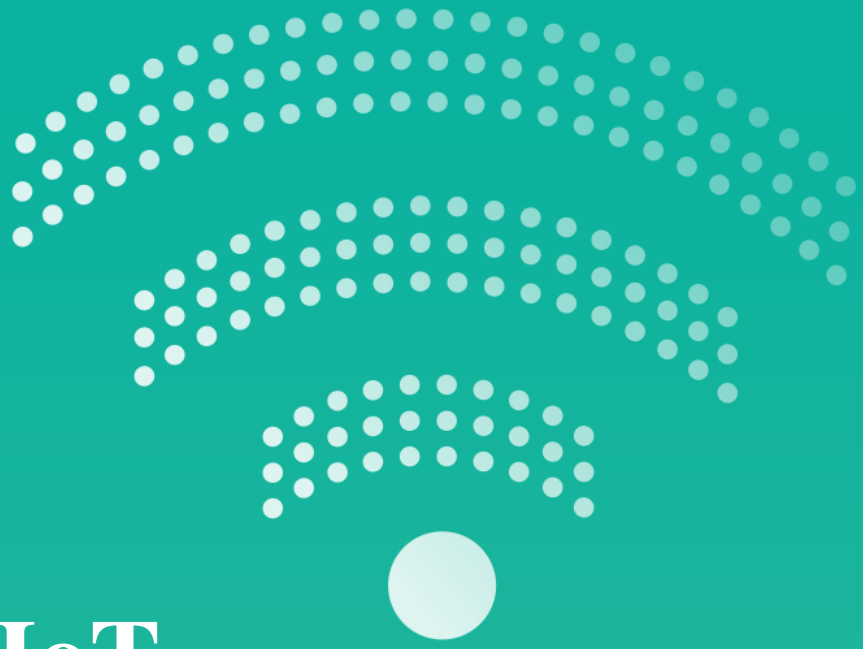


Building an IoT Telco Platform as a Service

How telcos can step out of their traditional role as providers of voice and data services and into the growing IoT market.

solace.

> **Telecommunication companies — with their long-standing ability to connect millions of devices to complex networks — are in a unique position to serve as active partners to commercial IoT customers, whom we expect to propel the IoT market to $470 billion.**

DARREN JACKSON AND HERBERT BLUM, BAIN INSIGHTS
A Massive IoT Opportunity In Search Of The Right Telco, *Forbes*

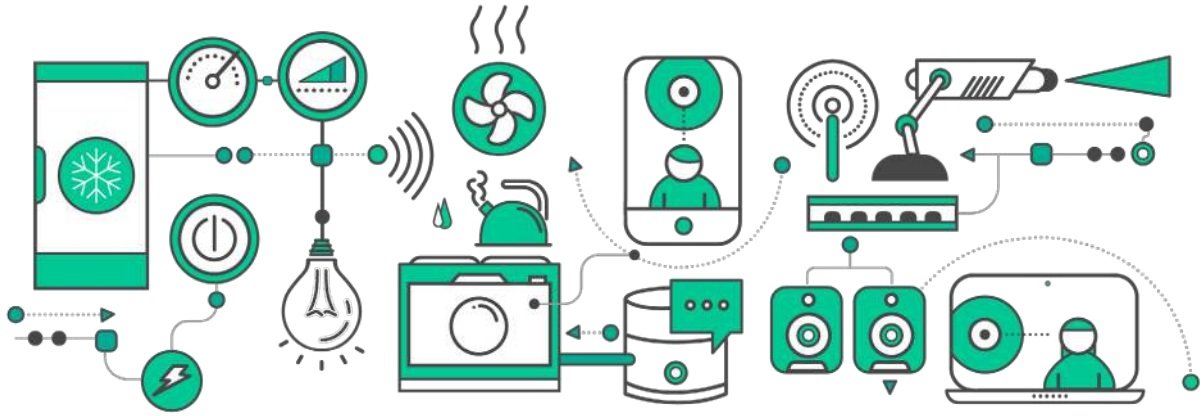
Solace
535 Legget Drive, 3rd Floor
Ottawa, Ontario K2K 3B8
Canada

Phone: +1 613-271-1010
Web: solace.com

TABLE OF CONTENTS

solace.

INTRODUCTION



The core offerings and traditional strategies of telecommunications companies (telcos) have, as researchers at McKinsey & Company put it, "entered a period of slow decline." To reinvent themselves and find new means for revenue, many are turning to the Internet of Things (IoT). Ricardo Gomez-Ulmke, Solace's VP of IoT, outlines the challenges and opportunities ahead.

By all accounts, the IoT market is skyrocketing. According to IDC's *Worldwide Semiannual Internet of Things Spending Guide*, it's projected to reach $1.13 trillion by 2021. Meanwhile, telcos are facing disruption on all fronts, including from the significant developments over the last decade of alternative communication services, namely over-the-top (OTT) content, messaging and even voice services. According to a whitepaper from Iot Ignite titled *Role of Telcos in Internet of Things*, OTTs are part of the reason many telcos have experienced declines in revenue.

DID YOU KNOW?

Gartner forecasts that 20.4 billion connected things will be in use worldwide by 2020, more than double than in 2017.

The rocketing smartphone industry and the software-based services that come with it have shaken the steady ground telcos previously stood on. Industries such as social media that were once considered wholly disparate have and will continue to change the way we communicate with each other.

Instead of being left behind in the ever-growing wave of communication technologies, forward-looking telcos are finding ways to grow and evolve — and many see the booming IoT market as a global canvas to paint what could potentially be their next masterpiece.

But it's important for telcos to step back from the hype and look at the trends in IoT so they can fully understand their place within it. There is no doubt that IoT is the way of the future, but it is up to telcos to discover how they will become part of that future.

The IoT industry itself is in a period of rapid mass discovery, so it's not enough for telco leaders to merely establish a place in the ecosystem. They must, to the extent possible, ensure the place they inhabit has room to grow and that they have the talent and tools to scale with it.

Perhaps the most exciting arena for IoT-focused telcos right now is in the IoT Telco Platform as a Service (IoT-TPaaS) space.

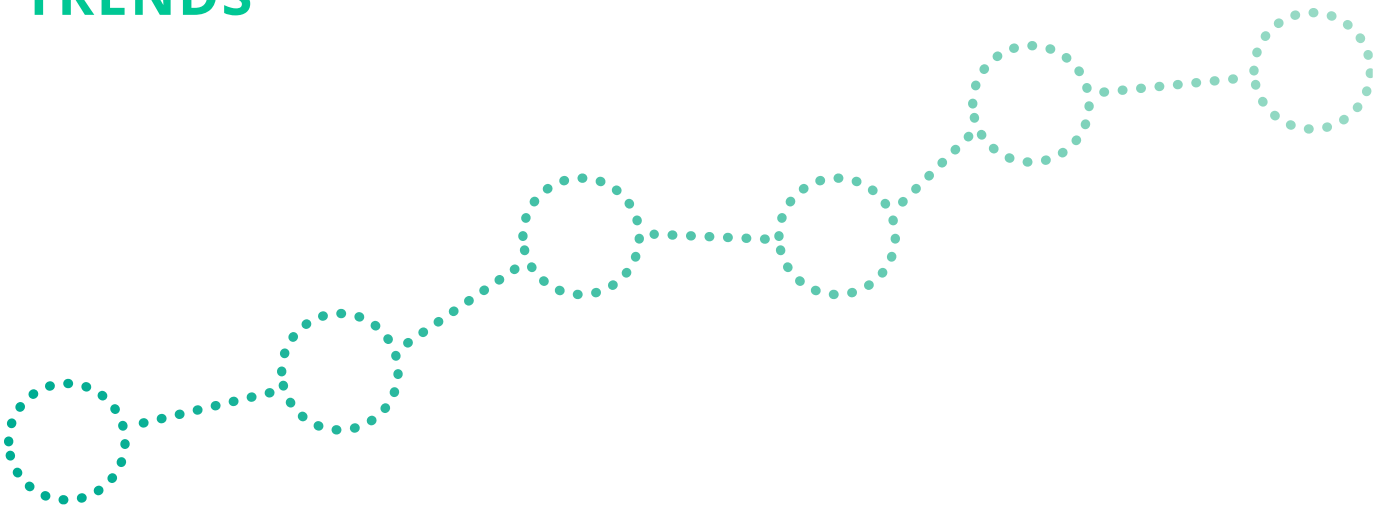
Cheng Qingjun, Huawei's head of IoT consulting, sees the Telco PaaS space split into two business models.

(1) PaaS: where the telco builds the connectivity management platform (CMP) and provides traditional SIM card management services. "Because CMP provides a link to industry customers," Qingjun says, "operators can package cloud services on top of connectivity services and also move into the module market."

(2) PaaS+: where the telco builds out the application enablement platform so operators can integrate SMS, video calls, and voice. "The operator," Qingjun says, "can open these capabilities to developers and industry customers through cloud APIs."

Pivots of this magnitude will not come without challenges. This paper outlines how telco leaders should prepare for and transition into the IoT ecosystem.

TRENDS



Faced with increased competition and downward revenue pressure on their traditional voice and data services, telcos are eyeing the growing IoT market as a new source of income. In fact, a study by IBM showed that 57% of surveyed telco operators want their organizations to become an IoT platform provider.

Many telcos already have a lot of experience in the IoT domain, having provided machine-to-machine (M2M) connectivity for applications such as smart utility meters. Traditionally, those connections were large-scale – millions of connected meters – but low volume, with devices unidirectionally sending data into the network using SMS several times an hour, at most.

Of course, telcos also have experience providing global SIM connectivity solutions and have developed expertise and retail knowledge managing millions of SIM cards under one contract with interconnect agreements between operators. That means they can deliver solutions to securely provision, activate, and register devices, which are all critical factors for IoT platforms.

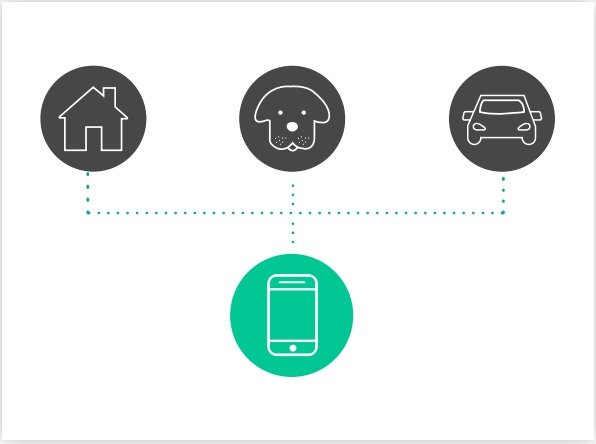
With 5G networks currently in testing, telcos expect to see an explosion of devices and applications that require lower latency at higher data rates, with autonomous vehicles at the top end of this spectrum. At the same time, as low-power, low-bandwidth networks are being deployed, there are vast opportunities to provide connectivity to large numbers of devices to track shipments or provide environmental monitoring using very low data rates.

To address this emerging space, most telcos have created separate IoT business units focused on providing more than just M2M connectivity solutions. For the most part, enterprises are the target

customer for these IoT business units. Smart metering remains an active market and supporting existing customers remains paramount.

Other enterprise opportunities have emerged, however, such as connected appliances, connected thermostats, connected cars, track and trace devices, smart factories, and entire smart cities.

What's more, consumer IoT is starting to emerge as an addressable market.



Some telcos have begun offering IoT services directly to individual subscribers, enabling them to remotely connect to home and leisure electronics products to perform activities such as streaming video from home security cameras, tracking the location of pets, or monitoring where their vehicles are and if they are in use.

As they delve deeper, however, telcos have begun to appreciate that no single organization can create and control the entire ecosystem of applications and business models enabled by IoT. As a result, they are looking outside their organizations and expanding their IoT ecosystem to include more third-party developers and partners.

For example, autonomous vehicles and their real-time, low latency requirements drive alliances such as the one between Vodafone, Huawei, and Bosch, who are testing 5G and Vehicle to Anything (V2X) technology to improve road safety.

In addition, competitive networks are coming to market, often offering connectivity over less-expensive unlicensed spectrum, such as LoRaWAN, which has been deployed in more than 50 countries worldwide and is forecast to capture up to 60% of the device connectivity market by 2021.

OPPORTUNITIES

It's clear that IoT has moved well beyond the hype and is quickly becoming a major market. What's not clear, however, is who will be able to create and participate in the ecosystem that will deliver IoT services to enterprises and consumers. To avoid being relegated to providing commoditized connectivity services while third-party entrants use their networks to create value and reap the lion's share of rewards, telcos must learn from their experience with new technology trends, such as those in the mobile application economy.

The time is now for telcos to establish themselves within the IoT ecosystem, while it is still fragmented and rapidly evolving. Taking advantage of network transformation programs and the move towards Software-Defined-Networking (SDN) and Network Functions Virtualization (NFV), telcos have an opportunity to offer IoT platforms at a much lower cost and with the flexibility and agility required to lay the foundation for new business models.

There are two main areas leaders in the telco space should focus on:

1

At the network and connectivity layer, telcos can provide a full suite of connectivity solutions, including 5G, Narrowband IoT (NB-IoT), LTE Cat M1, and LoRaWAN, and create interoperability between them so customers can mix and match connectivity solutions based on their cost and performance requirements — and without having to architect and integrate it themselves.

2

At the platform layer, telcos can create an open 'operating system' platform that offers value-added services such as device management and metering/billing. Third-party developers can connect their applications to this platform to quickly innovate and build new business models. This will allow telcos to participate in the monetization rather than trying to control the entire value chain by creating a walled garden, as was unsuccessfully attempted in the past with mobile applications (e.g., Vodafone 360).

Rather than locking others out of their IoT ecosystems, telcos must offer the ability to integrate with third-party cloud-based IoT platforms using standard interfaces and protocols to create a path to adoption. Siemens' MindSphere or Bosch's IoT Suite are both examples of successful open IoT platforms telcos could emulate.

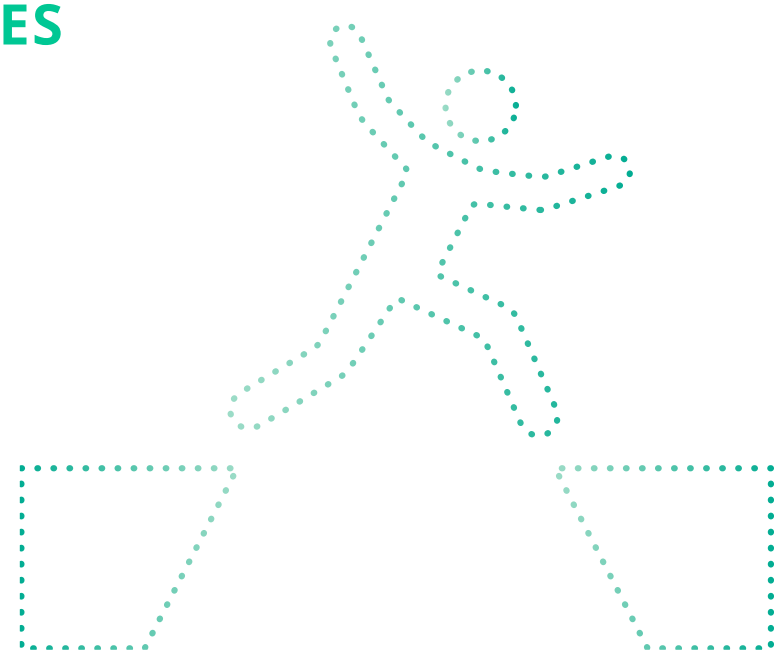
“

Carriers must shift focus from connecting people to connecting things, and access the industry vertical market via IoT to open up new revenue sources. On top of market competition from other telcos, carriers face many challenges.

CHENG QINGJUN, HUAWEI
SIX IOT MODELS: WHICH SHOULD TELCOS CHOOSE?

solace.

CHALLENGES



One of the major challenges telcos face when developing successful and scalable IoT strategies is that their current IoT business units operate more like traditional system integrators than platform developers.

Each new customer, be it a utility, factory or city, requires a new system and a new set of services, which essentially turns each effort into a custom project. While telcos are well versed in the business of providing connectivity and running data centers, this model will not scale, nor will it attract partners and new entrants to build their business within the telco's platform.

Instead, enterprises will choose to create new applications within public clouds and only use telcos for their connectivity needs.

DID YOU KNOW?

79% of IoT adopters think that more than 50% of businesses will be using AI and machine learning to make sense of their IoT data by 2022.

Source: The IoT Barometer 2017/2018

Another challenge is that while IoT is a high-volume market, it has low revenue and margins. According to Huawei's Cheng Qingjun, one IoT SIM card accounts for only 10 percent of the revenue generated by a consumer and the value of connectivity represents only two percent of the entire IoT industry. The value of IoT, therefore, is not in connecting a device and collecting its data, but in the applications built on top of the connectivity and the resulting value reaped for the end-user.

This challenge is similar to the one faced by public cloud operators. However, they have built a set of tooling and commercial models on top of their infrastructure that adds value for their customers and for which the customers are willing to pay. This is another model telcos can emulate.

The question then becomes: how can telcos create an IoT operating system and open ecosystem that provides value to innovators and developers beyond basic connectivity? And what exactly should it look like?

AT A HIGH LEVEL, THIS TELCO IOT OS PLATFORM SHOULD CONTAIN:

1. **A connectivity layer** that can handle any data volume, from millions of connections sending only a few bytes a few times an hour, to a small number of connections (e.g., a factory) sending hundreds of gigabytes of data per minute. This connectivity layer should also be able to accept any interaction, from billions of devices periodically connecting and 'dumping' logged data into the network, to millions of end-points – such as cars – that require 'always-on' connectivity.

These different scenarios also have different latency requirements; connected cars operating in V2X mode require extremely low latency, whereas updating the status of ocean-bound shipping containers is much less time sensitive.

2. **A value-added layer** that provides easy-to-consume services such as orchestration, analytics, device management, security, metering, and billing that developers can use to help build out their applications. It should also support cloud interoperability, so developers incorporating services from the major cloud providers can quickly connect to and interoperate with the telco platform.

To make the platform cost-effective for consumers, telcos should create a multi-tenancy fabric to onboard new customers and projects quickly (in minutes at best, or days at worst) in a replicable manner. Multi-tenant capabilities must be architected into every layer right from the start.

CONSIDERATIONS

Given these challenges, how can we set out a framework of technology and business considerations for telcos?

First and foremost, telcos must redefine their target market. Looking at the runaway success of public clouds, it's evident that the developer is the main driver and value creator.

The old tactics of telcos no longer work. Traditionally, very little actual development took place in-house. Telcos typically employed system integrators to deliver projects, whether it be OSS (operations support system) and BSS (business support system) projects or network projects. These projects could take anywhere from two to five years to complete but, even considering their lengthy production time, would still deliver immense value.

In today's fast-paced, cloud-first world, this system no longer works. It's not acceptable for telcos to work at system-integrator speed. Instead, they must

adapt to working at developer speed. For telcos to be successful, it's integral that they start understanding and thinking like developers.

THINK LIKE A DEVELOPER

So what does a typical developer journey look like? Here's a run through of an average process from start to finish:

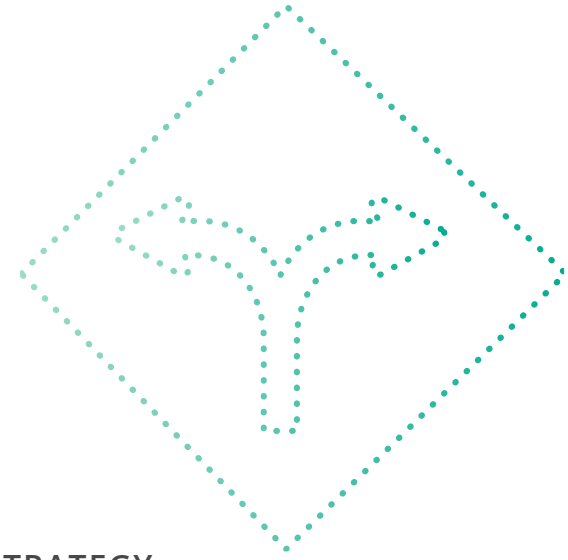
1. A new idea takes shape and prototyping begins.
2. Developers choose a cloud platform, a programming language, and a set of open-source tools to kick-start the prototyping process. Note: to avoid the need to call an account manager, negotiate, or create a custom contract, it is essential in this phase to offer free access to services and platforms.
3. Once the application evolves into the stage of small implementations, the developer is ready to start spending some money. However, it's important that the interactions remain completely digital — developers generally aren't looking for phone calls or discussions with salespeople.
4. After the first successful prototypes, developers start looking for small-scale (but fully functional) pilot projects. These projects will require the full stack of production features, including security, high availability, low latency, etc. At this point, it is also important to understand possible scaling scenarios, both from a deployment perspective as well as from a commercial perspective. Developers are looking for the freedom to deploy and interoperate between the telco platform and the public cloud.

Ensure you're creating the right developer experience by becoming a digital business.

Remember that developers prefer not to use the phone. All interactions — from opening an account, to provisioning of services, to invoicing — must be moved to a portal to be successful with this audience. The inclusion of blogs, community forums, and self-learning modules are paramount in a digital business catering to the developer crowd.

It's not enough for telcos to think like developers; they need to prove that they understand and are catering to their desired audience. These developers understand DevOps in-depth and are cloud-native. By hiring other developers and creating a new unit, telcos can prove that they are free from the traditional telco operations and restraints.

APPROACHING THE NEW ROLE IN IOT



STRATEGY

It's one thing to observe what it takes to build an IoT-TPaaS, but how can telcos take this advice and put it into action?

The first step is to define their private / public cloud strategy. Telcos need to break free from the legacy mindset of trying to compete directly in every area, and instead embrace existing technologies such as those offered by Pivotal Cloud Foundry, Red Hat OpenShift, Kubernetes and others that allow DevOps teams to create the foundation that works equally in a private cloud setting and in all the major public clouds.

In addition, on-ramps from their own cloud to all the public clouds via APIs and event-stream interfaces pave the way for developers to quickly and seamlessly tap into cutting-edge innovations in machine learning, AI, and blockchain.

This approach creates opportunities for strategic partnerships with public cloud and IoT platform providers, and can enable an open and scalable ecosystem for developers to experiment with their technologies of choice, without additional data and event integration efforts.

With the importance of very low-latency scenarios (e.g., vehicle-to-vehicle communications) and the emergence of edge computing, telcos are in a prime position to offer hosted capabilities of data aggregation, filtering and analysis (in real-time as well as in batch) directly in the mobile core network.

To scale the operations of the IoT-TPaaS, all components, services, and applications need to be designed to work in a multi-tenancy environment, right from the start. This entails complete separation of data, identities, and security set-up. Furthermore, data privacy regulation requires for end-users—be that consumers or businesses—to be able to finely control and report on which data items are being processed, when and by whom.

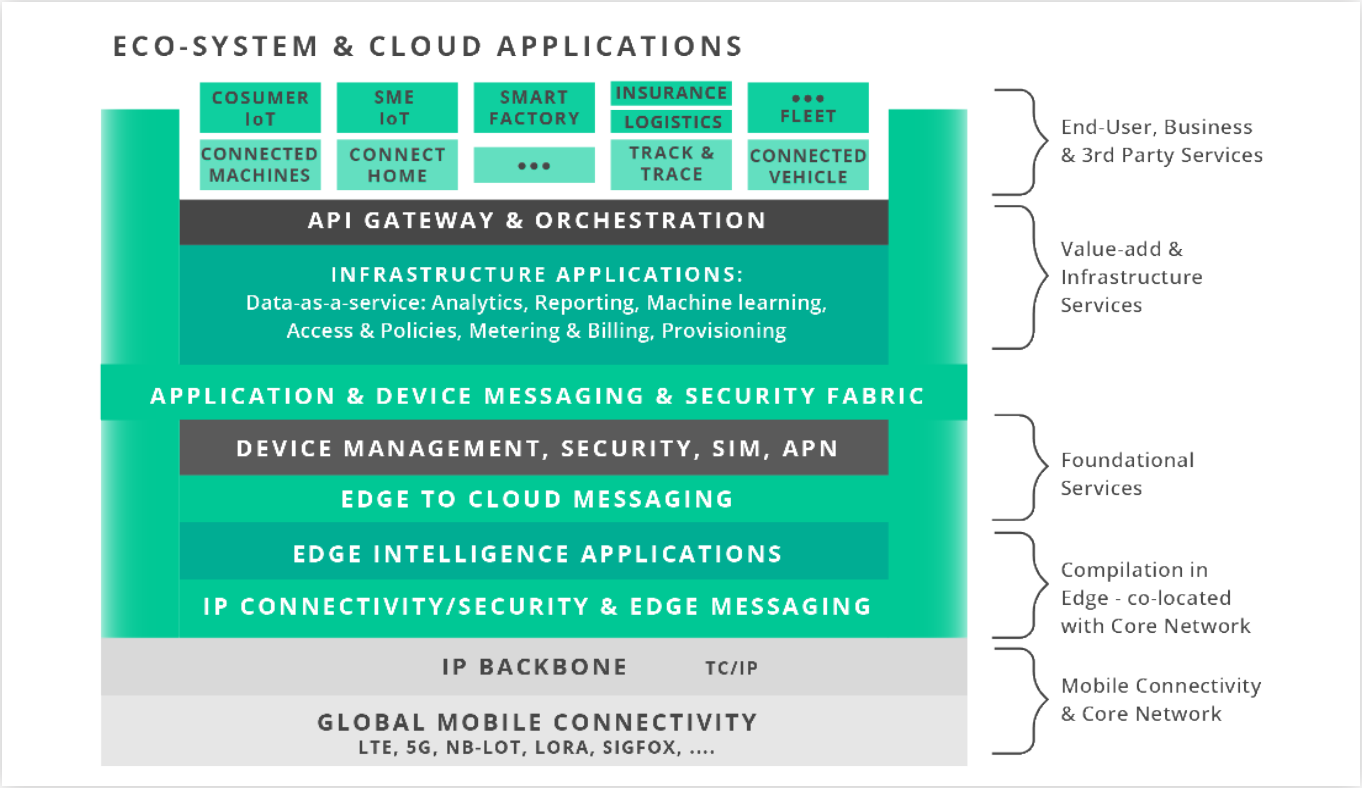
Overall, the IoT-TPaaS must combine all the tools and development processes known and loved from public clouds, while adding flexible and lightweight global connectivity and interoperability with existing cloud platforms, all while creating the required security and data privacy frameworks.

TECHNOLOGY AND TOOLS

To properly approach their foray into the IoT world, telcos must equip themselves with the right technology and tools. Here's a view of the bare essentials from the bottom up:

- **Device connectivity:** interoperability of networks (e.g., 5G, LoRaWan, NB-IoT) to cater to all connectivity requirements and device types.
- **Data connectivity & interoperability:**
- Deploy a global data and event distribution fabric that can handle various patterns and interactions (starting at the edge and co-located in the core network) and distribute it via aggregator nodes to the central cloud / public clouds.
- Support of a multitude of SLAs (from best effort to 100% guaranteed), event rates of up to millions of events per second.
- Flexibility to support multi-tenancy, from shared infrastructure to dedicated VPNs.
- **Security fabric & data privacy:**
- A security model that starts at the device layer and seamlessly deploys at the edge, the central cloud and the APIs.
- Integrated identity, data access control and unlimited auditing of data flows across all layers and applications, allowing for federation across producers and consumers of data services in the entire ecosystem.

THE TECHNOLOGY MAP



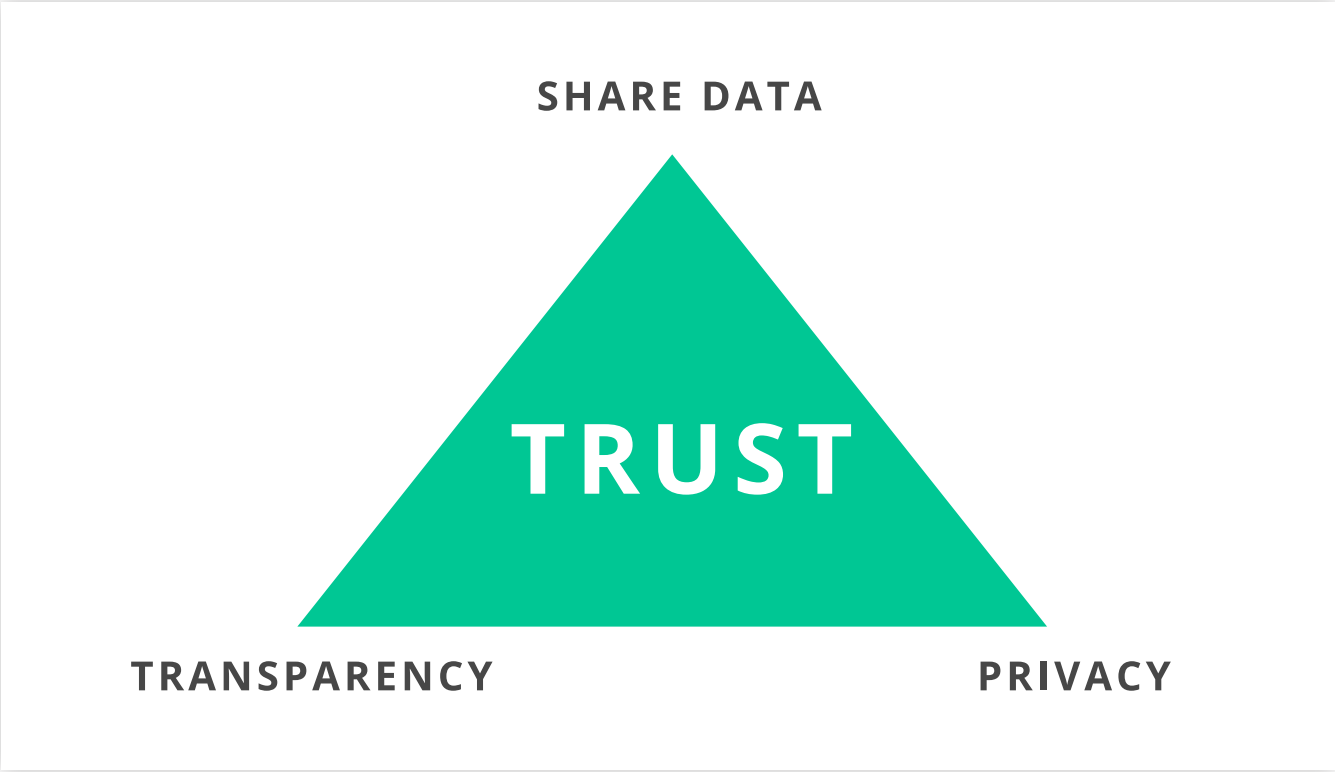
solace.

The key infrastructure element is the highly-scalable data and event distribution fabric. It should support the following:

- Flexible and elastic deployment options, including co-location within the core network to provide low latency edge computing, robust and fast WAN transmission over the packet data network, and private and public cloud environments.
- Resilient and self-healing.
- Dynamic routing capabilities to allow for topic-based pub/sub interactions regardless of where producers and consumers are located. In particular, it should allow for applications and services to be re-deployed without manual re-configuration as needs evolve.
- It scales in multiple dimensions, from the number of connections at the edge to high-volume continuous data streams in the application and API layers.

To provide the multi-tenancy required, the messaging fabric must support the secure separation of connections and data. Security is a key tenant of the messaging fabric which includes authentication, authorization, encryption and fine-grained data access policies controlled by the data owner.

MANAGING PRIVACY AT SCALE



Let's use an example to illustrate. Say a parent purchases a set of bag tracking devices for their family which allows them to keep tabs on their location via a mobile app. As part of the service, they agree for the location data to be consumed by additional services, such as notifications of unexpected locations (e.g., the child leaves the school grounds).

However, during the holidays, they employ an au-pair and want to federate this data to a new user and device for a specified time.

The architecture allows for a) visibility and control of which data items from which tracker are shared where and when and b) run-time enforcement of these rules directly executed within the messaging fabric so no data will flow unless explicitly activated.

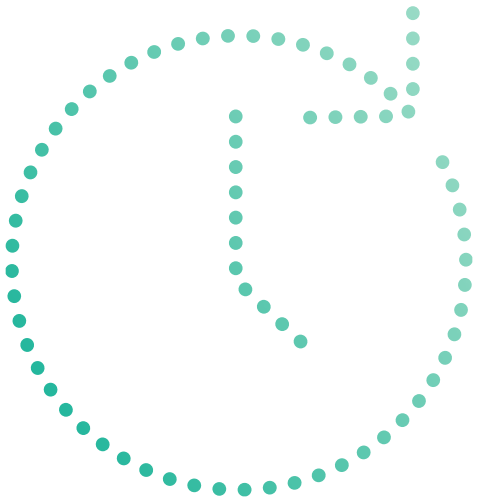
Depending on the project and tenant on the platform, different privacy requirements apply when managing data flows and, in particular, when sharing data within the ecosystem. To manage privacy at scale, we need to design a concept that supports the flexibility and transparency required to comply not only with regulations but also with society's expectations of privacy.

One such approach makes a clear separation between:

1. The definition of data access control, its management and 'opt-in' workflows; and,
2. The run-time enforcement of access & distribution policies.

It all starts with managing identities at scale, including each device, user, and organization, all the way to modeling individual data items directly generated from the devices (as well as data services provided to third parties). Modeling relationships between real (devices, users) and abstract (data items and services) identities allows for transparency and data lineage reporting to the owner of the data.

Once modeled, the owner of the data can agree or opt-in to share their data with third parties and other end-users. Once agreed on, and only if agreed on, the messaging fabric will activate the required data flows across the entire architecture.



CONCLUSION

There's no doubt that the IoT market is currently booming — and little question that traditional telecommunications providers are struggling. Taking into account the position that IoT is in and the experience many telcos have in the domain, the opportunity for telcos in IoT is one too good to pass up.

It's important to understand the opportunities and challenges, and carefully create a strategy around how to best enter the market.

However, to succeed in the field it is essential for telcos to make some changes to their traditional practices and adapt to the new creators and consumers of the IoT world. Telcos should work to understand and think like developers to free themselves from outdated operations and constraints.

By offering a platform that is componentized and interoperable at a global scale, telcos will allow the end-developer to choose which services to use—either build their own or quickly integrate third party, cloud-based offerings into their applications.

Telcos can succeed by using IoT data and event distribution as the foundation to create the required agility and flexibility for economies of scale. By having fine-grained privacy controls built into the platform, telcos can enable data to move without boundaries. And, similar to public cloud platform providers, telcos can drive adoption by creating commercial models that attract developers and businesses from small pilot to roll-out at a global scale. It is imperative that telcos become digital businesses and do not rely on traditional forms of account management in order to attract this new breed of potential customers.

The opportunity to exist within the IoT ecosystem is one that will undoubtedly be met with challenges, but joining the IoT ecosystem will be how telco leaders enter into the future of communication and write the next chapter of their story.

Ricardo Gomez-Ulmke **is Vice President of IoT at Solace. He works closely with customers and partners, helping to shape the vision of their IoT initiatives. With over 20 years of experience as a business technology professional, Ricardo has worked across many industries and technology cycles, always pushing the boundaries of traditional thinking to create lasting competitive advantage. Ricardo applies his passion for real-time, event-driven systems in use cases such as connected vehicles, IoT-as-a-Service, and Industrial IoT.**

ABOUT SOLACE

We are the creators of PubSub+, an advanced event broker that can be used to create an event mesh. As the only unified event broker that supports publish/subscribe, queueing, request/reply and streaming using open protocols and APIs across hybrid cloud and IoT environments, we rapidly and reliably route information between applications, devices and people across clouds. Established enterprises such as SAP, Barclays and American Express as well as high-growth companies such as VoiceBase and Jio use our smart data movement technologies to modernize legacy applications and successfully pursue analytics, hybrid cloud and Internet of Things strategies.

Learn more at solace.com.

A FEW OF OUR CUSTOMERS

OUR FEATURED PARTNERS

solace.