Meeting the IoT Connectivity Challenge Needs More Than a Lift and Shift of Mobile Technology – Here's Why

Business Insider predicts that there will be more than 64 billion connected devices by 2025. Organizations that don't have a global connectivity solution in place need to think fast.

Cellular-connected IoT devices may seem like a smart way to get fast connectivity, leveraging the same technology that gives us mobile freedom. But IoT devices are not mobile phones. They have their own considerations and challenges, and need a purpose-built security solution, or they will never break the connectivity barrier for global enterprises.

Go Big or Go Roam

IoT devices are jetsetters by nature. They are often manufactured in one country, before being sent to another - perhaps even multiple locations during a devices lifespan. For IoT to be successful, they need to have connectivity no matter where they reside, or where they're heading.

Nowadays when you book your vacation, you check the mobile coverage at the same time as you note down your check-in time to the hotel. No-one wants to be without connectivity. But how long is your trip? A week or two? In fact, anywhere between 1 and 3 months is usually covered by your mobile provider when you're using roaming services abroad. After that, you'll find that your provider expects the device to return to its home location. Your mom is probably wondering where you are, too.

Combine these restrictions with the expensive nature of international data roaming in the first place, and you're looking at a connectivity landscape that's just not viable when it comes to long-term IoT solutions.

Privacy is One Buzzword You Don't Want to Ignore

Here's a similarity between mobile phones and IoT devices – they both handle the sensitive personal data of their users. But while mobile phones usually stay put in the country of their users, under one service provider, the same can't be said for IoT. This means that roaming SIMs, or multiple operator solutions are much harder to keep compliant. Let's take just one regulatory authority for example – GDPR.

Straight off, unless your service provider has managed to jump through a whole lot of hoops, data originating from an EU device needs to remain the in the EU. Roaming SIMs that do not keep to all the GDPR requirements are in violation. But using multiple service providers is also not a sustainable option for data privacy. Consumers in the EU have certain rights over their data, such as the right to access the data held about them, the right to portability, and the right to erasure. How can this be managed in a transparent way, to allow for business optimization but still remain compliant?

IoT and Mobile are Distant Cousins, not Twins

Mobile operators have a very rigid way of doing things, and can rely on stiff processes because ultimately, most mobile phones are the same. We know, your iPhone X *seems* worlds apart from the neighbor's Samsung, but we promise you – they're basically the same thing. All mobile phones have a display for example – which makes it easier for the user to obtain information about any issues with connectivity or security. IoT devices don't promise the same capability. Service operators need to be able to handle troubleshooting and maintenance on devices that cover anything from M2M in factories, to a connected fridge, a smart city traffic light or an irrigation sensor on a remote farm.

Now consider this on the scale of IoT. While users will (generally speaking) have one mobile phone, or maybe one SIM or device for personal use, and one for work – an enterprise might legitimately have millions of IoT devices. According to McKinsey, 127 new devices are connecting to the Internet every single second. That's more than 30,000 in the time it takes to read this article.

Let's drive this home with one more important difference. IoT is simply more important in a lot of use cases. Think medical devices, healthcare equipment, M2M connectivity in industrial plants and thousands more IoT projects that are currently working around the globe. Enterprises need 24/7 visibility, connectivity and support, or there could be a real and measurable impact on human safety. Mobile phones are important, but we think you could probably crush that candy from your PC if the worst happened.

Securely Handling the Complexity of IoT

Because of all these reasons and more, security needs to be front and center of any IoT initiative. The last thing you want to do is hand over your visibility and control to a third-party service provider, or local carrier systems through roaming agreements. This will directly impinge on your ability to detect and stop a cyber attack against your customers, data and devices. You need to have eyes on your data, and in fact, your end-to-end systems, at all times.

floLIVE is a complete system for handling IoT and M2M connectivity, no matter where your devices are in the world. Manage your entire IoT operation from a single console in the cloud, including CRM, Billing, BSS, and remote SIM provisioning.

To address the limitations of mobile connectivity, floLIVE uses a unique Core Network functionality, with more than 200 locations around the globe – all hosting a local IMSI range. This means no roaming, and therefore no roaming restrictions or compliance headaches. We use smart networking solutions such as autonomous switching and network slicing to cover a limitless amount of IoT use cases, all with seamless connectivity and zero gaps. Not to brag, but we're kind of the best in the business at what we do.

Want to understand more about what we can offer enterprises looking to super-charge their IoT offerings for global connectivity? Connect with us.