TRANSFORMA INSIGHTS

POSITION PAPER

USING PERMANENT ROAMING FOR YOUR INTERNET OF THINGS DEPLOYMENT RISKS HUGE COSTS AND CONTINUITY OF SERVICE PROBLEMS

What is Permanent Roaming?

The concept of roaming for cellular phones has been well established for many years. A device with a SIM card registered in one territory can be used in another territory based on a reciprocal agreement between the two mobile network operators including the exchange of roaming fees. For IoT devices, which may be deployed in, and/or moved between, any country in the world, roaming can be very useful. In fact, for IoT specifically, being in a roaming state can be very useful as a roaming device can usually make use of more than one network, whereas a domestic device is typically limited only to the parent network.

During the 2010s many regulators, for instance in Brazil, China, India and Turkey, introduced, or more rigorously enforced, rules that prohibited permanent roaming. The regulations prohibited devices that are registered in another country from existing permanently in a roaming state within the market. 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, e.g. lawful intercept. Besides this, roaming was never envisaged to include a foreign device permanently being in a state of roaming. There is also a financial element to some of the decision-making as roaming devices don't attract the same taxes as domestic devices in some territories, for example Brazil and Turkey.

There were also commercial equivalents, particularly in the US and Canada, where the operators themselves prohibited their roaming partners from having devices permanently roaming on their networks.

Why is it a problem?

Permanent Roaming is a problem for two reasons. Firstly because compliance with regulations and partner operator rules are essential for continuity of service. Unless the connectivity that underpins your application is compliant with the regulations or commercial rules from host operators, your device will probably be disconnected without any prior warning. This will have very serious implications for continuity of service, customer satisfaction and cost.

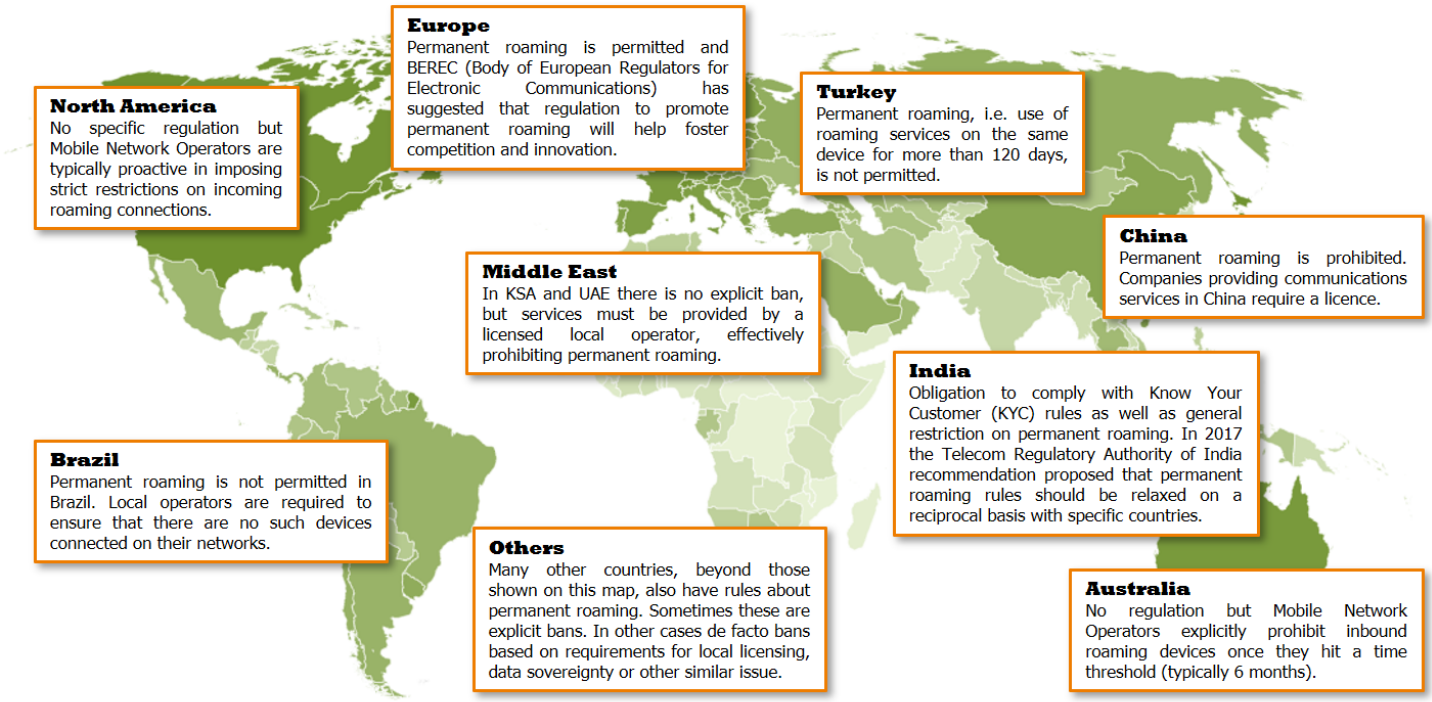
The worst-case scenario is that a company that has contracted in good faith with a network operator partner finds that devices in a particular market have to be switched off. This can happen suddenly and with little warning.

To get back to compliance might require a 'truck-roll', i.e. sending a person to replace the SIM card. Transforma Insights estimates that the average truck-roll to replace a SIM card is USD190 per device ((and in many cases much more). Extended to your entire base this is likely to amount to an eye-watering cost to return to compliance, and a very poor customer service while you are going through the process. There is also likely to be a significant legal bill associated with the issue.

In markets such as in North America where limits on permanent roaming stem from the operators choosing not to support it (rather than a regulatory ban), being caught infringing rules may not result in being removed from the network but may incur a significant increase in fees as a punitive measure against those operators and MVNOs that may have been selling permanent roaming connectivity. We have seen a significant increase in this type of behaviour from North American operators in 2020 and early 2021.

The second reason why it is a problem is because roaming is widely relied on for providing connectivity to IoT devices. In the most extreme cases 50% of cellular IoT connections in a country might be connected using 'roaming' (even though they mostly never move). Relying on roaming is the simplest way for a connectivity provider to offer global coverage. It may not be transparent to the buyer, but mobile network operators and mobile virtual network operators (MVNOs) frequently use roaming to connect devices on other operator networks. This contrasts with the fact that less than 2% of cellular connections actually roam regularly, and therefore justify the use of an out-of-footprint SIM card.

The rest of the IoT market is split between the 48% of IoT devices which are static (e.g. ATMs, elevators and smart meters) and have no prospect of ever moving to another country, and the 50% which can potentially roam (e.g. connected cars, offender tags, and smart watches) but certainly have a 'home' market and would be caught by permanent roaming rules if the connectivity in that home



market were provided using roaming. Many of both types of devices rely on roaming today.

Who does it affect?

It potentially affects everyone who uses cellular connectivity to connect their IoT devices. Just because you're not aware of it does not mean that you are not using roaming today with the potential for non-compliance in future.

Those applications where the device really does roam between countries e.g. shipping containers, don't have much to worry about. But that doesn't apply to the vast majority of devices.

In particular it affects customers that have their devices deployed in multiple territories. If you're limited to a single country the chances are that your partner operator or MVNO will use an appropriate approach. If you have a device estate deployed across multiple countries, however, it's important to check that your supplier is meeting their obligations to support your connections in an appropriate way.

Where will it cause problems?

The rules about permanent roaming vary dramatically between countries (as illustrated on the map above). In some there are explicit rules either prohibiting permanent roaming itself (for example Brazil, China, Turkey) or implicitly doing so through requirements for connectivity to be provided by a locally registered supplier (e.g. Middle East). In others (e.g. Australia, US) the rules are set by the operators themselves, which may choose to allow or prohibit permanent depending on their relationship with the provider of your connectivity.

In other countries there are no rules, and in some it is even being seen as a positive thing. BEREC, the umbrella organisation for telecommunications regulators in Europe is reviewing the rules but has stated that it may encourage the adoption of regulations to encourage permanent roaming: "To foster competition and innovation in the single market, and secure a more level playing field between established operators and new entrants, it is suggested to closely look at the possibility to introduce access obligations for M2M/IoT connectivity services requiring permanent roaming."

What should you do about it?

Your connections must be compliant with the laws of the market and the rules of the host network operators. The simplest way of doing this is to contract directly with a local operator which runs its own network. This is an obvious solution for an application whose deployment is geographically limited such as smart metering or smart cities.

If you need to connect in multiple territories you can opt for a multi-IMSI approach, which sees the SIM card on your device having multiple profiles from multiple different operators. It can then select from these as appropriate in order to ensure your connectivity is compliant.

The most recently available solution is eSIM. This can proactively update the SIM profile on your device to select a local profile, or other appropriate one. This can guarantee connectivity as if it were a local SIM.

Both multi-IMSI and eSIM will allow your to connect to an appropriate network within the territory in which the device is operating. Most importantly, however, you should speak to whoever provides your connectivity to check that your are confident that they provide a connectivity solution that is compliant with the local rules.

Ensuring compliance with regulator and partner rules about permanent roaming has become a critical potential stumbling block for multi-country IoT deployments.