information is collected and stored, it is required to be handled as part of your privacy treatment plan.

The five processes shown above are at a high level (L1) and the privacy impact assessment has to go down at least to level 4 and cover other horizontal areas such as service management, resource management, supplier and partner relationship management.

b) Employee Life Cycle Management

It is vital to consider employee personal information as equally sensitive as customer personal information. Therefore, all the sensitive touch points refer to Figure 2 should be examined to assess the PII details. Not only the HR department of the organization but also the outsourced agencies (e.g. the ones that do background verification) hold a lot of PII during the recruitment and hiring process. The PII in online systems also poses the same privacy risks.

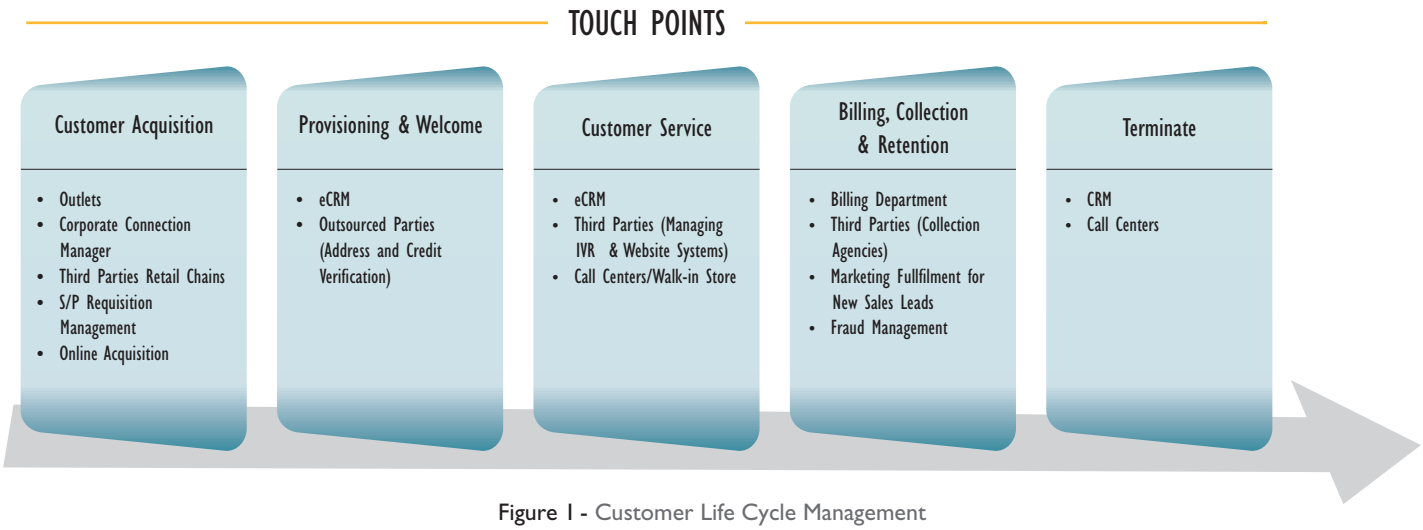

Figure 1 - Customer Life Cycle Management

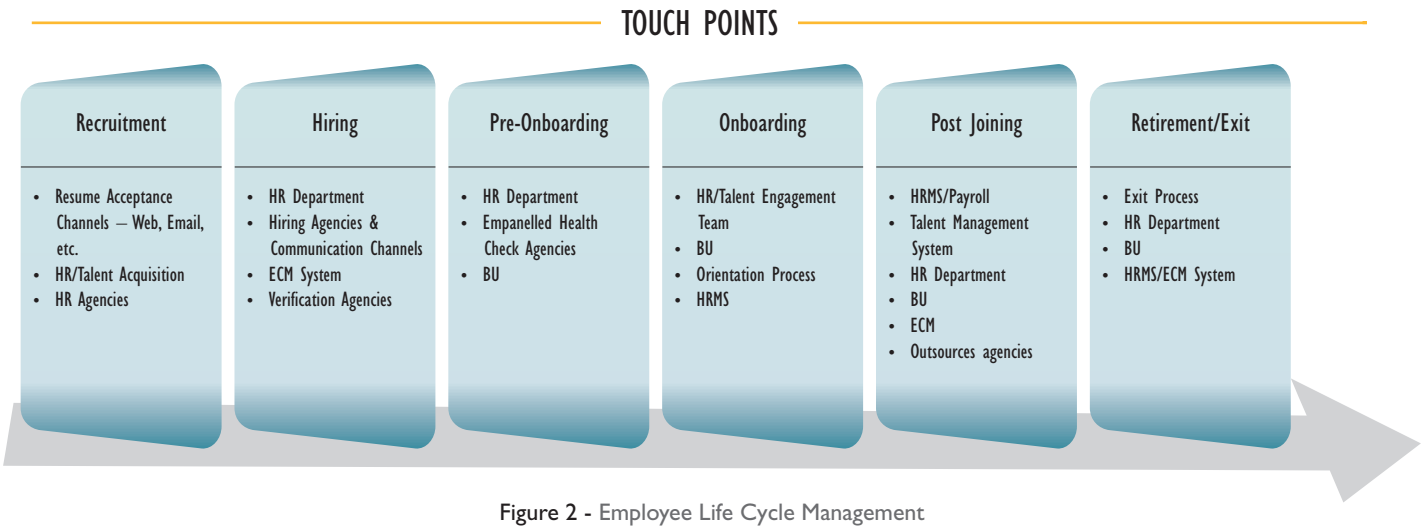

Figure 2 - Employee Life Cycle Management

The Approach

The short answer is a risk-based approach to do an impact assessment. Essentially there are four critical things to do. 1) It is important to define the privacy and PII elements as well as to identify the drivers. 2) Create the PII inventory to map business processes and underlying applications and infrastructure 3) Carry out an impact assessment and determine critical processes, their boundaries and touch points. This assessment will enable to assess and refine the existing controls and to determine the level of protection required. 4) Enforcement through policy and framework to comply with the impacting regulation will remain central to the solutions approach.

The Challenge

Implementing the appropriate enterprise-wide privacy framework and adopting the right technology are critical. For example, initially it is necessary to discover the PII data within the systems and then build the technical options for data protection. Other areas that are equally demanding are user awareness and training as well as privacy enhancing technologies that provide a degree of anonymity (which in turn help build trust and reduce risks), and monitoring and reporting violations. At a higher level, end-user entitlements, data storage at rest and in transit, and third-party agreements driven through the procurement and vendor relationship cells should not be overlooked.

Conclusion

Maintaining privacy and protecting customer and employee personal information is a risk-management issue for all organizations. It goes beyond the regulatory requirements because customers expect their data to be protected to avoid identity thefts; it impacts an organization's reputation and leads to financial loss due to lost revenue and litigation. Above all, customer confidence in the brand is impacted if there is no framework to deal with customer privacy.

About the Author

Manohar Ganshani

Manohar Ganshani heads the Governance Risk & Compliance practice in Wipro Consulting Services. He is a BE in Computers. Manohar carries 21 years of experience in the field of Information Technology with over 11 years in the area of information security, IT security, cyber security, data privacy, regulatory compliance, security strategy, policy and architecture design.

As a practitioner, he has handled many complex engagements in risk and compliance space for the clients in US, EU, APAC apart from India. As a practice head he commands significant experience on conceptualizing and developing new service lines around cyber security, social media security, data privacy, information security management systems, payment card industry compliance solutions, business continuity assurance services and Cloud security.

As a thought leader, he has written and spoken on various issues like mobile security, cyber security, critical infrastructure protection, privacy for telecom, insider threat, social media security and social awareness in various forums organized by industry and state governments.

About Wipro Consulting Services

Wipro Consulting Services (WCS) is a division of Wipro Ltd (NYSE:WIT), a $7 Billion enterprise that employs over 136,734 + employees across the globe. WCS offers Business Advisory, IT Consulting and Risk and Compliance services designed to improve business performance, drive operational efficiency and maximize ROI. With 1350+ consultants based in Western Europe, North America, India, Asia Pacific and the Middle East, our integrated Consulting, IT, BPO and Product Engineering services combine the benefits of expert proximity with global leverage to provide technology edge and speed to your strategic programs.

About Wipro IT Services

Wipro IT Services a part of Wipro Limited (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company, that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology" – helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation and an organization wide commitment to sustainability, Wipro IT business has 135,000 employees and clients across 54 countries.

For more information, please visit www.wipro.com or contact us at info@wipro.com

DO BUSINESS BETTER

NYSE:WIT | OVER 135,000 EMPLOYEES | 54 COUNTRIES **CONSULTING | SYSTEM INTEGRATION | OUTSOURCING**

WIPRO TECHNOLOGIES, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256

North America South America **Canada** United Kingdom **Germany** France **Switzerland** Poland **Austria** Sweden **Finland** Benelux **Portugal** Romania **Japan** Philippines **Singapore** Malaysia **Australia**

IND/CREST/OCT2012/E106DP