TOMORROW'S SMART CONNECTED PRODUCTS REQUIRE SMARTER CONNECTIVITY SERVICES TODAY

ABIresearch®
TRUSTED INTELLIGENCE SINCE 1990

Analyst: Jamie Moss

TABLE OF CONTENTS

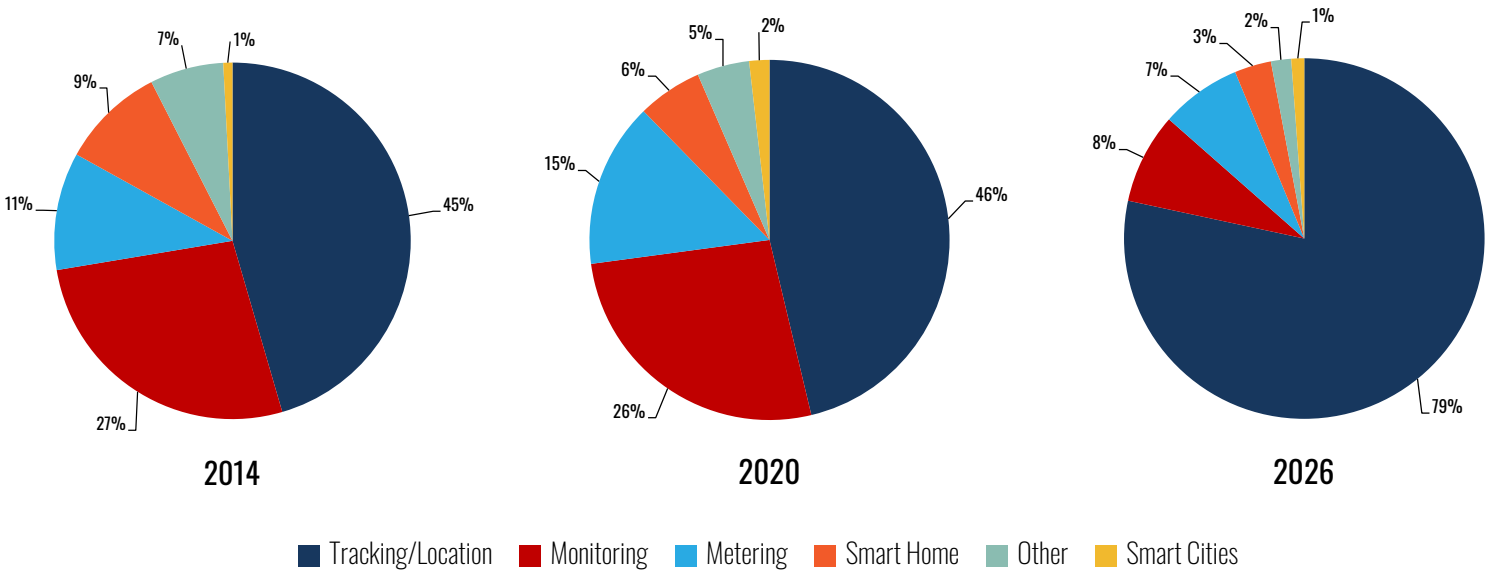
INTRODUCTION

At the end of 2020, 6.6 billion Internet of Things (IoT) devices will be connected and active worldwide; 840 million of them will use cellular networks, which is just under 8% of the total. At the end of 2014, there were 180 million cellular IoT devices active worldwide, and that number increased by over 4.5X in the 6 intervening years. In another 6 years' time, we will witness a further near-7X growth in cellular IoT devices, bringing the global total to 5.7 billion. More smart devices are being deployed, and more types of device are becoming smart.

All IoT applications are variations of either asset tracking (*i.e.,* "where is something?") or condition-based monitoring (*i.e.*, "how is something?"), in combination with use case-specific characteristics that distinguish them as markets in their own right. Applications can be thematically grouped by similarity and significance into: metering, tracking/location, smart home, monitoring, smart cities, and a long-tail selection of "others." Monitoring has consistently accounted for between a third and a quarter of all cellular IoT connections, strongly driven by automotive applications that include: Original Equipment Manufacturer (OEM) telematics, aftermarket telematics, and fleet management. Yet, this stalwart will account for less than 10% by 2026.

Figure 1: Cellular IoT Connections by Category, 2014, 2020, and 2026

(Source: ABI Research)



The fastest-growing category of cellular IoT applications is tracking/location, which is being spurred on by businesses' needs to diversify their supply chains and acquire greater visibility into the location of their assets and how they are performing. The post-COVID-19 economy will rely on automated supply chain management more than ever to ensure business operations are not disrupted by similar events again, protecting their liquidity, ensuring peoples' jobs, and strengthening society. The concept can be extended beyond fleets and goods, to reusable packaging and other returnable business assets that reduce waste and provide a Capital Expenditure (CAPEX) saving.

Consumer markets also play a role, as tracking technology finds its way into general-purpose use, enabling the notion of the shared economy. It encompasses myriad use cases for high-volume publicly rented or borrowed equipment and transforms fleets of physical products into networks of Connected Infrastructure as-a-Service. Supply chain visibility and general-purpose Low-Power Wide-Area (LPWA) asset trackers that are cheap enough to be attached to anything provide the ability and motivation to connect whatever we want; from shared cars and bikes for urban mobility, to power banks, lockers, and shared storage spaces.

It is clear the ability to connect diverse IoT device types, with different needs, at massive scale, and with global coverage is needed now. This whitepaper examines the role of Connectivity Management Platforms (CMPs) and global connectivity coverage solutions in accomplishing this task. Its assessment provides an operator view and, by association, an enterprise view, looking at the evolving needs of both stakeholders and the challenges faced by traditional connectivity management services. It concludes with recommendations for next-generation CMPs to address the IoT needs of the market today and in the future.

CONNECTIVITY SERVICES MARKET EVOLUTION

THE OLD APPROACH

CMPs are needed for managing access to carriers' networks, for testing and activating connected devices, and for rate plan and billing control. They are used by carriers and enterprises and are a fundamental technology enabler for the IoT. The first CMP vendors were infrastructure vendors, or were acquired by infrastructure vendors, and so already had long-standing supplier relationships with carriers. For them to do much more than offer equipment, and especially to offer managed connectivity, would have meant competing with their own customers. This was and remains something that traditional vendors are not comfortable doing.

As enterprises' connectivity needs have expanded globally, CMP vendors were asked to supply connectivity. To do so meant that a vendor had to operate its platform proprietarily and sell its services directly to enterprises, as a Mobile Virtual Network Operator (MVNO) or Mobile Virtual Network Enabler (MVNE). Proprietary vendors developed wholesale relationships with carriers in new geographies only when their enterprise customers requested it, or when it was required to secure a new contract. Global connectivity was not pre-emptively sourced, as the logistics of doing so in advance of securing customers was prohibitively time-consuming and expensive.

The IoT market originally had two types of CMP vendor: 1) those that supplied carriers who relied on roaming agreements to sell IoT services to enterprises, and 2) those that supplied enterprises and were customers of multiple carriers themselves. The former's business was restricted to the largest carriers, with its platforms being used to complement the sale of connectivity. Conversely, the latter would often hand off the provision of connectivity to a preferred carrier partner, using connectivity as a channel to sell more licenses for its value-added platform.

In neither scenario was connectivity monetizable as a value-added feature. This is ironic considering that global roaming with a guaranteed Quality of Service (QoS) at a constant price point, and the utter fragmentation of permanent roaming regulations, both remain fundamental barriers to IoT adoption today, decades after the IoT market was born. A solution to these requirements and restrictions is valuable all by itself, as carriers worldwide continue to struggle to find an answer.

TRADITIONAL SHORTCOMINGS

The pricing structures offered by traditional CMPs are not competitive today. Charging a set fee per device per month takes away a portion of the revenue carriers earn from each IoT connection. That fee can be between 10% and 20% of a carrier's connectivity revenue. This makes traditional CMPs a loss leader, not directly monetizable, not enabling carriers to charge any more for connectivity, and only allowing them to serve IoT connections and win enterprise contracts. Vendors are unwilling to revise their licensing strategy, despite it being especially inappropriate for Cat-M and Narrowband IoT (NB-IoT), which are technologies that did not exist when the platforms were conceived, but which will make up the majority of cellular IoT connections in the near future. While high in volume, Cat-M and NB-IoT are low in data usage and Average Revenue per User (ARPU), and expensive licensing structures will make them uneconomical for carriers to serve.

Carriers' efforts in developing a network to serve IoT connectivity are naturally focused on their own footprint, as that is where they have full control and can make the biggest difference. Internationally, carriers must rely on roaming agreements, just as they do with consumer mobile connections. But roaming agreements are not good enough to guarantee the QoS and Service-Level Agreements (SLAs) demanded by the business-critical nature of IoT devices. This is especially true for Tier Two carriers that do not have the clout to negotiate the best international rates or to effectively assemble global coverage at a price that is low enough and predictable enough. Continuity of service availability at a guaranteed price anywhere in the world is crucial for provisioning the IoT. Traditional CMPs could not help with this, severely limiting many carriers' opportunities.

Carriers do not have a physical network outside of their footprint. Even the biggest international carriers that are influential enough to easily negotiate the most favorable roaming rates do not have PGW/UPFs (Packet Gateway/ User Plane Function) or a core network in those other countries. Very large Tier One carriers may have a couple of PGW/UPFs at most, co-located with strategic partner networks, but no more. And Tier Two carriers certainly do not operate any international infrastructure. All carriers, regardless of size, also have a single core network that all consumer and IoT connections must share. This causes acute issues as consumer mobile broadband connectivity, which is the bread-and-butter income for carriers, cannot risk being disrupted by IoT demands, most often signaling. Meanwhile IoT devices might need functions that a consumer core network cannot be tuned to support.

NEXT-GENERATION REQUIREMENTS

Enterprises would like to maximize the IoT coverage they receive from individual service providers. Carriers will not willingly work together to augment each others' international coverage. Despite the earnest efforts of the IoT World Alliance and the Global M2M Association (GMA), the carriers participating in those industry associations will only authorize the transformation of a roaming connection's International Mobile Subscriber Identity (IMSI) to that of a partner carrier's network as a last resort if maintaining the roaming connection is utterly uneconomical. Conversely, directly competing carriers will each share their network resources with a common third-party MVNO/MVNE. And to an IoT carrier's advantage nationally and internationally, an MVNE will just as easily collaborate with multiple carriers in the same country, giving best-of-breed roaming in a single business relationship, as well as full domestic redundancy.

An MVNE's platform and network is built for integration, unlike a carrier's. Carriers need domestic fallback more often than they admit to in order to provide the guarantees their IoT customers demand. Partial coverage is not good enough, and multiple carriers' networks may be needed to provide full coverage. Although strong local rivals will never work together to enable each other to be more competitive and more effectively serve the same addressable market, they are willing to use a roaming IMSI to do so. There is irony in the fact that MVNOs and MVNEs can provide a more complete service than the carrier partners on which they rely. But it is a practical irony that purposely exists for other carriers to interface with and to allow carriers to do a better job of their own business. It is hard for carriers to build infrastructure outside of their own footprint, and should they do so, they would always prefer an Operational Expenditure (OPEX) over a CAPEX model, and to only incur costs when revenue is guaranteed.

IoT services need different billing plans. Carriers that go to traditional Operations Support System (OSS) and Business Support System (BSS) vendors to change their billing system could face 18 months of work and millions of dollars in costs. Again, this would incur CAPEX before a carrier's prospective IoT opportunity has provided any returns. Like the rest of a carrier's core network, its existing OSS and BSS has been built for consumer services, with carriers being charged by their vendors on a per Subscriber Identity Module (SIM) basis. Carriers do not want to pay for IoT SIMs separately, they want a single payment package that will cover them for a million IoT SIMs at a time. Enterprises buy into the IoT to improve the efficiency and effectiveness of their existing businesses. To successfully deliver IoT services and to profit from them, carriers need to implement efficiencies of their own. Small differences in supply-side costs and improvements in demand-side margins pay dividends at IoT levels of scale.

AN ANSWER FOR MOBILE OPERATORS

Traditional CMPs allow a carrier to serve IoT connectivity in-country, but they do not provide a global network of equipment. Carriers want a global system, not just one that will give them local business. IoT device OEMs want connectivity embedded at the point of manufacture for activation in countries not yet known. Enterprises are increasingly global in operation and want a centralized solution from a single provider that will solve their business problems company-wide regardless of location. Traditional CMP vendors do not offer global connectivity augmented by extensive IMSI libraries to provide carriers with an off-the-shelf international IoT network. The IoT market has grown in size and sophistication, with legacy vendors still offering systems that did not start out looking to solve this global problem.

Enterprises are not telecommunications-minded and are not interested in joining up the services of multiple carriers; nor should they have to. How should a carrier go about serving the global networking needs of an enterprise? Today's carrier needs a vendor that provides two products that are modular, but natively integrated. First, they need a tripartite IoT platform consisting of: a CMP for rate plan setting, data consumption monitoring, and connection activation; a dedicated IoT core for separating out the routing of IoT data and signaling traffic from consumer services; plus a simplified BSS for IoT billing only. Second, they need a global network made up of an international array of PGW/UPFs and an IMSI library of carrier partners that is already deployed and ready for use by enterprises anywhere in the world. QoS, low latency, and privacy regulation compliance are ensured by the dedicated network, while cost control issues are solved using local IMSIs.

CASE STUDY: A NEXT-GENERATION CMP DEPLOYMENT

A regional North American carrier was looking for an IoT CMP. Having been established for many years, this carrier wanted to build a new IoT business to complement its overall business strategy. A comprehensive Request for Proposal (RFP) was published and the carrier's top priorities were:

1. A complete CMP (including SIM management, dedicated core network, device management, and integration layer)
2. Full integration with the carrier's legacy systems (BSS and third-party systems)
3. Quick time-to-market

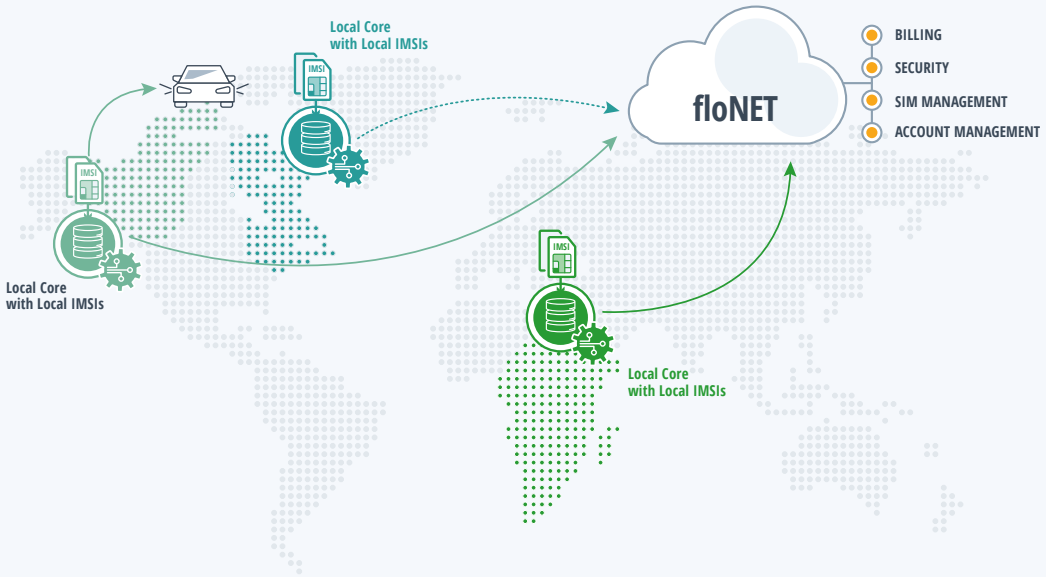
4. Coverage in areas in which the MNO did not have its own Radio Access Network (RAN) deployed
5. A pricing model that will allow the MNO to offer attractive services for low ARPU use cases

The RFP process demonstrated that entering into such a project with multiple vendors would: 1) take a long time to implement; 2) entail a higher cost than originally expected as a result of each vendor needing to integrate with the other; and 3) be nearly impossible for the carrier to offer a single, unified SLA to its customers. Having a back-to-back SLA with multiple vendors would result in escalation skipping from one vendor to another every time there was an incident or fault.

To meet the original business requirements of its RFP, the carrier decided to select floLIVE as its sole vendor. The reasons it gave for doing so were that floLIVE provided the following:

- A complete solution for IoT connectivity management, including CMP, core network, BSS, Remote SIM Provisioning (RSP), and device management, plus the option of decoupling functions and integrating new ones in the future.
- Quick time-to-market. A single vendor that provides the entire system will require significantly less time to deploy, test, and operate; being natively integrated yet modular and not monolithic.
- Comprehensive billing that enables the carrier and its enterprise customers to sell products and services that span beyond connectivity to hardware as well.
- SLA guarantees. A single vendor that can commit to a system-wide service level, while taking end-to-end responsibility for every modular component.
- Extended Coverage. floLIVE provides the carrier with extended coverage in-country and overseas via a global IMSI library and RAN switching capability. Compliance with local regulations is built-in to guarantee consistent performance at global scale. This is regarded as critical by the carrier.
- Cost effectiveness. Purchasing from a single vendor eliminated the need for the more costly and time-consuming deployment and integration of multiple systems.
- Adaptive business model. floLIVE proposed for the carrier different cost structures for low ARPU and high ARPU devices to enable it to be competitive across the gamut of IoT diversity and scale.

Figure 2: floNET—floLIVE's Software-Defined Connectivity (SDC) Platform Architecture
(Source: floLIVE)



The IoT market has changed, with new needs that must be supported by CMP vendors on both the supply side and the demand side. On the supply side, the cellular industry has made new air interfaces available in LPWA networks and 5G. They have made new provisioning techniques possible with Embedded SIM (eSIM) and have changed the way networks themselves can be deployed with private and hybrid architectures. On the demand side, connected devices have changed in terms of the international scope of their rollout, their power consumption and security needs, and in the local privacy restrictions that apply to the data they collect. The wide variety of IoT connectivity needs among device OEMs, enterprises, municipalities, and especially carriers is reflected in the richness of the addressable market for next-generation CMP vendors, who have the opportunity to serve the following:

- Enterprises that want a single means of accessing multiple carriers' networks
- Carriers that want a management platform to serve their domestic customers
- Carriers that want to extend their network for the benefit of existing IoT customers
- Carriers that want to enter the international IoT market as an MVNO
- Carriers that wish to lease network capacity to IoT service providers
- IoT MVNOs that require an MVNE to get them up and running
- Enterprises that want a dual-IMSI backup to existing services for redundancy
- Enterprises that want an IoT platform and core to marry up to existing carrier services
- Enterprises needing modular platform/connectivity competency for existing IoT systems

SUMMARY

Carriers are facing more specific and diverse demands for guarantees from IoT customers, especially when roaming. Enterprises are seeking new technical capabilities from networks and connected devices to expand their services, but in a cost-effective way that meets customer and local requirements. Despite increasingly differentiated uses cases, enterprises want IoT connectivity that is easier to buy. Carriers want to serve enterprises, but in an environment where no operator will have a globally deployed wireless network they are inadequately equipped to manage and need help. The ability to connect different IoT device types with specific network requirements at a massive scale and with global coverage is valuable and vital to the future growth of the IoT market. The capabilities of next-generation CMP vendors are a way to realize this.

Enterprises want a one-stop-shop, more so now than ever. Large multinational corporations that can afford to employ systems integrators to assemble customized systems are few, and while they were some of the earliest IoT adopters, they only represent a portion of the market. Most enterprises do not have the funds or inclination and may not even know what the IoT can do for them. Instead, they value specialist expertise that can deploy and host services for them that "just work," leaving the enterprise itself to focus on what it does best—its existing business. Next-generation CMP services can provide international connectivity for enterprises by allowing carriers to become international MVNOs. The core network of a CMP vendor can collectively manage the routing of IoT traffic across many carrier customers' RANs, allowing them to sell international IoT services with the guarantee of a single price point for data and a consistent QoS.

CMP deployments may be private or hosted for domestic or international service provision, with PGW/UPFs and local IMSIs; and the freedom for customers to add new features without service shutdowns or having to write new code. Flexibility solves complexity by making things simple for carriers regardless of their customers' needs. Next-generation CMP capabilities build on the essential features of traditional systems by adding options that solve problems on the business side, not just the technical side. Roaming agreements are replaced with local connectivity, reducing risk thanks to partners having done this work for the carrier. This means faster time-to-market, fewer carrier resources consumed, carrier access to extra resources, and no large CAPEX investment, just OPEX.

Published November 2020

249 South Street

Oyster Bay, New York 11771 USA

Tel: +1 516-624-2500

www.abiresearch.com

About ABI Research

ABI Research helps organizations–and visionaries within those organizations–successfully conquer digital transformation. Since 1990, we have partnered with hundreds of leading technology brands, cutting-edge companies, forward-thinking government agencies, and innovative trade groups around the globe. Through our leading-edge research and worldwide team of analysts, we deliver actionable insight and strategic guidance on the transformative technologies that are reshaping industries, economies, and workforces today.