IoT Now: ISSN 2397-2793

2024 • VOLUME 14 • ISSUE 3

IoTNOW

HOW TO RUN AN IoT ENABLED BUSINESS

COVER INTERVIEW

Ryan Keefe explains why it's time for SIMPL IoT connectivity

IoT Now CEO Guide to Mitigating Roaming Risks 2024

PLUS: How to navigate the multicarrier management maze • Have permanent roaming regulatory issues been resolved? • Mobile operators to cash-in on IoT roaming • How to unlock the future of agriculture with eUICC • Is IoT data and security management ready for cloud-connected IoT devices? • Read the latest News, Features and Interviews at **www.iot-now.com**

TRANSFORMA INSIGHTS

Global Advisors on IoT, AI and Digital Transformation

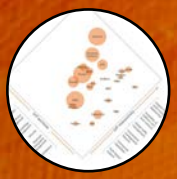
Transforma Insights can increase your revenue, reduce your costs, and limit your exposure to risk

How?

We're glad you asked...

Our white papers, webinars and other marketing support will expand your lead pipeline

Every company's top priority is selling. We can support by building your profile and feeding the sales funnel. In the last 12 months we have supported connectivity providers, platform vendors, hardware makers and many others in promoting their products and services to would-be customers through tailored white papers, events, webinars and more.



Our deep knowledge of the vendor community can ensure you pick the right suppliers who can deliver what you need

Our regular immersive benchmarking reports in IoT, AI and other emerging techs are used by clients to select the right vendor for them. We also undertake numerous client-specific vendor selection engagements, including recent projects supporting an industrial equipment maker select an IIoT platform and an auto vendor to choose a connectivity provider.

Our understanding of market dynamics means we are the best placed to advise on potential M&A, helping you make the right decisions

Bad M&A decisions can have the most serious repercussions. Our understanding of the companies, technologies and markets puts us in pole position in vendor selection and technical/commercial due diligence. We regularly work supporting Private Equity due diligence, and technology vendor acquisition target identification and rating.

Our ultra-granular IoT and AI market forecasts ensure that you're pursuing the right opportunities

Transforma Insights provides the most granular market forecasts across our technology markets, particularly in IoT and AI. Our country-by-country forecasts include detailed technology splits and use-case level granularity. If you want to identify the right markets to pursue, set company priorities, or just set sales targets, they are an invaluable resource.

Our tracking of the complexities of the rapidly evolving regulatory environment mean your risks are mitigated

Regulation is fast-moving today and mis-steps could have catastrophic implications. Our new Regulatory Database helps enterprises and technology vendors navigate through the increasingly complex regulatory environments associated with enterprise digital transformation, including related to Artificial Intelligence, Internet of Things, Data Sharing and Privacy.

Sign up to your free 'Essential' subscription to explore our research at: transformainsights.com/signup/essential

transformainsights.com enquiries@transformainsights.com @transformatweet

The IoT Now CEO Guide to Mitigating Roaming Risks 2024

06 COVER INTERVIEW

10 MULTICARRIER MANAGEMENT

12 CASE STUDY

IN THIS ISSUE

04 MARKET NEWS
China targets 3.6 billion mobile IoT connections, Oracle integrates AT&T IoT connectivity into enterprise communications platform

06 COVER INTERVIEW
Ryan Keefe, the chief operating officer of SIMPL, tells Transforma Insights' Matt Hatton that it's now time to keep IoT connectivity SIMPL

10 MULTICARRIER MANAGEMENT
How SIMPL is revolutionising IoT and fixed wireless access deployments

12 CASE STUDY
How agribusiness is accessing new use cases with eUICC and SIMPL

14 PERMANENT ROAMING
Transforma Insights demystifies the resolution of permanent roaming regulatory issues

18 SECURE ROAMING
Antony Savvas assesses how modern SIM platforms are supporting cloud-connected IoT devices

20 IoT ROAMING CONNECTIONS
How IoT roaming is driving new revenue for mobile network operators

22 EVENT DIARY
Where to go and who to see

News in Brief

Smart meters evolve from analogue to digital

In a report titled, 'Electricity Smart Meters: Government policies and sustainability initiatives will drive 2.1 billion connections in 2033' **Transforma Insights** estimates that the total number of electricity smart meter devices will grow to reach 2.1 billion in 2033. The firm says smart metering systems either use wireless communication options or fixed wired connections such as powerline carrier (PLC). A wide range of different wireless communication options have been used, such as Wi-Fi, RF mesh networks, LoRa, Wize, Zigbee, NB-IoT, traditional cellular communication technologies (2G/3G/4G) and Wi-SUN.

Technologies such as PLC and RF mesh are currently the most common primary communication technologies with a share of 60% of devices shipped in 2023. The vast majority of the remaining new devices use 5G massive machine-type communication (mMTC) (including NB-IoT and LTE-M) and non-mMTC LPWA (including, for example, LoRaWAN) as their primary means of communication. In 2023, 5G mMTC had a share of 17%, non-mMTC LPWA had a share of 10%, 4G had a share of 9% and short range had 2%. In 2033, 5G mMTC (share of 32%), LPWA non-mMTC (30%) and PLC and RF-Mesh (30%) will be the pre-eminent means of connectivity for new devices.

Remote patient monitoring to grow at 12.8% CAGR, reports Berg Insight

Berg Insight has reported that the number of remotely monitored patients reached 76.7 million worldwide in 2023 as the market acceptance continues to grow in several key verticals. This number includes all patients enrolled in mHealth care programmes in which connected medical devices are used as a part of the care regimen. Connected medical devices used for various forms of personal health tracking are not included in this figure. Berg Insight estimates that the number of remotely monitored patients will grow at a compound annual growth rate (CAGR) of 12.8% to reach 140.1 million by 2028.

The three main applications are monitoring of patients with sleep therapy devices, glucose level monitoring of patients with diabetes and monitoring of patients with implantable cardiac rhythm management (CRM) devices. Sleep therapy is by far the most connected segment, dominated by **ResMed**. In 2023, approximately 32.2 million sleep therapy patients were remotely monitored, which has more than doubled since 2018. The growth is driven by the compliance monitoring requirements introduced in the US and across European countries.

Glucose level monitoring has grown in the last few years and is now the second largest segment with 12.6 million connections at the end of the year. The growth is driven by the increased adoption of continuous glucose monitoring (CGM) systems from providers such as **Abbott** and **Dexcom**. Other device categories include ECG, telehealth, medication compliance, blood pressure monitors and others. The fastest growing market segments in the next five years are anticipated to be remote ECG monitoring and medication compliance monitoring.

"With advancements in AI and machine learning, mHealth platforms are evolving from monitoring tools to comprehensive systems that assist in diagnosing and treating patients, paving the way for more effective healthcare," said Vatsala Raina, an IoT analyst at Berg Insight.

China targets 3.6 billion mobile IoT connections by 2027

China's Ministry of Industry and Information Technology has unveiled a plan to push the development of the mobile Internet of things (IoT), aiming to boost the sector's supply, innovation capabilities and industrial value. By 2027, China will strive to further improve its mobile IoT ecosystem, with the number of mobile IoT terminal connections expected to exceed 3.6 billion, according to the plan. The country expects to support the establishment of more than five mobile IoT industrial clusters and set up over ten mobile IoT industry demonstration bases by 2027, it said.

The plan outlined four key tasks, namely strengthening the foundational IoT network, enhancing industrial innovation capacity, boosting the integrated application of smart technologies and fostering a favourable development environment. China will promote the application of mobile IoT in fields such as intelligent connected vehicles, healthcare and smart homes, according to the plan.

For intelligent connected vehicles, it said efforts will be made to drive the application of mobile IoT in scenarios like driving monitoring and autonomous driving, and realise functions like information exchange and sharing, complex environment perception and intelligent decision-making.

The ministry said it will also work to accelerate the integration of mobile IoT with key industries to support their digital transformation and new industrialisation. By the end of July this year, the number of mobile IoT connections in China neared 2.55 billion, accounting for 59% of China's total mobile terminal connections, official data showed.

Swisscom Broadcast and Nokia launch Drones-as-a-Service network in Switzerland

Swisscom Broadcast has selected **Nokia** to deploy a nationwide Drones-as-a-Service network across Switzerland. 300 Nokia Drone-in-a-Box units are planned for deployment to enable emergency response, perimeter protection and infrastructure inspection, which will help keep public safety workers safe. The companies will continue cooperating with competent regulatory bodies to ensure that operations comply with regulatory frameworks, especially from spectrum and aviation safety standpoints.

This will be the second nationwide Nokia Drone Networks project after Belgium's **Citymesh** deployment. It will support Switzerland's public safety and Industry 4.0 efforts and highlight Nokia's strength in modernising digital infrastructure projects and utilising mission-critical industrial edge computing (MXIE) with the support of 3GPP technologies for beyond visual line of sight (BVLOS) autonomous operation.

Public safety agencies in Switzerland will tap into the nationwide drone network by requesting a drone flight, similar to a ride-sharing service, from Swisscom Broadcast. They will also be backed up by a service portfolio with expertise, compliance, data collection and analysis of the collected data from Nokia and Swisscom Broadcast. The deployment is expected to be available in all areas of Switzerland.

"We are pleased to select Nokia as a partner for this important infrastructure project in

Raghav Sahgal, Nokia

Switzerland. Together, we can speed up the go-to-market of our Drones-as-a-Service offering to our customers in the industrial and public safety landscape in Switzerland," Dominik Müller, CEO at Swisscom Broadcast, said in a media statement. The integration of our existing People Density Tool and our Drone Operations expertise with Nokia's industrial grade hardware in combination with an open and future proof Software architecture is an important key to support such large-scale projects."

"We are proud to partner with Swisscom Broadcast, a true innovator in Drones-as-a-Service operation, for this important project to establish a nationwide Drones-as-a-Service network in Switzerland," said Raghav Sahgal, president of cloud and network services at Nokia. "Nokia's Drone Networks solution enables large-scale projects as it incorporates our mission-critical industrial edge (MXIE) technology to power its advanced computing functions and software. It will undoubtedly help Swiss enterprises gain access to a superior Drones-as-a-Service offering to enhance worker and public safety."

Oracle integrates AT&T IoT connectivity into enterprise communications platform

Oracle is incorporating **AT&T** IoT connectivity and network application programme interfaces (APIs) into its Enterprise Communications Platform (ECP). The initiative will enable Oracle's industry cloud application customers to connect and manage their IoT devices on the AT&T network all in one platform, enabling reliable and secure communications.

Supported by AT&T, ECP delivers IoT connectivity and near real-time communications to Oracle's suite of industry cloud applications. With integrated capabilities such as IoT edge application management, this all-in-one offering removes the customer burden of managing complex integrations and network contracts.

Built on the high performance and security of Oracle Cloud Infrastructure (OCI), the unified communication and edge architecture gives businesses the connectivity and real-time data intelligence they need to power critical new services and experiences. The integration with AT&T IoT connectivity and network APIs is available across OCI regions in the U.S.

"Our mission has always been to help improve the way the world communicates, and with ECP supported by AT&T and FirstNet, we're taking a massive step toward that vision," said Andrew Morawski, executive vice president and general manager at Oracle Communications. "Together, we can help organisations across industries benefit from the full potential of 5G, by building a new generation of vertical applications offering endless opportunities to innovate."

Sarita Rao, the senior vice president of AT&T Partner Solutions, added: "By teaming with Oracle to incorporate IoT connectivity and programmable APIs into Oracle industry applications, we are providing businesses and organisations a tighter level of integration between the network and application, driving performance and reliability gains while also eliminating integration requirements and separate contracting events. It's co-creation at its best."

News in Brief

Kargo unveils lift for forklifts and AGVs

Kargo has announced the Kargo Lift, a new addition to the Kargo product portfolio, that has been purpose-built for forklifts and automated guided vehicles (AGV). The Kargo Lift extends the AI capabilities of the Kargo Towers, automating critical processes and enhancing visibility for warehouses, manufacturing facilities and distribution centres.

"Our goal has always been to push the boundaries of what's possible in industrial automation," said Sam Lurye, the founder and CEO of Kargo. "Like with all Kargo products, we have meticulously designed the Kargo Lift to be easy to install, drive immediate value and handle all the complexity of an industrial environment."

Intelligent Living and Specifix join forces for smart locks

Intelligent Living Application Group has announced that it has entered into a cooperation agreement with **Specifix**. Specifix deploys its artificial intelligence (AI) assisted robotics research and development for construction and industrial engineering services and technology. This cooperation underscores its commitment to enhance its technological capabilities for new product development which will expand its market presence.

Specifix's approach and technology align with Intelligent Living's goal for development of smart locks and smart home security devices. The cooperation will enable it to use Specifix's technologies to enhance research and development abilities, and even new automated industrial production processes to help improve efficiency and precision.

It's time for IoT connectivity to keep it SIMPL

Ryan Keefe, the chief operating officer of SIMPL, tells Matt Hatton, the founding partner of Transforma Insights how the company is disrupting the permanent roaming market by preloading its SIM card with native operator profiles. This brings flexibility and choice with an easy-to-use management via the SIMPL platform

The biggest misunderstanding or unknown or maybe intentional omission from some providers is not sharing that roaming agreements between MNOs are not perpetual

Matt Hatton: At Transforma Insights we do a lot of work looking at how cellular-based IoT connectivity is delivered, including our recent Communications Service Provider IoT Peer Benchmarking report. One of the things that comes up is that there is continuing friction around both roaming and the emerging eSIM localisation. How do you see it?

Ryan Keefe: Our view is that there's a natural friction between the emerging technologies we are working with and some of the existing permanent roaming solution providers in the space. They've spent a lot on capital investment in infrastructure and until now it did require heavy integration. For every carrier you want to deploy an international mobile subscriber identity (IMSI) with, you typically need a subscriber management data preparation + (SM-DP+) integration. One of the challenges with some of the existing players in the space is that domestic US mobile network operators (MNOs) are not willing to license or lease IMSIs. So, most end up with IMSIs from international carriers to roam back into the US, where there is high risk of permanent roaming. But with the evolution of the GSMA standards it's much easier to localise and be disruptive.

The localisation that we provide is for specific carriers in the US pre-loaded at time of manufacture, and then the ability using SGP.22+, we refer to it as .22+ or 22 1/2, and with work in progress to use SGP.32, to be able to localise with activation codes rather than doing a full SM-DP+ integration.

With the SIMPL solution we can get an activation code from any MNO and download it to the SIM alongside the preloaded **T-Mobile** and **Verizon Wireless** profiles. The activation code is essentially the extracted QR code string.

What we've done is disruptive to the permanent roaming models. Our SIM card comes preloaded with T-Mobile and Verizon profiles and new profiles can be added with a carrier activation code. If it's a carrier that we already contract with, then they can buy services from us. If the customer has their own carrier agreements, they can bring their own commercials and manage it in our single pane of glass, SIMPL, side-by-side.

MH: Thinking specifically about permanent roaming, what are the big problems? And specifically problems in the US.

RK: The biggest misunderstanding or unknown or maybe intentional omission from some providers is not sharing that roaming agreements between MNOs are not perpetual. Customers and solution providers will be very exposed to increased rates, capped usage, capped number of SIMs or termination of agreement between MNOs.

And one of the things that most people aren't familiar with is QCI which stands for quality- ▶

of-service class identifier. There are nine classes of SIM priority. In the US, roaming SIMs are QCI 9. For context, a conversational voice connection is typically a QCI 1 priority on the network. First responders in the US are often on QCI 6, which is still pretty high. Most of the rest, where consumer, wholesale and business sit, are QCI 6 or 7. QCI 9 is where all roaming traffic resides, this traffic has the lowest priority assuming there's room on the network, translating into reduced reliability and high latency.

There are numerous permanent roaming customers with buyer's remorse, citing latency and reliability issues. They're looking to come back to domestic networks in the US, but they want to be able to use a single SIM with multiple carriers and download more if they need more. This is really impacting a lot of businesses. Customers are definitely feeling that pain in the US and Canada. That's why we prefer the localisation and why we've built what we've built.

Another thing to consider is quality of revenue, a term more common with private equity. The economics of roaming SIMs generally look better than domestic, so naturally as you're building out your business model and looking at recurring costs, your goal is better margins. But that's not the whole story. I've personally been hired by private equity firms to perform due diligence, and increasingly they scrutinise the risks associated with the revenue derived from permanent roaming agreements. ▶

Ryan Keefe
SIMPL

In one case I know of, it reduced the valuation by 45% because they couldn't guarantee the SIMs would be out there in 30, 60 or 90 days after closing

For instance, roaming agreements between operators is best case a three-year term. But in many cases the carrier can't and won't tell how much time is remaining. So, you may be building a business today in security or point-of-sale where devices might be out there 5-10 years, and you have no idea how long is left on the roaming agreement upon which your connectivity provider is relying. And for someone looking to invest in that kind of company and starting to ask those questions it can be a heavy hit to your valuation. In one case I know of, it reduced the valuation by 45% because they couldn't guarantee the SIMs would be out there in 30, 60 or 90 days after closing. It's something else to consider in the US. And I get it, as a start-up or enterprise venturing into new connected devices, you'll take all the margin you can get. But five years later you have a base built on roaming and PE now has this type of research on their due diligence check list.

MH: What about some horror stories? Do you have some specific examples?

RK: I don't know if I can name names but I have many examples. While working for a mobile virtual network operator (MVNO), I was engaged in a dispute between a US and Canadian carrier where the MNVO's costs increased 25x overnight. In another case, there was a dispute between two MNOs where the main carrier being roamed onto increased rounding up from 1KB to 100KB sessions.

I've also experienced a tier 1 US and a tier 1 EU MNO getting into dispute over 40,000 connections, which by today's standards isn't very much. The US MNO sent a cease-and-desist with 48 hours' notice terminating SIMs that were permanently roaming. Can you imagine the pain the MVNO, and underlying customer went through? This is not an isolated incident.

As you're no doubt aware, the tier 1 US MNOs have become much more aggressive at terminating permanent roaming agreements over the last few years as they seek to stop the revenue bleed they're experiencing from unapproved practices. This has significant downstream effects and has resulted in more than one solution provider filing for bankruptcy

And in yet another experience, several years ago, a Tier 2 US operator roaming onto a Tier 1 operator's network with 500,000 devices was given notice to cease and desist. And the same thing happened again last year with a different Tier 2 operator.

MH: Has the situation changed in the last couple of years? How does the landscape change with eSIM localisation and how do you see the network operators' approach evolving?

RK: This is interesting. Over time you can see the pendulum swing back and forth between the carriers and the aggregators. For instance, initially the carriers would send the business towards the aggregators. Then we saw the carriers invest heavily in IoT, for instance in connectivity management platforms like **Jasper**, **Ericsson**, and **Vodafone** building GDSP and signing customers directly. And they reduced the commitments so anyone could sign direct. What's been interesting with localisation is the pendulum is swinging back to aggregators. We see the MNOs wanting to partner with them for localisation. One big reason is that the carriers won't agree to purchase orders with each other for profiles, so they need to partner. And then the aggregator can work to develop the agreements for the other operators.

And the world has changed. Back 15-20 years ago most of the solution providers had no existing base but today they do. If you're trying to get into disrupting the space now you have to account for that. Most people don't have an escape plan between operators. The buyers don't want a new platform or new application programme interfaces (APIs). So, the big question is how do you manage multiple carriers with legacy and new SIMs on 'day two'? So, we put a big emphasis on that part, creating that horizontal experience with SIMPL.

MH: That brings us on to the topic of the single pane of glass interface across multiple connectivity providers, right?

RK: Yes, that's what I'm talking about. The eSIM evolution solves the localisation problem. But the 'day two' item on the list is how to manage it across all those operators. The SIMPL approach was to integrate with all the platforms, the ▶

customer can bring their own connectivity or buy from SIMPL. All with the same horizontal experience for diagnostics, alerts and automation, and cost savings dashboard enabling them to manage both old and new SIMs together and gives the industry a plan for moving on from using other carriers.

MH: Can I ask you also about online channels? This seems to be a big feature of the SIMPL approach. We see some connectivity providers shy away from online because of most customers' requirements for customisation. But for other customers it's exactly what they want. Is that how you see it?

RK: We identified this as a need in the market after doing a lot of research. One thing we discovered was that according to **Gartner** 80% of research by the next generation of buyers is online. And 44% don't want any interaction with a salesperson at all, and for it to be completely self-serve. We estimate that for 60% of new generation buyers and heavy influencers we have a silver bullet with online channels. The other 40% need more touch points, and those are usually bigger clients. We launched our B2B ecommerce platform 90 days ago and we already have people coming in and buying in a completely self-serve way. These customers can log into our B2B commerce site and have SIMs and service the same day vs. weeks or months from other providers.

MH: One trend we see is that a sophisticated online channel capability is giving customers some confidence of efficient and joined-up fulfilment. Is that how you see it too?

RK: We think it is. We have some ecosystem clients who are more hardware oriented. And we're finding it good to push to these online channels. So, it's not just a joined-up mechanism for us internally but also including the client processes too. I've been joking for years that you can **Uber** a helicopter faster than you can purchase SIMs. That's the reason for us pushing the B2B commerce experience.

MH: Talk me through some of the other features that you see as being the ones that customers really value from a connectivity standpoint.

RK: In addition to the other aforementioned features, mid-cycle billing changes is a big one. It's something the MNOs allow but the MVNOs often don't. A few of our competitors have changed their approach because SIMPL has been offering this. We've even alerted customers before a billing cycle ended, giving them the chance to resolve an issue and avoid a million-dollar overage.

One key advantage we offer is helping customers identify SIM bleed or dormancy waste - an insight that some competitors only share with c-level approval. In addition, our transparency sets us apart; we openly share data on over- and under-utilised pools, whether the carriers are purchased from us or ones you've brought yourself, along with automation tools that drive savings.

Finally, we expose a single API and SIM lifecycle experience connecting to 100 MNOs and delivering 200 built-in key performance indicators (KPIs) with interactive analytics. Customers can also buy or bring their own MNO. Interactive is the key word with our analytics experience.

MH: As another part of our research we've found an increasing importance for connectivity providers to also get involved with the device side of things, is that also part of your experience?

RK: We do offer full kitting and staging and fulfilment for connected things. The client buys the hardware, drop ships it to SIMPL and as orders come in, we fulfil, insert the SIM, provision, update firmware, test and handle support, return merchandise authorisations (RMAs) and even potential churn and saves when a customer calls to cancel.

MH: What message can enterprise buyers take away from our conversation?

You no longer have to be handcuffed to the risk and inflexibility of permanent roaming but can instead now benefit from the power of localisation and data transparency to improve quality and revenue. ■

I've been joking for years that you can Uber a helicopter faster than you can purchase SIMs. That's the reason for us pushing the B2B commerce experience

https://simpliot.com

Navigate the multicarrier maze: How SIMPL revolutionises IoT and fixed wireless deployments

In today's hyperconnected world, where devices outnumber people and the Internet of Things (IoT) is rapidly expanding, managing multiple mobile network operators (MNOs) for IoT and fixed wireless deployments has become an intricate, almost Herculean task. Each MNO operates within its own technological bubble, offering proprietary platforms that vary in protocols, application programme interfaces (APIs) and management tools. For companies looking to scale across regions, the complexity can be overwhelming. Enter **SIMPL** – a **SIM PL**atform that's taking the chaos out of multicarrier management and making global IoT deployment not just possible, but streamlined, efficient and cost-effective

Picture this: You're deploying IoT devices across the US, Europe, and Canada. In the US, you're deployed with the **Cisco Jasper** platform. Cross the Atlantic, and you're working with **Vodafone**'s GDSP. Up north in Canada, you're **Ericsson** DCP. Then, add the intricacies of integrating home grown platforms such as **T-Mobile's Netcracker**'s deployment, **Verizon**'s Thingspace, and **Telefonica**'s Kite, and it becomes clear - this isn't a simple game of plug-and-play.

Each of these platforms is like a distinct language. Getting them to communicate with each other, without data loss or service disruption, requires not just technical expertise, but a considerable investment of time and resources. For companies operating on tight deadlines and even tighter budgets, the stakes are high. A delay or disruption could mean the difference between market leadership and playing catch-up. ▶

SPONSORED ARTICLE

SIMPL: The unifying force in a fragmented landscape

SIMPL's platform has been designed from the ground up to integrate seamlessly with all major MNO platforms. Whether it's T-Mobile Netcracker, Cisco Jasper, Verizon Thingspace, or Vodafone's GDSP, SIMPL brings them together under one roof, offering what the industry so desperately needs - a single, unified pane of glass.

SIMPL's platform isn't just about integration; it's about simplification. With one-touch onboarding, businesses can deploy their IoT devices across multiple carriers without getting entangled in the technical complexities that typically bog down such operations. Imagine a world where your IoT devices can be activated, managed, and scaled with the ease of flipping a switch - that's the reality SIMPL is making possible.

A blended buy and bring your own MNO experience

In addition to its integration capabilities, SIMPL also offers a unique bring your own MNO experience. This feature allows companies to ingest SIMs from their existing MNO platforms, managing both legacy SIMs and new SIMs from SIMPL within the same unified platform. Whether you're dealing with a legacy SIM estate or rolling out new deployments, SIMPL's platform provides a seamless, single-pane management experience. This ensures that companies can maintain continuity and control over their entire SIM portfolio, regardless of the MNO, all while benefiting from the advanced features and streamlined operations that SIMPL delivers.

Ensure quality of service across the globe

One of the biggest concerns in managing IoT and fixed wireless deployments across multiple MNOs is maintaining consistent service quality. While network performance - such as coverage, latency, and bandwidth - can vary greatly between MNOs, SIMPL focuses on what it can control: the behaviour of your SIMs. Through its advanced analytics and algorithms, SIMPL can detect when SIMs start to behave abnormally, whether they become overly chatty, experience connection failures or exhibit inefficient packet sizes and high usage patterns. This proactive approach allows businesses to quickly identify and address issues that could impact customer experience, ensuring performance is optimised across all regions and carriers.

Scalability and flexibility: the hallmarks of a future-proof solution

In the fast-paced world of IoT, the ability to scale quickly and efficiently is crucial. However, scaling across multiple MNOs is no easy feat. Each platform has its own limitations and scaling strategies, which can lead to bottlenecks and inefficiencies.

SIMPL's platform is built for scalability. By integrating with all major MNOs, SIMPL allows companies to scale their operations without being held back by the limitations of any single MNO platform. Moreover, SIMPL's flexible architecture means that businesses can switch between MNOs as needed, ensuring that they always have access to the best possible service and pricing.

Navigate permanent roaming waters with confidence

In the tangled web of global IoT, permanent roaming regulations can feel like walking a tightrope without a net - one misstep and you're in trouble. SIMPL shines a light on which networks you're roaming on, for how long, and how much data you're using, so you have the opportunity to stay in step with regulatory and contractual requirements.

For businesses expanding across borders, SIMPL ensures you can play by the rules. Consider it your compliance safety net - no matter where in the world your devices wander, we've got your back.

The future of IoT is SIMPL

In a world where managing multiple MNOs has traditionally been a complex, resource-draining endeavour, SIMPL is rewriting the rules. By offering a platform that integrates seamlessly with all major MNOs, unifies APIs, simplifies billing and ensures compliance, SIMPL is not just making IoT and fixed wireless deployments easier - it's revolutionising them.

As the IoT landscape continues to evolve, companies need solutions that can keep pace with their ambitions. SIMPL is that solution. It's more than a platform; it's the future of multicarrier management.

For companies looking to navigate the multicarrier maze and emerge victorious, SIMPL offers the map, the compass, and the key to unlocking their full potential. The future of IoT is interconnected, it's global, and with SIMPL, it's finally within reach. **https://simpliot.com**

For companies looking to navigate the multicarrier maze and emerge victorious, SIMPL offers the map, the compass, and the key to unlocking their full potential

Unlock the future of agriculture with eUICC and SIMPL

As the agriculture industry faces increasing pressure to optimise resources, reduce environmental impact, and meet growing global food demand, the integration of connected solutions becomes paramount. Among these technologies, embedded universal integrated circuit cards (eUICC) for both physical (pSIM) and embedded SIM (eSIM) stand out as a transformative tool, enabling seamless connectivity for a wide range of agricultural applications. By adopting pSIM and eSIM technology, the agriculture sector can make use of connected solutions to monitor, analyse and manage various aspects of farming, without the frustration caused by inconsistent cellular coverage, writes Ryan Keefe, the COO of SIMPL

As this equipment migrates across different farms or various sections of large properties, maintaining consistent network coverage becomes a critical challenge

This article explores the benefits of eUICC for the agriculture industry, discusses specific use cases, and highlights the importance of future readiness for **GSMA** specifications, particularly LPAe .22 (although not official, we refer to it as .22+ or .22.5) and .32. We will delve into how eUICC can address critical challenges in agriculture and contribute to a smarter and resilient industry.

The evolution of agriculture and the need for connectivity

In today's rapidly evolving agricultural landscape, even small-scale farmers may depend on over 100 pieces of equipment - ranging from man-powered and robotic tractors to advanced irrigation pumps. This figure represents nearly double the machinery in use just 15 years ago. As this equipment migrates across different farms or various sections of large properties, maintaining consistent network coverage becomes a critical challenge. If a device moves to a new location and loses coverage without the ability to switch network profiles, it effectively becomes a useless brick in the field. Historically, agriculture has been slow to adopt cutting-edge technology, but that's no longer the case.

eUICC in AgTech makes network switching seamless. The future belongs to solution providers who can offer seamless connectivity across multiple native networks, using the latest eUICC technology to ensure that no piece of equipment - and no farmer - is left behind.

The benefits of eUICC in agriculture

1. **Seamless connectivity:** eUICC allow devices to switch between mobile network operators (MNOs), ensuring continuous connectivity in areas with limited coverage. This minimises downtime and ensures data flow across large, geographically dispersed agricultural operations.
2. **Remote management:** eUICC enables remote management of devices, allowing farmers to update network profiles, change service providers and adjust settings without physical intervention. This reduces costs and simplifies managing large fleets of connected devices.
3. **Scalability:** As connected solutions proliferate, eUICC supports the scalable deployment of new devices, crucial for large-scale farming operations with hundreds or thousands of sensors and IoT devices.
4. **Enhanced security:** eUICC offers enhanced security features, such as encryption and authentication, to protect the sensitive data transmitted by agricultural devices, especially for monitoring critical resources like water usage and soil health. ▶

Use cases of eUICC in agriculture

1. **Water level monitoring in soil:** Efficient water management is crucial for sustainable agriculture, especially in regions prone to drought or water scarcity. eUICC-enabled soil moisture sensors can continuously monitor the water levels in the soil, providing real-time data to farmers. This data can be used to optimise irrigation schedules, ensuring that crops receive the right amount of water at the right time. By preventing over-irrigation, farmers can conserve water resources and reduce costs.

2. **Water usage monitoring:** In addition to soil moisture monitoring, eUICC technology can be used to track overall water usage on the farm. Connected water meters equipped with eUICC can provide detailed insights into how much water is being used for irrigation, livestock, and other agricultural processes. This information can help farmers identify inefficiencies and implement strategies to reduce water consumption.

3. **Livestock monitoring:** Livestock health and productivity are closely tied to their environment. eUICC-enabled sensors can be attached to animals to monitor their vital signs, movement patterns, and overall well-being. For example, temperature sensors can detect signs of illness early, allowing for prompt intervention. GPS tracking can also be used to monitor the location and movement of livestock, reducing the risk of loss or theft.

4. **Crop monitoring:** eUICC technology can also be applied to monitor crop health and growth. Connected drones equipped with cameras and sensors can capture high-resolution images of fields, which can then be analysed to detect signs of disease, nutrient deficiencies, or pest infestations.

5. **Climate monitoring:** Weather and climate conditions play a significant role in agricultural productivity. eUICC-enabled weather stations can be deployed across farms to monitor temperature, humidity, wind speed, and precipitation. This data can help farmers make informed decisions about planting, harvesting, and protecting crops from adverse weather conditions.

Future readiness with GSMA specifications LPAe .22 and .32

As eUICC technology continues to evolve, it is essential for the agriculture industry to stay ahead of the curve by adopting solutions that are future-ready. The GSMA specifications LPAe .22 and .32 introduce new features and capabilities that will further enhance the benefits of eUICC in agriculture.

LPAe .22: This specification focuses on improving the interoperability of eUICC devices across different networks and service providers. For agriculture, this means that eUICC-enabled devices can seamlessly switch between networks, even in regions with limited connectivity options. This is particularly important for ensuring continuous operation in remote or rural areas.

GSMA Spec .32: The .32 specification introduces enhanced security features, such as improved encryption and authentication protocols. These features are critical for protecting the vast amounts of data generated by connected agricultural devices. With the increasing prevalence of cyber threats, adopting .32-compliant eUICC solutions can help safeguard sensitive information and maintain the integrity of agricultural operations.

The adoption of eUICC technology in agriculture presents a significant opportunity to revolutionise the industry by enabling more efficient, sustainable, and connected farming practices. From monitoring soil moisture and water usage to tracking livestock and crop health, p/eSIM provides the seamless connectivity and remote management capabilities needed to optimise agricultural operations.

As the industry continues to embrace digital transformation, it is crucial to consider future readiness by adopting solutions that comply with the latest GSMA specifications, such as LPAe .22 and .32. By doing so, agricultural businesses can stay ahead of the curve, ensuring that their operations are not only efficient and sustainable but also secure and resilient in the face of evolving challenges.

In the years to come, eUICC technology will undoubtedly play a central role in shaping the future of agriculture, driving innovation and enabling a smarter and more connected world.

The adoption of p/eSIM technology in agriculture presents a significant opportunity to revolutionise the industry by enabling more efficient, sustainable, and connected farming practices

https://simpliot.com

Permanent roaming for IoT: a regulatory issue finally resolved?

One of the major challenges for deploying multi-country cellular-based IoT connectivity has been the restrictions placed by regulators and host operators on the use of permanent roaming. In this article, Matt Hatton, the founding partner of Transforma Insights, explores the current status of permanent roaming, the recent strides made by IoT connectivity providers to deliver compliant services, the impact of the shift from roaming to eSIM localisation, and the continuing challenges in the space

Permanent roaming: the constant challenge

A recent Transforma Insights report 'Regulatory landscape for the Internet of Things'[1] analysed the various regulations that affect deployments of the Internet of Things and the associated provision of connectivity, device functionality, and management of data, as well as regulatory drivers and barriers to IoT adoption, as illustrated in **Figure 1**.

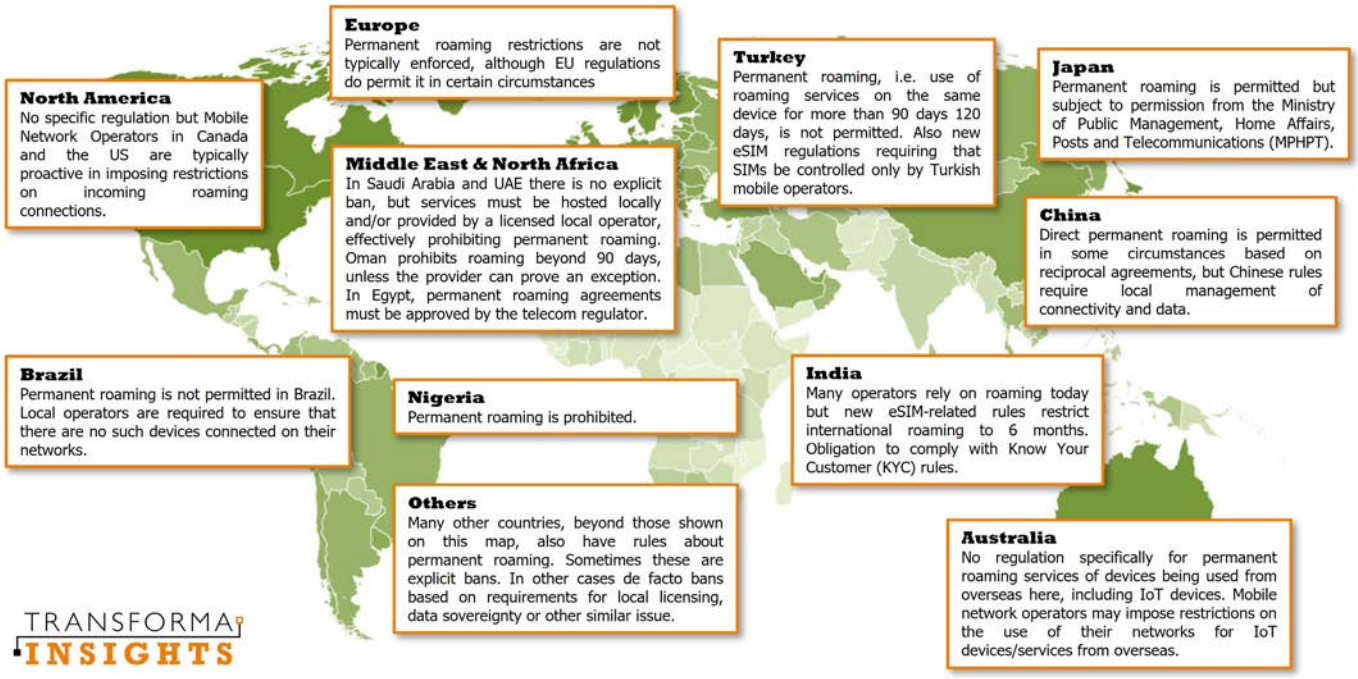
One particularly relevant set of regulations for supporting IoT relates to 'extra-territorial use of E.164 numbers' (which is generally referred to as 'permanent roaming'). Many, perhaps most, IoT deployments using cellular connectivity involve ▶

Figure 1: Seven key regulatory areas for the Internet of Things
[Source: Transforma Insights, 2024]

Hardware and spectrum	There are many long-standing regulations related to factors such as RF regulations, device certification and product safety which are relevant to IoT. Recent years have seen a flurry of regulations related to energy efficiency and sustainable disposal. We also consider import/export controls.
Licensing and permanent roaming	Relates specifically to the provision of public networks (most usually cellular networks) and very specifically the restrictions that might apply to extra-territorial use of E.164 number (otherwise known as 'permanent roaming').
Privacy	Some of the first regulations affecting IoT data were those related to data privacy more broadly, which address the collection, storage, and processing of personal data. This includes the EU GDPR regulation and various consumer privacy regulations around the world.
Security	The last few years have seen a major expansion in the amount of legislation related to cybersecurity in general and IoT device security particularly. There are also numerous examples of codes of practice pertaining to cybersecurity topics such as passwords and firmware updates.
Data sovereignty and access/portability	Many countries have particular rules about the circumstances in which data may or may not be accessed by government, shared within countries and sent overseas. This includes the US CLOUD Act and various EU regulations such as the Data Act and the Data Governance Act.
National resilience	As a further evolution on the requirements for device security and data sovereignty, an increasing number of countries are implementing stricter rules related to national resilience and protection of critical national infrastructure (CNI), including rules around procurement.
Regulations in vertical sectors	As well as the general regulations related to IoT and associated fields outlined under the headings above, there are also numerous vertical-specific regulation which can also be relevant for IoT, including in automotive, energy, financial services and the public sector.

[1] https://transformainsights.com/research/reports/regulatory-landscape-iot

Figure 2: Permanent roaming rules around the world
[Source: Transforma Insights, 2024]



connecting devices in multiple countries. Many have specific rules about how that connectivity is supported, in particular whether cellular-connected devices could exist in a state of permanent roaming, i.e. whether a device that is connected by a connectivity provider that is not licensed in the territory could use its roaming agreements with local licensed operators to support a connection that was not simply temporarily roaming but would be present on a permanent basis in that country.

During the 2010s, many regulators, for instance in Brazil, China, India and Turkey, introduced, or more rigorously enforced, rules that prohibited permanent roaming. Sometimes the rules were explicitly against permanent roaming and in other cases were based on local registration requirements or tax obligations. The regulators are often motivated to protect the local market and enforce local rules with which a roaming connection may not comply, such as lawful intercept. Besides this, roaming was never envisaged to include a foreign device permanently being in a state of roaming.

Measures to restrict permanent roaming can come in various guides, for instance related to licensing, taxation, rules on management of eSIM localisation, or know your customer (KYC) rules, all of which can act to effectively prohibit the practice. In many cases, the issue relates to licensing, i.e. the company providing the services needs to be a locally licensed legal entity in the country.

Limitations on permanent roaming are not solely the preserve of regulators. There were also commercial equivalents, particularly in the US and Canada, where the operators themselves in some cases prohibited their roaming partners from having devices permanently roaming on their networks.

Figure 2 presents a summary of some of the rules. We should add the caveat that the rules do change often and there are often exceptions whereby permanent roaming is permitted despite seemingly explicit restrictions to the contrary.

Problem solved?

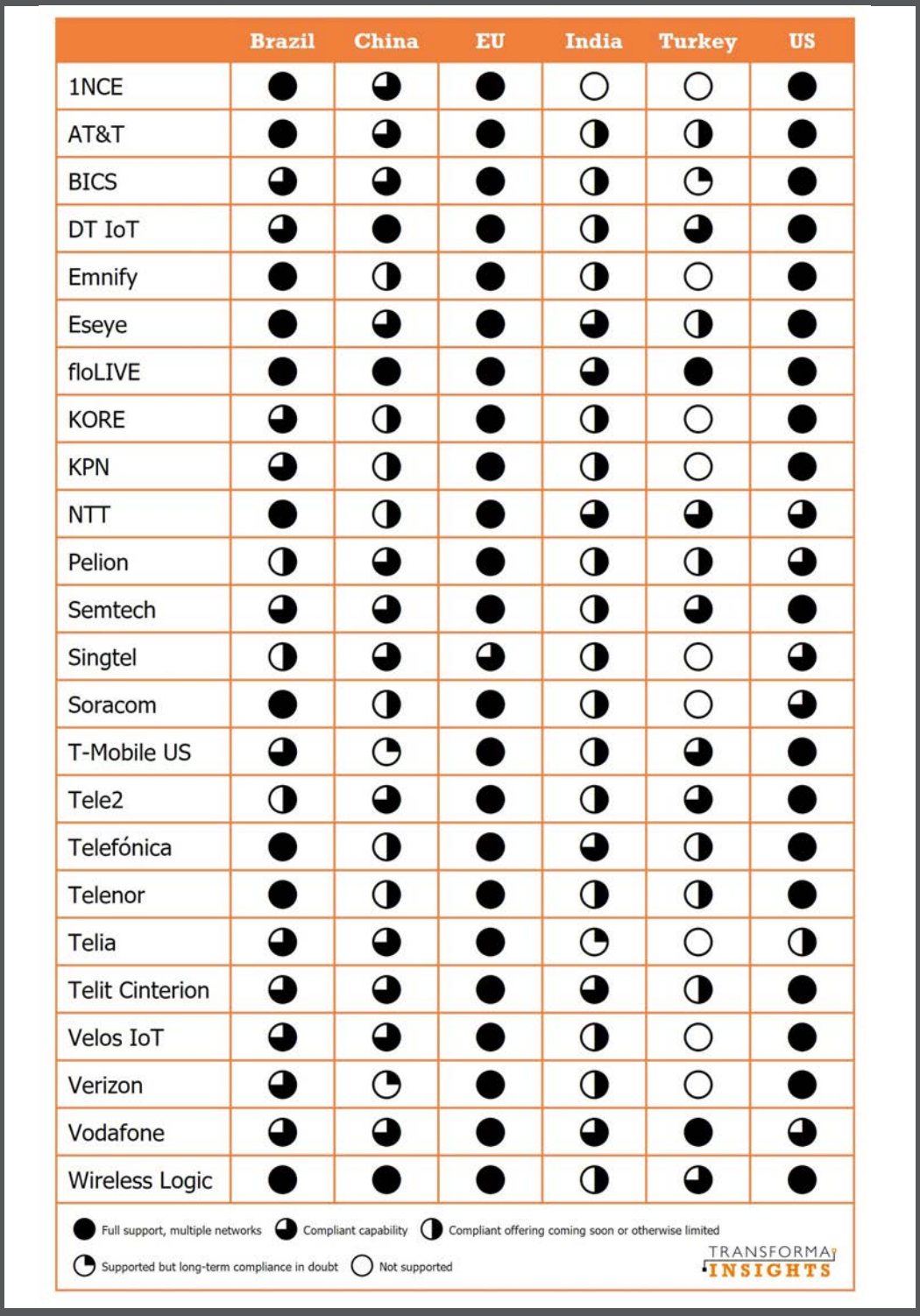
The limitations on permanent roaming have caused some headaches. Historically, roaming was the main – and certainly the simplest – mechanism used by MNOs and MVNOs to support connections across multiple territories. However, over the last decade IoT connectivity providers have made great strides in addressing the challenge.

In July 2024, Transforma Insights published its annual 'Communications Service Provider (CSP) IoT Peer Benchmarking report'[2] which analyses the capabilities and strategies of 25 of the world's leading IoT connectivity providers. As part of that research, we assess the ability of the companies to provide compliant connectivity around the world. Specifically this year, we asked each of the CSPs about their ▶

[2] https://transformainsights.com/research/reports/csp-iot-peer-benchmarking-2024

The compliance situation in India is in flux with ongoing changes to requirements related to eSIM localisation; as a result it's very hard to identify which CSP offerings are currently compliant or will be in the near future

Figure 3: Approaches of communications service providers to IoT connectivity in selected geographies
[Source: Transforma Insights, 2024]



approach to addressing connectivity in each of six countries/regions (Brazil, China, EU, India, Turkey, US) for permanently located devices. In **Figure 3**, we provide a summary of the approach of the 25 CSPs profiled.

The general trend is that CSPs have largely resolved the challenges in the most relevant countries. Compliant connectivity in the EU and US is more or less universal. Brazil, which has historically been the market most commonly quoted as being a challenging market, is now very well addressed by almost all CSPs. China continues to represent a few challenges, but where CSPs wish to address it there are commercial mechanisms for working with Chinese MNOs to support compliant connectivity. ▶

But it's not all plain sailing. The compliance situation in India is in flux with ongoing changes to requirements related to eSIM localisation; as a result it's very hard to identify which CSP offerings are currently compliant or will be in the near future. The current strict rules about localisation within Turkey are also causing significant friction, with many providers unable to support connectivity in that country other than through the use of local SIMs. There are suggestions that the regulatory environment there might need to adapt to be rather less onerous on non-Turkish operators.

It is important to note that in almost all cases, the CSPs concerned would be in a position to negotiate and implement fully compliant solutions for specific clients regardless of current capability. The aim of **Figure 3** is to illustrate the current state of the off-the-shelf offerings of the various players.

eSIM: a universal panacea?

Perhaps the most significant mechanism used for supporting compliance with permanent roaming rules is through the increasing use of some form of SIM localisation, so moving away from relying on roaming using a foreign international mobile subscriber identity (IMSI) to the use of a local IMSI (as part of a multi-IMSI offering) or switching of the eSIM profile to that of a local operator. In the last few years, the technology landscape related to eSIM has changed dramatically and we anticipate an ongoing impact on how global connectivity is delivered. To date there have been three main standards unveiled for remote SIM provisioning (RSP). Each of the three standards established slightly different mechanisms for the user or owner of a device to change the SIM profile while the device is deployed in the field.

Transforma Insights has explored in detail the capabilities and implications of the three standards in great detail, including in the June 2024 Position Paper 'Key considerations for Enterprises looking to adopt SGP.32'. In summary, the SGP.02 (or M2M) standard was introduced in 2014. This was a 'push' model, whereby the donor and recipient network providers would act together to replace the SIM credentials on the device. The challenge with SGP.02 is that it requires cooperation between the subscription management infrastructure of the donor and the recipient networks to perform the hand-over. This was followed in 2016 by the SGP.22 (Consumer) standard where the end user can, via direct intervention using the device user interface (UI), 'pull' a new profile from a chosen provider down to the device. The limitation here was the need for an advanced UI as well as user intervention, neither of which are typically available on any IoT device. The SGP.32 (IoT) third variant, unveiled in 2023, was aimed at resolving some of the limitations of the earlier versions. It effectively amended the SGP.22 technology to allow for remote management. Compliant devices can be expected in 2025. In addition, several connectivity providers have developed variants on SGP.22 that place an agent on the device, removing the requirement for user intervention; these approaches effectively work in the same way as SGP.32, although with some element of proprietary technology.

While the new remote SIM provisioning technology might be well-defined, what is not yet entirely clear is what commercial models will prevail to make use of the new technology. What is completely clear, based on the research that Transforma Insights has done for the aforementioned CSP IoT Peer Benchmarking, is that the view from the CSPs is that they are willing, and in many cases keen, to work with the technology.

The big change, in the context of addressing permanent roaming, is that SGP.32 (and to a lesser extent variants on SGP.22) allow for much easier recredentialling of SIMs to a local profile. Local, compliant, profiles are relatively easily swapped in. However, we should add a caveat or two here. Most pertinently there is still a requirement to establish a commercial relationship with the network onto which the connection will be transferred. Some enterprise customers may well have these in some circumstances, which accounts for the increasing relevance of bring-your-own-connectivity (BYOC) offerings. However, in most cases enterprises will still have requirements for someone to negotiate commercial relationships with appropriate network operators for connectivity and ideally act as a single point of contact. And, furthermore, simply switching between networks is not the only consideration, there is a further requirement to orchestrate data flows and back-end processes to ensure a seamless transition between carriers. Simply put, the provision of compliant cellular-based IoT connectivity will need to be delivered as a managed service, albeit one where much of the friction of localisation and compliance is removed.

While the new remote SIM provisioning technology might be well-defined, what is not yet entirely clear is what commercial models will prevail to make use of the new technology

[3] https://transformainsights.com/research/reports/key-considerations-enterprises-adopt-sgp32

Plenty of action in the IoT data management and protection market

SIMPL, among other solutions, supports the rapid creation of cloud-connected IoT devices from the ground up, while fully securing them to send and receive data in the cloud. Antony Savvas looks at the state of the IoT data security and management market

According to analyst firm **MarketsandMarkets**, the global IoT security market is projected to grow from US$24.2 billion in 2024 to US$56.2 billion by 2029, at a compound annual growth rate (CAGR) of 18.4% during the forecast period.

This market includes identity and access management (IAM), data encryption and tokenisation, device authentication services, secure communication protocols, private key infrastructure (PKI) certificate lifecycle management, security analytics and virtual firewalls.

And according to **Mordor Intelligence**, the IoT data management market is expected to grow at a CAGR of 16.6% between now and 2026. This growth covers solutions including data integration, security, analytics and storage solutions.

Market drivers

When it comes to security spending, the growth is down to organisations facing significant financial losses and reputational damage because of increasing cyber attacks on IoT devices. The particular risk in the IoT sector is that every device and every system usually have their own specific firmware, which is software that controls the device or facility itself.

And since hardly any guidelines or binding specifications have existed in this area for device manufacturers to boost security, hackers and criminals have been attacking the unprotected. ▶

This may change with the European Commission's Cyber Resilience Act (CRA), for instance, which is intended to address data security problems surrounding devices and systems with network connections, from printers and routers to smart household appliances and industrial control systems.

To press manufacturers, distributors and importers into more protective action, with the Cyber Resilience Act, they face significant penalties if security vulnerabilities in devices are discovered and not properly reported and mitigated.

"The pressure on the industry is growing immensely," says Jan Wendenburg, CEO of cyber security firm **ONEKEY**. "The financial fines for affected manufacturers and distributors are severe: up to €15 million or 2.5% of global annual revenues."

Under the Act, suppliers active in the European Union market, must now prepare to complete a Cyber Resilience Readiness Assessment, if they want to avoid facing large fines. That said, the market sales for IoT security show organisations are already increasingly adopting security solutions to help protect against threats like device hijacking, data theft, supply chain intrusions, and widening ransomware attacks.

Key players

Key players in the IoT security market, says MarketsandMarkets, include **Microsoft**, **Fortinet**, **Amazon Web Services**, **IBM**, **Intel**, **Cisco**, **Thales Group**, **Infineon**, **Atos**, **Palo Alto Networks**, **Mobileum**, **Entrust**, **NXP Semiconductors**, **MagicCube**, **Claroty**, **Ordr**, **Armis**, **Nozomi Networks**, **Keyfactor**, **Particle Industries** and **Forescout**, among others.

Microsoft, for instance, offers capabilities for its Defender security protection that promise to bring the same level of vulnerability management, threat detection and response for enterprise IoT devices, previously only available for managed endpoint devices.

The Defender for IoT offering provides extended detection and response (XDR) coverage to IoT devices like digital signage, conference room systems and operational technology (OT) devices, which have all been prone to software vulnerabilities and attacks from cyber criminals.

With Defender for IoT, agentless monitoring secures 'things' connected to IT networks, voice over IP systems, printers and smart TVs, for instance. And it allows firms to gain the essential visibility into devices without additional configuration, through a deployable network sensor that can collect all network data needed for discovery, behavioural analytics and machine learning. Microsoft adds that artificial intelligence (AI) is being used to augment IoT threat intelligence generally.

Government agencies, such as US National Institute of Standards and Technology (NIST), are also investigating IoT security technology on a number of fronts, including protocols, security assurances, use cases, applications and current services, to help drive further data security development to better protect companies and end users.

Zero trust

An emerging concept to help improve data protection is zero trust, which eliminates implicit trust from IT systems, and assumes that every user and every thing on the network is a threat to data security. It treats all data traffic as untrusted, requiring strict identity verification for every user, device and process before granting any permissions.

Such an approach acknowledges that the biggest threats to security can come from lateral movement within a network, so if something untoward is detected on it, then it has to be stopped and quarantined there and then. Companies accepting this principle are now adopting zero trust network access (ZTNA) systems.

Network segmentation

As a first step to adopting ZTNA, organisations should move towards network segmentation. This is the practice of dividing networks into different logical segments, such as IoT connected portions, and having complete control of the traffic going through and between those segments. It is designed to reduce the attack surface, preventing threats from spreading laterally throughout an organisation.

To do this, businesses need a full view of all networks within the organisation. You must have visibility into the network, application, workload and process levels, as well as a view into multi-clouds or on-premise data centres where data assets are distributed across all geographies.

However, while technology methods like ZTNA are expected to become essential, it isn't just technology that is needed to protect apps and data, it is also policy. IT governance, audit and compliance policies as part of a framework must be adopted by organisations with the full backing of their boards.

By combining ZTNA, for instance, and working to a framework, companies can potentially see costs related to any data breach coming down. Spiralling cyber insurance costs are a problem across industries, as a result of wider and more serious cyber security threats. Organisations working to a framework may well see their cyber insurance costs better controlled, as they can demonstrate to insurers that they are more prepared to deal with a breach, and therefore have a better chance of curtailing it, and reducing its damage.

While the IoT data management and protection market may well be growing, now is the time for the whole ecosystem to step up to the plate to help keep out the rogues.

Government agencies, such as US National Institute of Standards and Technology (NIST), are also investigating IoT security technology on a number of fronts

IoT roaming set to drive revenue growth for mobile operators

With IoT connections now composed of various different technologies from non-terrestrial networks to low power wide area networks, cellular connectivity offers a sweetspot for devices that move between different countries or that are designed as part of global deployments. For communications service providers (CSPs), supporting IoT roaming can be an appealing generator of revenue but assuring connectivity is available in multiple countries is complex and involves navigating a complex web of commercial and regulatory conditions

The priorities of many mobile operators and their IoT businesses are becoming increasingly misaligned as the telecoms industry focuses on consolidation of operations to their main markets but IoT demands global connectivity

The growth of IoT is resulting in increased connectivity revenue. IoT market research firm **Berg Insight** has reported that global IoT connectivity revenues increased 16% to reach US$13.82 billion in 2023. As IoT has matured, the firm says there is greater focus on reliability, security and support for international deployments, contributing to new types of market dynamics for cellular IoT connectivity providers. By 2028, the firm projects that there will be six billion IoT devices connected to cellular networks worldwide, generating annual connectivity revenues of US$23.41bn.

The top ten mobile operators reported a combined active base of 2.9 billion cellular IoT connections at the end of 2023, accounting for 88% of the total 3.3 billion connections. **China Mobile** is the world's largest provider of cellular IoT connectivity services with 1.32 billion cellular IoT connections. **China Telecom** and **China Unicom** ranked second and third with 527 million and 494 million connections respectively. **Vodafone** ranked first among the Western operators and fourth overall with 184 million connections, followed by **AT&T** with 128 million in fifth place. **Deutsche Telekom** and **Verizon** had in the range of 50–57 million cellular IoT connections each. **Telefónica**, **KDDI** and **Orange** were the last players in the top ten with about 41 million, 40 million and 37 million connections respectively. The growth in the installed bases of the largest mobile operators varied, reports Berg Insight, with changes ranging from a 1% decrease to a 31% increase year-on-year.

International connectivity constitutes one of the largest and fastest growing segments of the cellular IoT market. Mobile operators with regional and multi-regional operations are naturally well-positioned to offer IoT connectivity services for international deployments at competitive rates, utilising their network footprints and ability to negotiate favourable roaming agreements.

The priorities of many mobile operators and their IoT businesses are becoming increasingly misaligned as the telecoms industry focuses on consolidation of operations to their main markets but IoT demands global connectivity. This has led to a greater separation between mobile operators' IoT businesses and network operations, resulting in more open approaches to global network access in line with the strategies of IoT managed service providers, says Berg Insight.

Established IoT managed service providers however typically have more advanced localisation capabilities through international mobile subscriber identity (IMSI) and embedded SIM (eSIM) profile donor agreements. Berg Insight believes that the separation of IoT connectivity businesses and networks will continue, driven by changing industry dynamics and a shift to new eSIM technologies. This implies a strong case for global consolidation of cellular IoT connectivity platforms.

There is significant growth in the number of connections and **Juniper Research** has uncovered that the number of roaming IoT connections will ▶

Figure 1: Roaming IoT Connections to Grow 300% by 2028 - At what cost to subscribers?
Average cost per MB of data generated by roaming IoT connections in 2028 ($)

grow 300% over the next five years; from 145 million in 2023, to more than 600 million by 2028. **Figure 1** details the average cost per megabit of data generated by roaming IoT connections in 2028.

A study by the firm has found the global number of 5G IoT roaming connections will rise from 15 million in 2023 to 142 million by 2027, representing over 27% of all 5G roaming connections in four years. It predicted that this growth will be driven by the acceleration of 5G standalone (SA) deployments, with intensifying roll outs in home markets providing increased momentum and a strong value proposition for 5G SA-specific roaming agreements.

The research forecast that 21% of global 5G IoT roaming connections in 2027 will be found in West Europe, despite that region only accounting for 5% of the global important for to incentivising IoT users to implement a roaming business model, thus driving growth of IoT roaming connections.

Report author Elisha Sudlow-Poole commented: "To further capitalise on the growth of 5G IoT roaming in West Europe, operators must form roaming agreements that utilise standalone 5G networks to improve network performance for roaming connections, and provide the same level of service when roaming as they do on home networks."

Operators look to add value

In addition to 5G standalone-specific roaming agreements, the report urged operators to implement roaming analytics tools that use AI to maximise roaming revenue, as they enable operators to efficiently assess the significant amount of roaming data generated by 5G roaming connections in real-time. The report anticipates key verticals, such as autonomous vehicles, will necessitate advanced roaming solutions, owing to their data-centric nature. The research emphasised that roaming analytics must be integrated directly into platforms to maximise their value proposition to network operators, and enable swifter reconciliation of clearing for stakeholders.

IoT roaming will remain a key driver of revenue with **Kaleido Intelligence** finding in a recent operator survey that 64% of respondents see IoT roaming use cases as the main driver of roaming revenues over the next three years. Research from the firms has forecast that combined wholesale and retail roaming revenues generated by consumer and IoT mobile connections will reach US$45 billion in 2024. That represents a 47% increase compared to pre-pandemic levels.

The firm says the increase will be driven by rising data roaming activity, primarily fuelled by consumers transitioning to 5G roaming services. This anticipated expansion in both consumer and IoT roaming data usage is expected to soar by 36% annually, reaching close to 5,000 petabytes in 2024.

IoT roaming will remain a key driver of revenue with Kaleido Intelligence finding in a recent operator survey that 64% of respondents see IoT roaming use cases as the main driver of roaming revenues over the next three years

Our pick of the IoT industry's upcoming events

Innovate Americas 2024
24-25 September 2024
Dallas, Texas, USA
https://www.iot-now.com/event/innovate-americas-2024/

Data2030 Summit
24-26 September 2024
Stockholm, Sweden and online
https://www.iot-now.com/event/data2030-summit/

AI & Big Data Expo Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/ai-big-data-expo-europe-2/

Cyber Security & Cloud Expo Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/cyber-security-cloud-expo-europe/

Intelligent Automation Conference Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/intelligent-automation-conference-europe-2024/

Unified Communications Conference Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/unified-communications-conference-europe/

IoT Tech Expo Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/iot-tech-expo-europe-3/

Momentum AI London 2024
2-3 October 2024
London, UK
https://www.iot-now.com/event/momentum-ai-london-2024/

Network X
8-10 October 2024
Paris, France
https://www.iot-now.com/event/network-x-2/

MWC Las Vegas
8-10 October 2024
Las Vegas, Nevada, USA
https://www.iot-now.com/event/mwc-las-vegas/

weknow

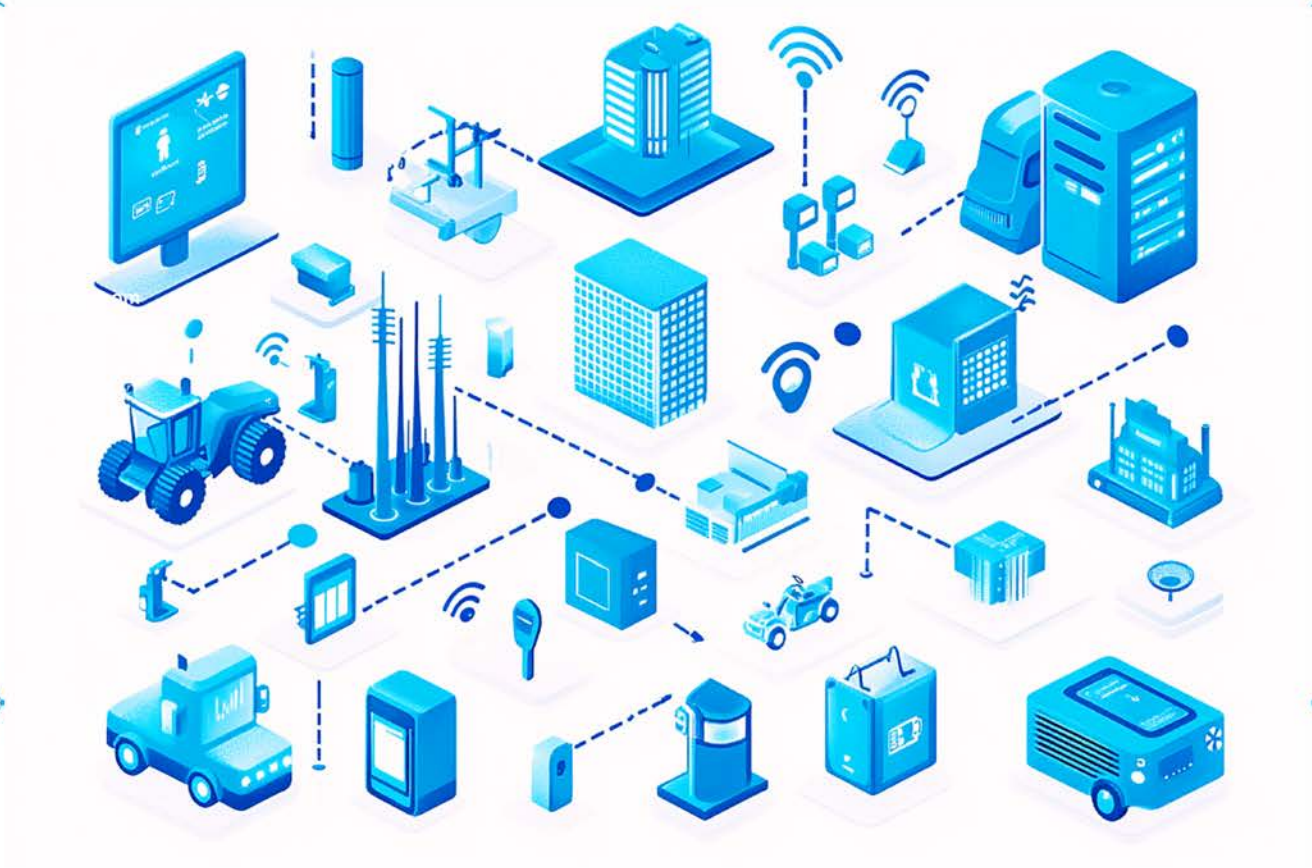
Did you know IoT has been market leading for over 15 years and has a global community of over 240K decision makers?

We are experts in driving your marketing messages to our loyal, engaged audience – Don't take our word for it….

"We tried the content syndication ABM program with 4 campaigns. We got all leads that were guaranteed from our target account list. Beyond that, working with the team has been a great experience, high quality and are always very responsive and eager to help."

Pamela Trevino, EMEAI Marketing Manager, Gurobi Optimization

IoTNOW
HOW TO RUN AN IoT ENABLED BUSINESS



MAKING IOT

SIMPL

- eSIM Localization
- Harmonized SIM Operations
- Buy and Bring your own MNO

www.simpliot.com