WHITE PAPER

PROTECTING EMPLOYEE DATA THROUGH INFOSYS PRIVACY WALL

Abstract

As work and personal environments have started to merge into one, the privacy of employees is placed at increased risk. There are numerous channels through which employee data is collected, processed, and persisted in the new-age workplace. This proliferation of personal and professional data enables us to leave users to unwittingly leave "digital footprints" – this has caused a huge risk in data privacy breaches.

This whitepaper aims to explore the need for building a digital divide through Privacy Wall. This secure Privacy Wall provides a digital security boundary providing a logical separation of individual information in a boundary-less data construct.

Infosys®
Navigate your next

Table of Contents

Rise of the Boundary-less enterprises and increase in Privacy Risk of Employee Data

Most of the organizations let lawyers and privacy compliance teams design their privacy experiences for their employees. It is time to question this practice, from the design of the employee onboarding portal to collect of employee's date of birth or the employee's consent which we never read…Employee Privacy experiences could be amazing opportunities for organizations to earn the trust and advocacy of their employees, customer, and partners.

As work and personal environments have started to merge into one, the privacy of employees is placed at increased risk in today's world. There are numerous channels through which employee data is collected, processed, and persisted in the new-age workplace. This proliferation of personal and professional data enables us to leave users to unwittingly leave "digital footprints" – this has caused a huge risk in data privacy breaches.

Infosys Privacy Wall is a simple framework combining a reference architecture for your organization, Infosys privacy-enhancing technology, and a financial model that enables the organization to create an engaging, employee-centric approach in handling regulated personal information collected across multiple data sources from the employee during the tenure in the organization.

This whitepaper aims to explore the need for building a digital divide through Infosys Privacy Wall. This secure Privacy Wall provides a digital security boundary providing a logical separation of individual information in today's boundary-less data construct.

Evolution of the Employee Digital Footprint in the modern workplace

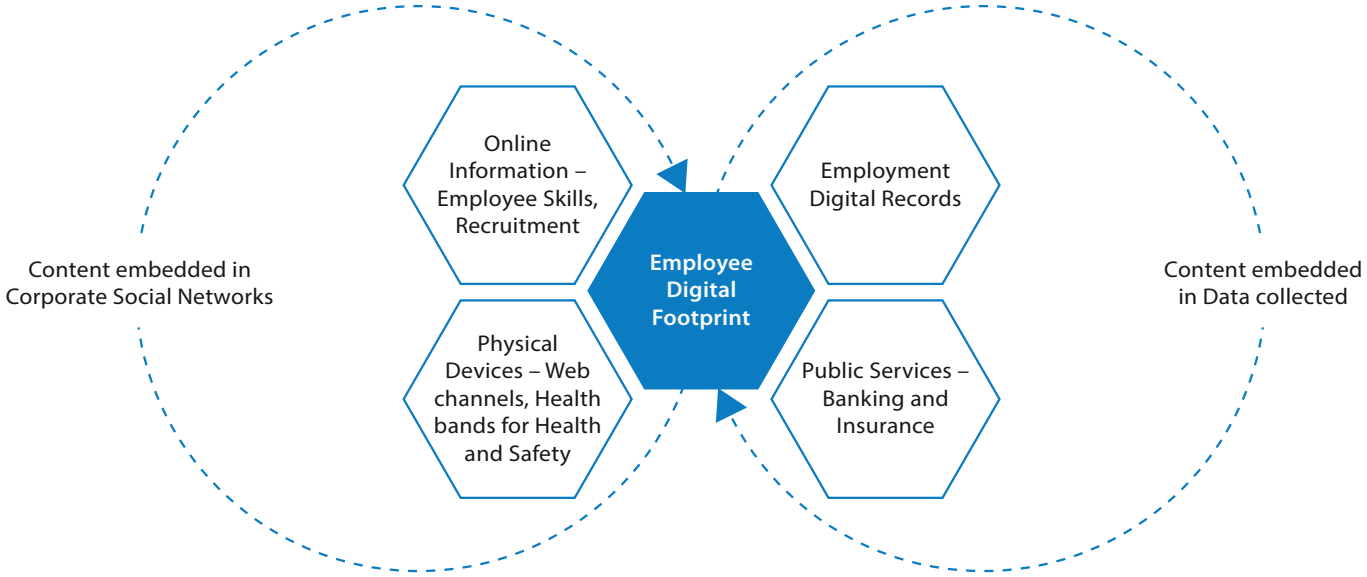
As workplaces have been very pervasive, and users are getting exposed to a larger data privacy risk. There is a lot of information collected from users voluntarily and involuntarily. In today's post-pandemic world, requires the employee to connect remotely and there is a diverse set of sensors like the basic identification reader to more complex fitness devices that keep collecting employee health information.

In his book The Fourth Industrial Revolution, Klaus Schwab, the founder and executive chairman of the World Economic Forum, the International Organization for Public-Private Cooperation, asserts that there are four distinct periods of industrial revolution throughout history, including the one we're beginning right now. The digital footprint of an employee has evolved over the industrial age to what we see today as an "employee digital footprint" which could be a combination of an individual's personal and official data.

	1st Industrial Revolution Mechanization	**2nd Industrial Revolution** Electrification	**3rd Industrial Revolution** Automation	**4th Industrial Revolution** Cyber - Physical
				
	1800s	1900s	1970s	2000s
How did data on individuals evolve?	Agrarian societies gave way to urbanization – Limited or no records on individuals	New Key inventions – electricity, aero planes, assembly lines. Employee and citizens records created for operations	Semiconductors, mainframe computing, personal computing, and the Internet – Rapid computerization caused digital records of individuals	Commoditization of Digital footprint across social networks and cyber-physical world
What are the key controls?	No regulation	Minimal control on data collection and management	Localized Regulations	Specific law and policies across the globe to manage the Digital Footprint

The phase of the Industry Revolution	How was the Digital footprint evolving?
1st Industrial Revolution- Mechanization	Agrarian societies gave way to urbanization – Steam engine powered ships and trains and changes the way people travel. This is the first time, there is a need to collect data on employees. Diverse disconnected manual records of individuals were collected
2nd Industrial Revolution - Electrification	New Key inventions – electricity, airplanes, assembly lines. The 1900s saw workers leaving their rural homes behind to move to urban areas and factory jobs. Factories needed to keep track of their workers. Employers collected data for payroll and operations. Further governments started collecting data on citizens for better management
3rd Industrial Revolution - Automation	Semiconductors, mainframe computing, personal computing, and the Internet – Rapid computerization needed digital records of individuals for ease of operation. This is the first time – Digital footprint was recorded and shared across multiple entities
4th Industrial Revolution - Cyber-Physical	Social networks and the internet boom in the Cyber-Physical world need us to manage the Digital Footprint. Governments are working on policies to manage the breach and invasion of privacy or abuse of the digital footprint. The footprint could be on social networks or even spread through cyber-physical channels such as Card Readers, Routers, fitness bands, or sleep monitors.

The key problem statement to solve is how do we define the digital footprint in today's world, ensure the right data privacy controls are applied to the digital footprint available only to authorized employees and share information only before proper consent is shared.



Digital footprints are derived from multiple sources in today's workplace

- Employment information: Starting from the employment information collected as background information before inducting a new employee.
- Public services: Data shared on the individual for health care benefits, banking, or government taxation.
- Online Information: Active data shared on various corporate social networks or passively collected information on the browsers or online forms.
- Cyber-Physical devices: There are numerous devices which are used in an office place such as card readers, routers, adaptors, networking tools, and health tracking devices which could have specific data on individuals.

Why Infosys Privacy Wall for an Enterprise?

Privacy by design for employee data is a multi-faceted concept. Legal documentation and process in one hand and specific privacy-enhancing technologies on the other hand. However, in practice, there is always the tendency to treat privacy as a binary thing. We either care for it or not.

Very few enterprises realize that for a risk-free operation, there is a need for multiple degrees of privacy controls, this is why feel there is a need for Infosys Privacy Wall, which gives a degree of varying privacy intensity based on the privacy experience required for each persona in an enterprise handling employee data.

The privacy wall is an innovation as a result of combining a technical reference architecture, Infosys Privacy Enhancing Technology (Infosys IP), and a comprehensive financial model which helps organization design the right privacy experience and manage data privacy risk.

Infosys Privacy Wall is a framework which consists of the following:

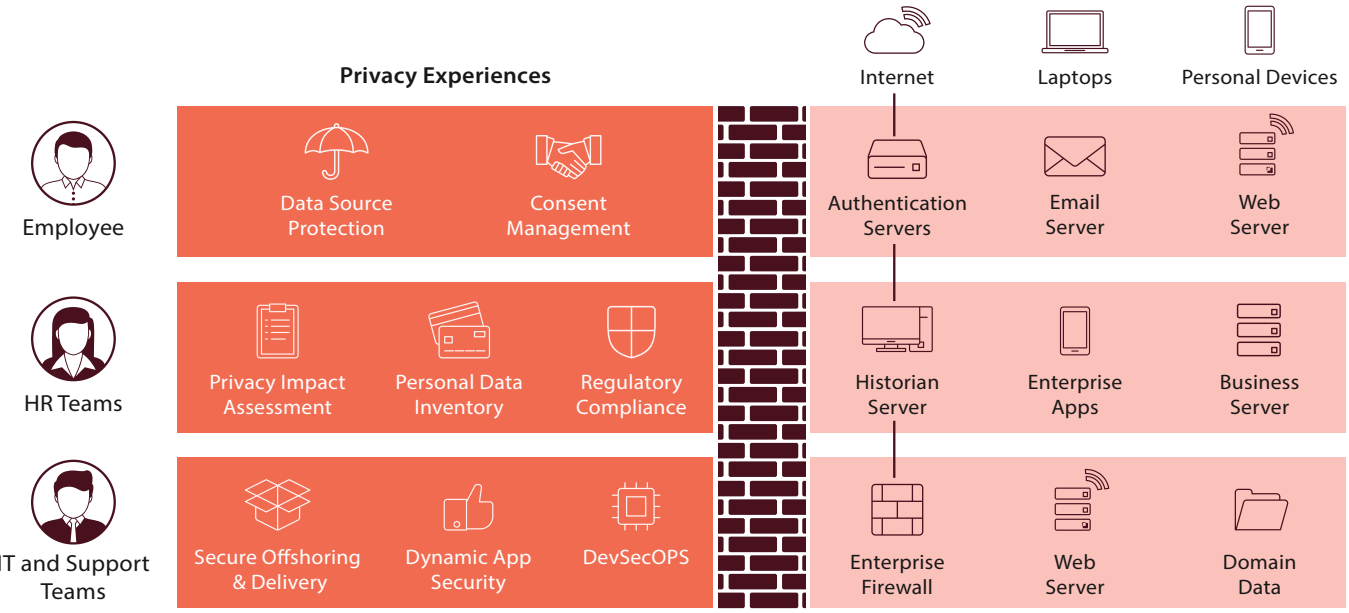
1. Reference Architecture for enterprises – Can we build an enterprise-level evolutionary architecture to manage the privacy experience of each employee?
2. Infosys Privacy Enhancing Technology – Can we ensure there is the right protection of employee data that is collected and managed by the organization?
3. Financial Model for Privacy Risk Management – Can we calculate the cost of the financial risk if there is an employee data breach?

How can we help you build your Privacy Wall?

In Today's Post Pandemic world, the Information Risk and Data Privacy threat are universal. Data Privacy Breaches in recent times have exposed vulnerabilities not only in the software or people-based but also hardware or process-based.

When enterprises are struggling to build awareness across their employees, partners and most importantly their end customers, the execution of Data Privacy initiatives is confusing and unmanageable. Even after years of discussion and debate, the risks continue and even escalate. Most companies don't fully understand the threat and don't always prepare as well as they might. We don't claim to have all the answers, either, but Infosys Privacy Wall provides a logical framework to define the problem and the pitfalls will help companies calibrate their current stance on Data Privacy on their employee data.

Reference Architecture for Enterprises



Employee data is incredibly useful for measuring performance, identifying skill gaps, and recruiting new talent, but balancing access and analysis with data security can be a major challenge—especially when information is dispersed across numerous HR systems.

Infosys Privacy Wall provides protection at each level of the organization functions.

1. Employee – Employee data should be protected, and proper consent should be taken from Employees before collection, processing, retention and deletion of employee data
2. HR Teams – HR Teams have access employee information, there should be a personal data inventory store for quick and easy access and review cross border compliance. Also, periodic audits and privacy impact assessment should be taken care
3. IT and Support Teams – Access to sensitive employee data should be carefully curated and protected through masking and dynamic application security. Infosys privacy wall also recommends DevSecOps while building and testing applications which leverage sensitive employee information

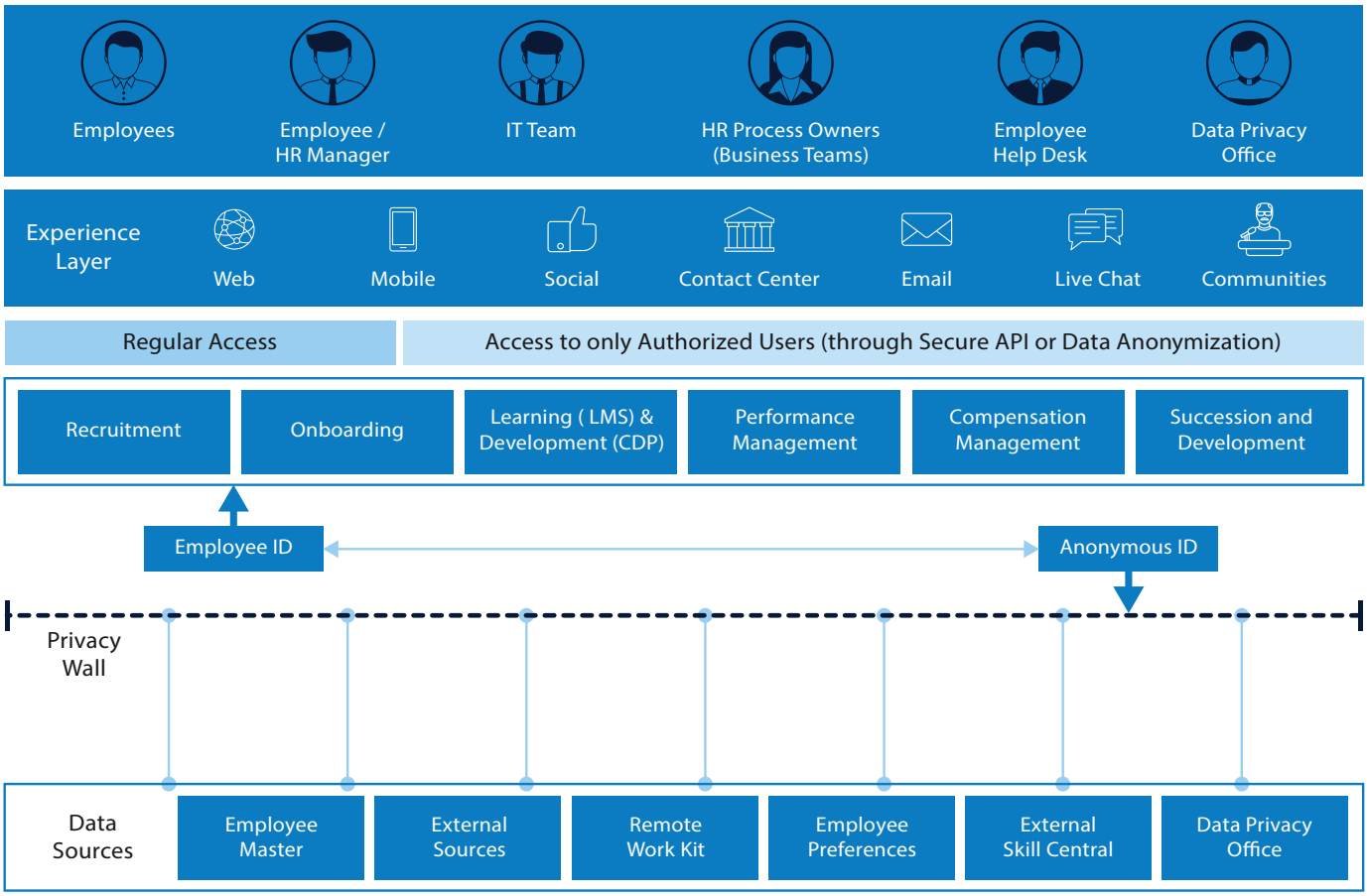
Infosys Privacy Enhancing Technology

Major pain points that companies face is the vast amount of information there is to protect. This is a problem even for organizations with handful employees, each employee has quite a bit of sensitive information held by the company—meaning it's a pretty big task to securely manage and safeguard it all, especially as organizations grow. Add to that the prevalence of internet-connected devices and the ability to work remotely from any location, there are more access points than ever before for intruders to try to breach employee data.

Many of the enterprises do not have standards to collect, process, and most importantly securely retain and dispose of employee information, the result is a "data graveyard" of employee data. There are large volumes of unaccounted employee data collected and persisted in multiple

storage sources which could be potential sources of data privacy risk.

Infosys privacy wall aims to address this by providing a logical separation of the data by secure access and locally encrypting the data leveraging standard industry algorithms. The focus would be to anonymize employee records with a unique reference derived from the employee ID and a random key generated by our Privacy Suite. This would be the standard reference through the employee records that would be accessed across multiple sources of data that contains sensitive information. This logical layer separates sensitive information and ensures the data is unusable without the right employee reference provided by Privacy Wall.

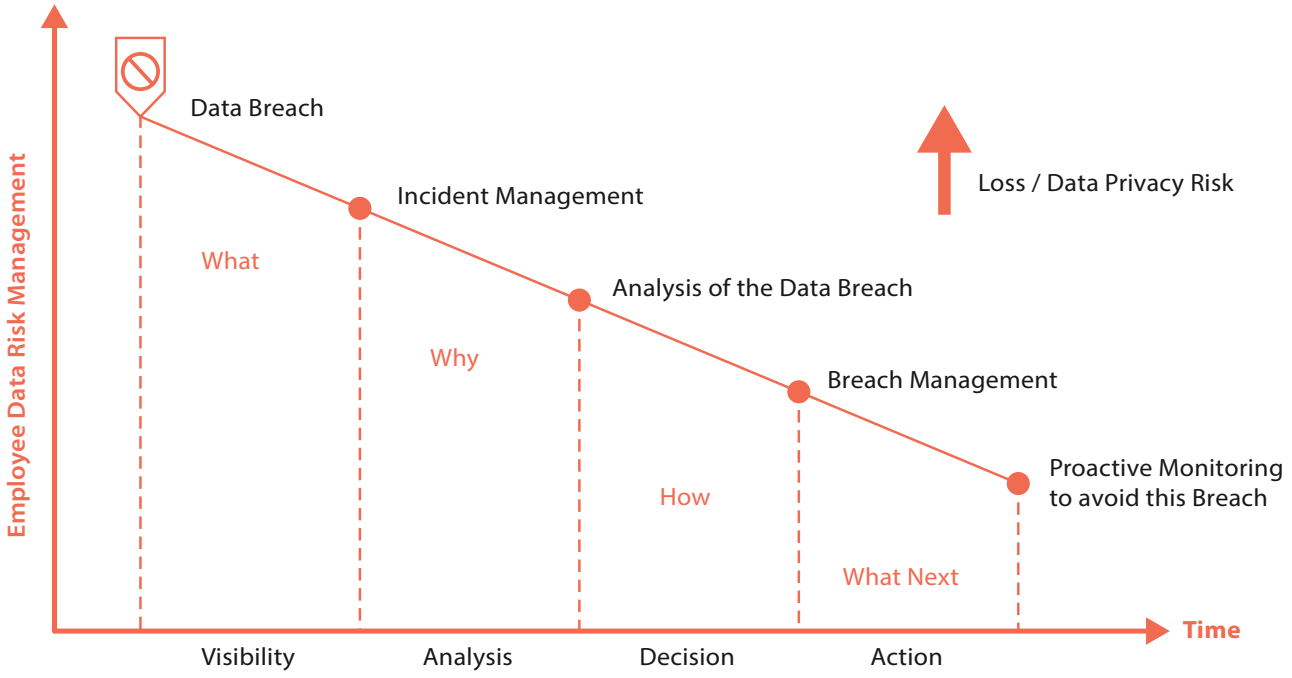


Financial Model for Privacy Risk Management

Over and over, enterprises around the globe complain that they do not get enough funding for the kind of employee privacy programs they want to create. After firms were forced to spend more than they expected in GDPR compliance and post-pandemic Data Breaches in 2020, we felt there is a need to build a robust Financial Model to complement the reference architecture and our best in class Privacy-enhancing technology. Privacy Wall aims to build a positive ROI which will drive the CFO to find a budget that will enable the teams to turn compliance to a competitive advantage.

Privacy Wall focusses on providing a financial model that focuses on 4 specific areas of the employee data breach.

Risk Stage	Positive Impact	Negative Impact
Visibility	Opportunity to reinforce the security of employee data	The hard cost of the Privacy Breach on Employee Data
Analysis	The positive impact of a robust incident management	Cost of managing the incident and cost of communication
Decision	Repository of employee data risk breaches	Time and effort are taken for the analysis of the incident
Action	Proactive monitoring and prevention of breaches in the future	Cost of proactive monitoring solution to avoid this breach



How do we see enterprise evolving around the Privacy Wall?

As an organization grows, the data collected on the employee also grows in multifold times creating a large potential for data risk. Privacy Wall enables us to Assess, Architect, and Assure the employee data which is collected in an enterprise. We understand each customer could be at a different level of maturity in managing their employee data.

Infosys Privacy Wall	Organization Maturity Level	How can we help our Enterprise Customers?
Assess	Greenfield implementation – Getting started on Employee Experience	• Planned Audits and Continuous watch on Privacy norms updates for Employee Data • Discovery the sensitive data across SF data sources and your IT landscape
Architect	Digital Transformation of Employee Experience	• Threat modeling across business processes processing of Sensitive Employee information • Data Protection through 180+ Algorithms for anonymization, pseudonymization, and obfuscation of sensitive employee data • Deploy Privacy Wall for managing your employee data across the enterprise
Assure	Well evolved Employee Data Privacy Process	• Privacy by Design and Default – Checks and balances across the lifecycle of employee data • Continuous Audit Process of Employee Data

About the Author

Karthik Nagarajan, Industry Principal Consultant, Infosys Center for Emerging Technology Solutions (ICETS), has 14+ years of CRM Expertise, focused on Solution Architecture, Product Development, and Business Development. He is currently a part of the product team of Infosys Enterprise Data Privacy Suite, Data for Digital iCETS.

His focus includes Data Privacy, Data Augmentation and CX Strategy.

Sujith Joseph, Senior Technology Architect, is the Product Manager of Infosys Data Privacy Suite. He has been pivotal in successful Data Privacy assessments and implementations of iEDPS across many customers across the globe.

He specializes in Product Management, Data Architecture, and Data Security.

Guruprasad N V (Guru) – A Senior Principal Technology Architect working with the Infosys Center for Emerging Technology Solutions (ICETS). Guru has over 19 years of experience in architecting, designing, driving first of its kind experiments, incubating and institutionalizing new products and services using emerging technologies. He's currently part of Digital Engagements CoE at iCETS, which encompasses Conversational Interfaces, User Experience, Internet of Things, and XR Technologies.

For more information, contact askus@infosys.com

Navigate your next