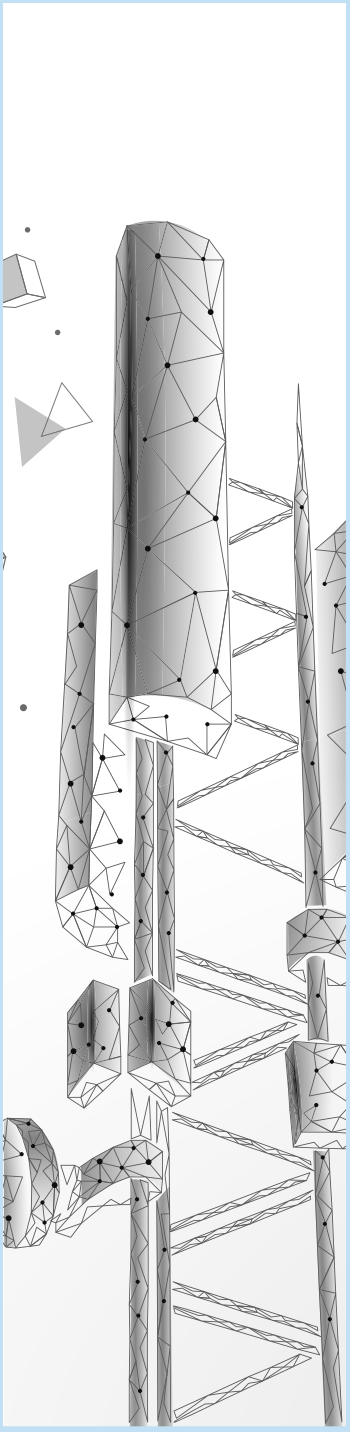
VIEW POINT



THE BALANCING ACT – PROMISE OF 5G VS GROWING PRIVACY CHALLENGES

Abstract

We are in the era of 5G with promises of faster speeds and lower latency. However, constantly connected IoT devices are collecting, transforming and transporting large volumes of data across heterogenous data sources and pose a serious risk in personal data privacy. 5G technology evolution promises key security technologies, but are they enough?

This point of view explores managing the balancing act by leveraging effective privacy engineering based on Privacy by Design to build the privacy wall to benefit from 5G with minimal data privacy risk.

Infosys®
Navigate your next

Table of Contents

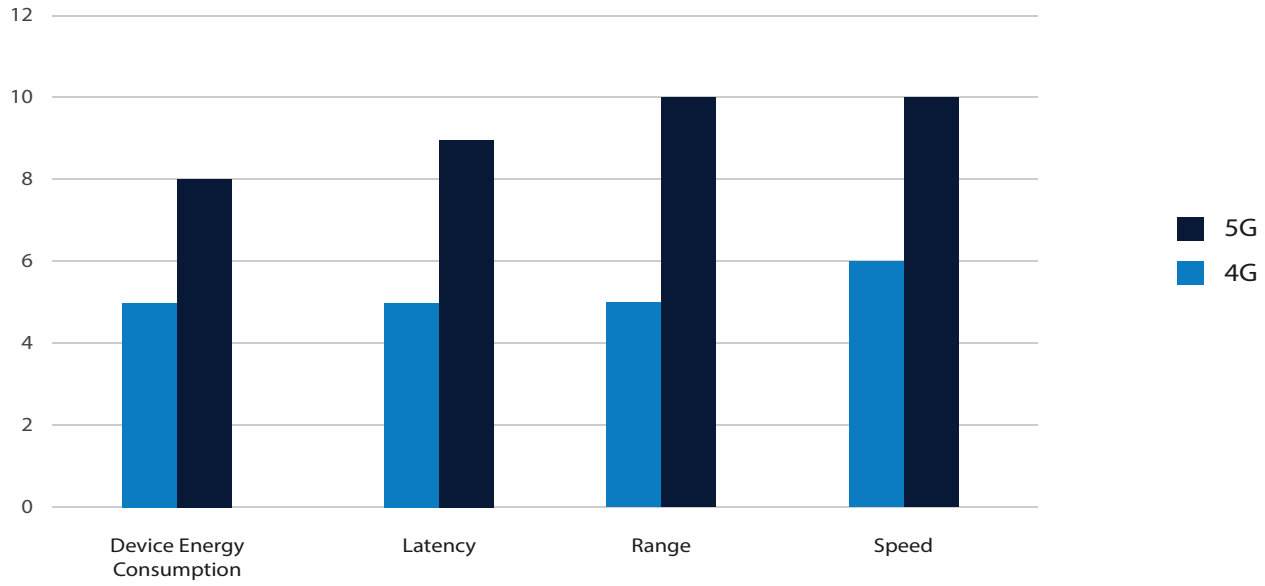
Why this balancing act?

We live in an age of data-oriented organizations which collect and maintain a significant amount of data associated to individuals including their personal data preferences and financial history.

In the recent past, you would have noticed a slew of data breaches in India from reputed household names.

- 25,00,000 customer personal data records leaked from a Major Indian Telco including social security number, address and DOB
- 100,000,000 user data records breached from a local search engine
- 20,000,000 customer records compromised from an online grocery store

Once 5G comes into our lives, along with the promise of endless possibilities, the proliferations of connections and unstructured device data will make today's data look like the tip of an iceberg.



The rise of 5G will also lead to new regulations and standards coupled with a focus on changing expectations from the end consumer as well as an emphasis on consumer consent management. The question organizations need to ask themselves is - are we truly ready with the right knowledge, skill, design and investments for these changes and can we effectively protect the end consumer's data?

Why this growing concern of privacy around 5G?

5G is poised to power smart cities, IoT driven servitization, improve mobility in healthcare and experiential marketing in retail. In total, industry experts believe the financial gain of 5G to be in the tune of 2 trillion dollars by the end of 2030.

But constantly connected IoT devices are going be collecting, transforming and transporting very large volumes of data across heterogeneous data sources and pose a serious risk in personal data privacy. 5G technology evolution promises key security technologies, but are they enough?

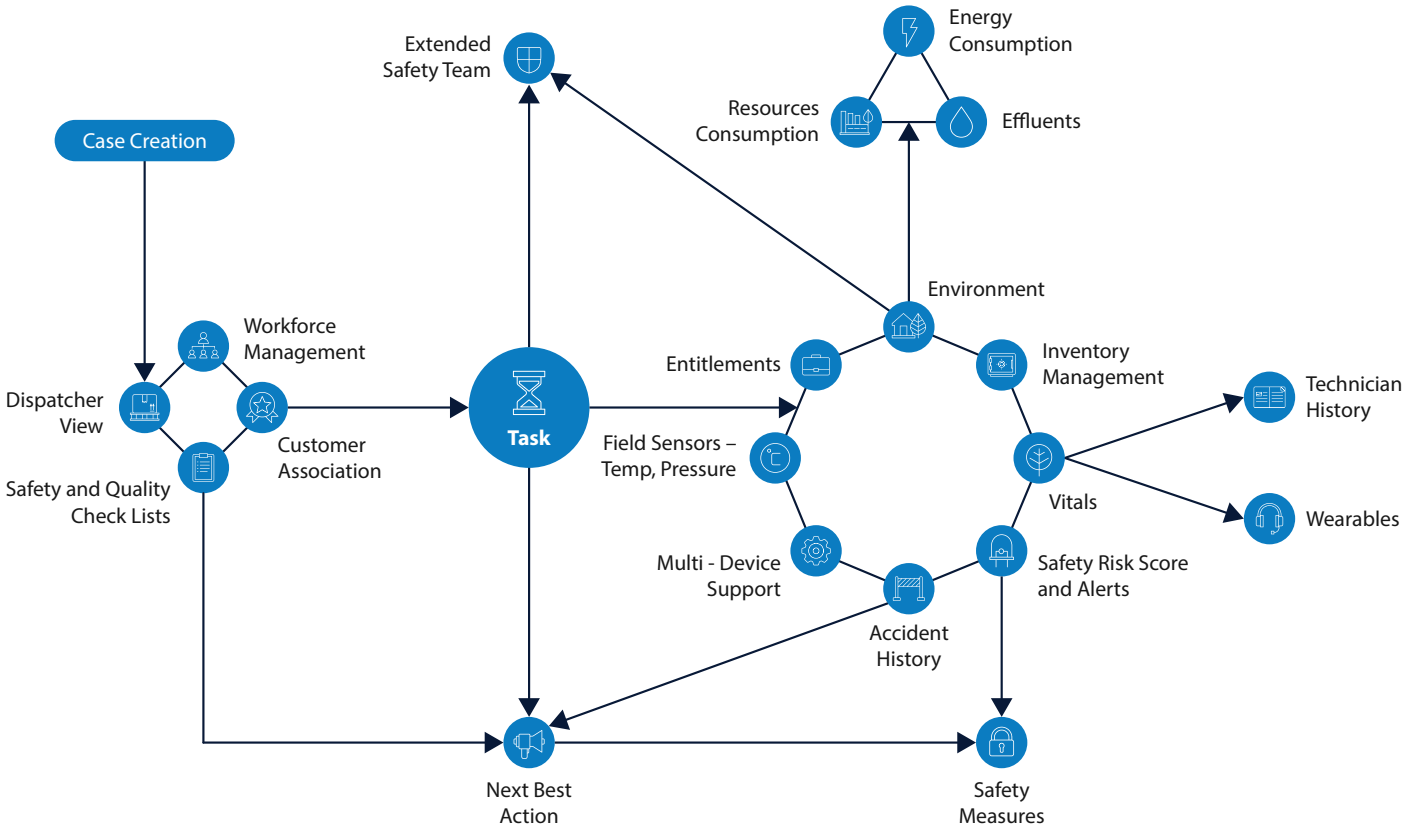
Let us look at some of the real-life scenarios in the 5G world which we need to analyze to understand the gravity of the data privacy risk.

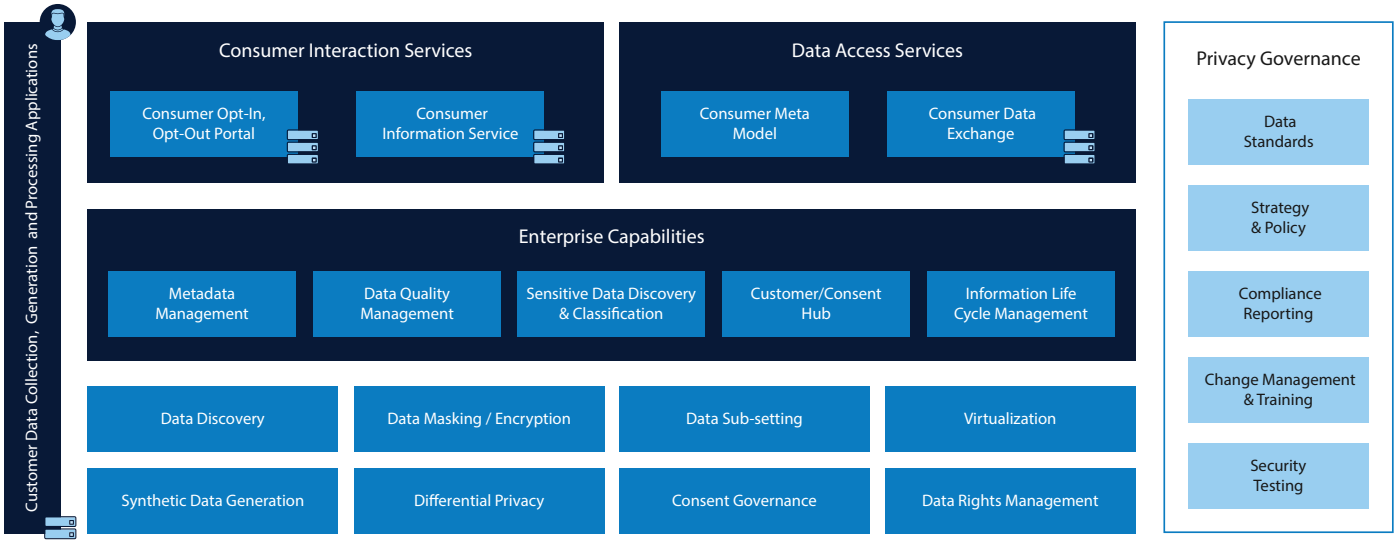
- Smart cities will have IoT devices designed by key players to pick up speech, facial expressions, gestures along with personal data and pose a major security risk.
- In the 5G world, smart appliances and wearables connect to a network, transmit personal and sensitive information. For instance, heart rate monitors and fitness bands can transmit your PHI (Personal Health Information) which will need protection from cyber breaches.
- Location Data Privacy is another major concern in the 5G Internet space. 5G can provide very accurate and precise coverage area. Also, there would be a more dense volume of tower range within a small radius. This higher accuracy movement trail and precise location creates a significant risk for major data breaches.
- Low Latency – 5G promises IoT optimized high energy efficiency. These changes on devices are left running without monitoring. An example is the "Always ON" device feature that can pose a surveillance nuisance.
- Finally, the most concerning is privacy in our personal life- smart appliances which are not designed with an orientation toward data privacy and security. Consider a scenario when a manufacturer can remotely program a device to provide a back-door entrance into the owner's personal life without consent. For instance, imagine your smart kitchen appliance sharing what you cooked to a food delivery service or neighborhood restaurant chain.

Privacy Engineering for 5G

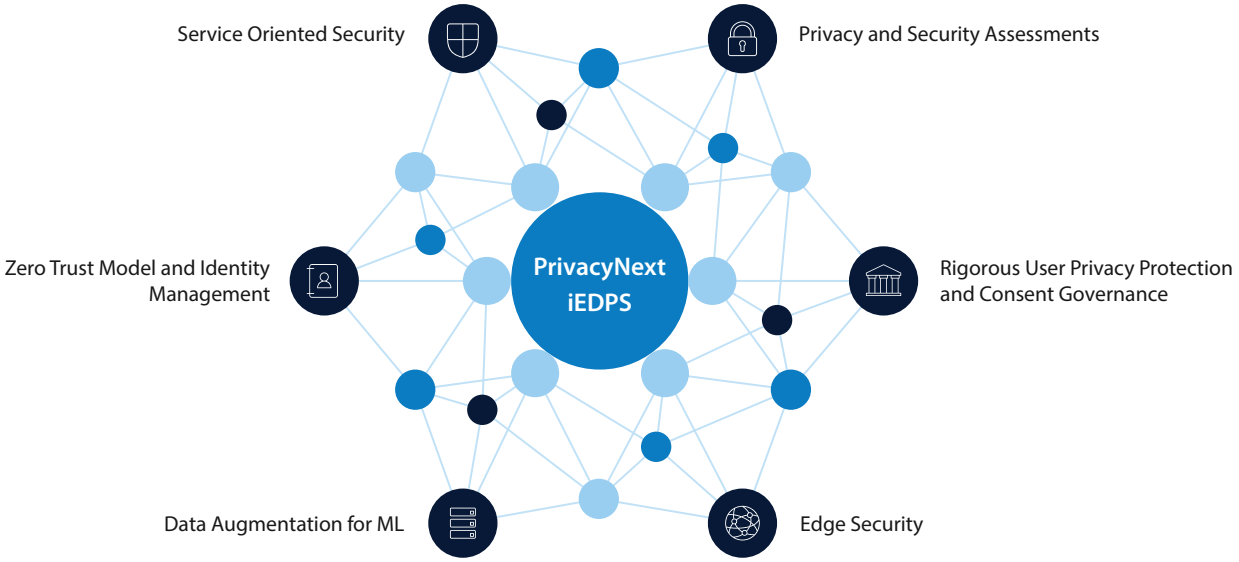
As the 5G era draws near, the volume and types of data with heterogeneous data sources will increase many fold. To manage the balancing act, we need effective privacy engineering to act as a catalyst and build the privacy wall to benefit from 5G with minimal data privacy risk.

Privacy Engineering is an evolving discipline that incorporates the 7 foundational principles of Privacy by Design. There are also numerous efforts underway by NIST and other Data Privacy regulatory bodies to build global standards like ISO/ISR PTDR 27750. These standards need to be applied for engineering 5G technology and its accompanying security techniques.



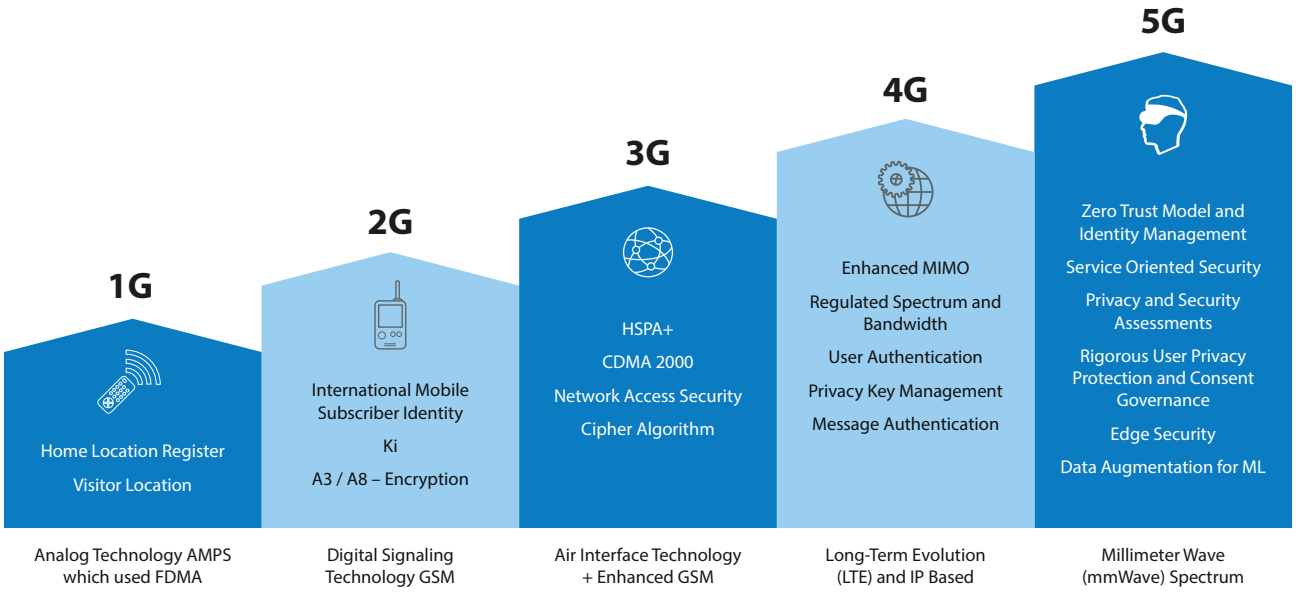


Our top focus areas for 5G Privacy Engineering are as follows:



- **Zero Trust Model and Identity Management** – There will be security standards to discover, capture and protect bio-metric authentication from users including data on fingerprints, photos, videos, voice, physiological recognition, and DNA signatures. This will enable zero trust and fail proof identity management.
- **Service Oriented Security** – Flexible architecture for different network slices and data stores. This will focus on improving the current encryption standards including reinforcement with Quantum encryption standards.
- **Privacy and Security Assessments** – 5G needs an open software and hardware ecosystem which can be audited and assessed at regular intervals to comply with emerging regulatory norms.
- **Rigorous User Privacy Protection and Consent Governance** – Data leaks without the right consent governance must be avoided at any cost.
- **Edge Security** – Low delay mobility in ultra-dense networks need security on the edge. Edge Pro is our key offering for providing data privacy and security for this.
- **Data Augmentation for ML** – There are going to be petabytes of data which need to be shared for AI/ML algorithm learning and training. The focus should be to augment data through synthetic data generation or de-identification before this. Key privacy preserving techniques like Differential Privacy will have a large role to play in data aggregation and resistance to reconstruction of sensitive personal information.

In conclusion, Security and Privacy for 5G cannot be built after system design or in silos. Privacy Engineering must be a part of the design with the active dialogues between the CSP, privacy communities and policymakers.



References

- https://iapp.org/news/a/5g-to-raise-privacy-challenges-and-opportunities/
- https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/connected-world-an-evolution-in-connectivity-beyond-the-5g-revolution
- https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/the%205g%20era%20new%20horizons%20for%20advanced%20electronics%20and%20industrial%20companies/the-5g-era-new-horizons-for-advanced-electronics-and-industrial-companies.pdf

About the Authors

Sujith Joseph

Sujith Joseph, Senior Technology Architect, is the Product Manager for Infosys Enterprise Data Privacy Suite. He has been pivotal in successful Data Privacy Assessments and implementations for multiple customers across the globe.

Jagadamba Krovvidi

Jagadamba Krovvidi is an Associate Vice President at Infosys Center for Emerging Technology Solutions (ICETS) with 24 years of experience. She focusses on Data for Digital for Infosys's Enterprise Customers.

Karthik Nagarajan

Karthik Nagarajan is an Industry Principal Consultant at Infosys Center for Emerging Technology Solutions (ICETS). He has more than 15 years of experience in customer experience solution architecture, product development, and business development. He currently works with the product team of Infosys Enterprise Data Privacy Suite, Data augmentation, and CX strategy.

About iCETS

The incubation center of Infosys called 'Infosys Center for Emerging Technology Solutions' (iCETS) focuses on incubation of NextGen services and offerings by identifying and building technology capabilities to accelerate innovation. The current areas of incubation include AI & ML, Blockchain, Computer Vision, Conversational interfaces, AR-VR, Deep Learning, Advanced Analytics using video, speech, text and much more.

To know more, please reach out to iCETS@infosys.com.

For more information, contact askus@infosys.com

Infosys®
Navigate your next