The Law of the Smart City – is it smart enough?

Smart cities are complex. The FTTH Council MENA's work in this area shows us how difficult it can be to understand how to integrate the different needs of users with the complexity of the systems. In all this, the legal aspects tend to be under-estimated and so this paper includes expert input to provide a context for the legal challenges of smart cities.

To understand this aspect better, we turned to Malcolm Dowden and Dave Berry from law firm Charles Russell Speechlys for their legal expertise.

What makes a "Smart City" smart?

Increasingly, the answer lies in the deployment of connected devices and the "internet of things" (IoT). From traffic and transport to energy management systems, key functions are being equipped to provide real-time and actionable data to inform the operation of city-wide systems and services. Machine to machine (M2M) communication drawing data from sensors embedded into objects, vehicles, street furniture and infrastructure vastly increases the potential for gathering and using data about everything from traffic jams to pedestrian flows, energy demand and supply, outages and maintenance needs in utility services. These developments are rapidly adding up to the "fourth industrial revolution".

At the heart of these will always be the fibre network. This may be at metro level, carrying signals around a town or city, or may extend to access. This means the tree like network of connections extending to home and businesses. It is this last part that will really power the connectivity to the different sensors and systems that power a smart city.

Smart city and "industrial internet" developments jostle with domestic and consumer-facing innovations to create an increasingly complex and interdependent web of connections. All, of course, depend on the capacity and resilience of electronic communications networks, and all either create or intensify the challenges facing regulators responsible for ensuring competitive access to efficiently managed networks. They also generate huge and expanding quantities of data at every scale, from individual to complex organisation, and with that data comes new and enhanced vulnerabilities.

The volumes of data demands the power of fibre. A single fibre has transmitted 100 terabits/second. That means you could download the entire contents of the Library of Congress in only a few seconds. However, that same power is at the heart of the legal issue in that you are combining two important factors together – speed of transit and accessibility to data. In an IP based fibre network, new systems (e.g. access control, traffic management, fire control) may not be managed within one over-arching system but they will have been allocated addresses in the network. On that same network are other pieces of information that may seem relevant to different systems and so the natural approach is to increase data integration. That ability to read across from one system to another is powerful but potentially creates issues of data privacy (data used for purposes that have not been granted permission by the data owner) and also location. Increasingly, laws are in place that prevent data being stored outside the relevant country, but this data free for all that can be created makes it more complex to manage permissions within different systems.

Law and regulation, typically, lag some decades behind technological development. The result is that courts and regulators in any jurisdiction, whether common law or code-based, generally have to reach for the legal tools that provide the closest analogies from earlier stages of development to deal with new challenges. While that remains true of legal and regulatory responses to IoT and smart city developments, it is possible to identify areas in which legal issues are likely to arise.

Electronic communications networks: There is an interesting difference between the communication mechanisms in a network is the level control that an operator can exert. A fibre is difficult to hack and impervious to any electromagnetic interference (unlike copper connections that struggle to maintain broadband speeds when subject to high frequency signals from nearby pairs of copper wires). However, wireless signals are even more prone to issues of interference.

A key challenge for regulators is how best to accommodate M2M and IoT within regimes that have tended to assume close control over wireless spectrum often (as in Poland and India during 2015) involving auctions under which operators pay extremely large sums for licensed frequencies to propagate wireless signals from fibre linked base stations.

With M2M and IoT increasingly being directed to unlicensed or “white space” spectrum, such as that vacated by analogue tv services, tensions are becoming apparent between licensed operators and the developers of IoT devices. A key battleground is therefore the treatment of interference. Many IoT devices are designed to operate across a range of frequencies, scanning for currently unused bands. Where IoT devices use frequencies that are close to licensed parts of the spectrum, the holders of expensive licences understandably demand protection.

Within a smart city, this could mean the increasing density of smart and IoT devices results in a degradation of experience and performance! The simple response might be to try to have as many devices on fibre networks as possible. This is more reasonable where the network is entirely new and can be optimised. However, smart city projects in existing towns and cities are often done piece by piece and that thinking can limit the ability to fully integrate IoT devices etc. Wireless is therefore a flexible complement to fibre in these cases.

One key answer to the problem of interference, and also data integrity, is the “kill switch” - a database-driven mechanism that allows regulators to force the disconnection of offending IoT devices. For IoT developers and investors, viability can depend on the approach taken by regulators in each jurisdiction to this key question: when and how should a “kill switch” be used? How far can IoT developers warrant the reliability of their services when faced with anything more than a momentary switch-off. For others, the stakes might be even higher as IoT devices play an ever-more significant role in critical systems ranging from traffic safety to healthcare. Arguably, established electronic communications operators who have become used to being the “disruptors” now themselves face disruption as governments and regulators enter into close and mission-critical relationships with IoT device providers.

In the UK, the sector regulator Ofcom has elected to avoid the issue, instead opting for a “guard band” approach, under which channels considered most likely to risk interference may not be used. While that approach marks a clear attempt to balance interests, it does rule out

the use of potentially key parts of the available spectrum. However, in jurisdictions in the Gulf, operators are running high power WiFi as a communication mechanism even though it is illegal. There is no 'one size fits all' approach.

Product liability: who would be responsible if a self-driving car crashed and caused death or personal injury? As technology develops and regulations are put in place, the prospect of self-driving cars on city streets is becoming far less futuristic or fanciful. Questions of liability are also moving from the realms of thought-experiment and into reality. Equally, who would be responsible if a wearable device designed to administer medication failed due to a regulatory intervention or a data breach? Such questions would not be resolved by reference to a wholly new body of specially-created law. Rather, they would have to be dealt with by applying existing principles and causes of action.

Data: perhaps the most significant areas of concern relate to the ownership, processing, use and security of data generated by IoT devices and smart city infrastructure. Data concerning individual location, activities and even intimate personal information will be gathered and stored. Who is responsible? In Europe, much attention is currently focused on implementation of new data laws extending duties to cloud service providers. These are expected to be copied in other jurisdictions such as the GCC.

Other concerns focus on the question of how resource-starved municipal authorities might seek to fund smart city projects. If, and to the extent, that the solution lies in commercial partnerships or public-private joint ventures then a key question must be how far private sector involvement is driven by the potential value of data. For civil society, the balance between security and facility is a live and pressing question. The cost of infrastructure in a smart city is significant and the civil works in a brownfield FTTH/B deployment could theoretically be amortised by more than just operator revenues. What about the quality of life of residents and the economic competitiveness of the town/city? Municipalities in the same country are being set against one another in attracting investment and the drive to have high speed data networks may reduce principles of data integrity and security.

Contract structures: the coming together of public and private entities and the meshing of young technology with old infrastructure in commercial partnerships and public-private joint ventures can create a challenging array of relationships. Multiple service and system suppliers may be involved in the development, testing and implementation of some solutions whilst interfacing with existing infrastructure can create the risk of potential gaps in legal responsibilities.

As is often the case, lessons can be drawn from analogous situations. In particular, consortium and multi-sourcing models have been developed from an interest in "best of breed" contracting or "select sourcing". This is a strategy of allocating different components of a project to separate best of breed suppliers. Structures vary. The suppliers may be grouped in a consortium, or the procuring entity may contract with each separately, whilst placing supplier management and integration responsibilities onto a lead supplier. This results in an interesting matrix of relationships, up and down between the procuring entity and suppliers, and from side to side with operating level and integration agreements between the suppliers. However, the upside of this complexity is that the approach can lessen the

performance and credit risk for the procuring entity. The cutting edge technology may reside within a start-up venture, whilst the project financing and organisational demands require the involvement of an established “name” to add muscle.

Alternatively, large and established players may well opt for acquisition. Recent examples include the 2014 acquisition by Huawei of “internet of things” pioneers Neul (the name being the Gaelic word for “cloud”).

Overview: any survey of the legal and practical issues affecting smart city projects and IoT implementation rapidly arrives at the realisation that they touch the full range of communications law and regulation, data law, commercial contracts, tort and product liability, administrative and even constitutional law. Further, they require close attention to questions of jurisdiction, governing law and cross-border liability and enforcement.

Globalisation of data services requires an understanding of issues in every relevant jurisdiction.

Richard Jones – Partner, Ventura Team LLP and Chairman – Smart Cities Committee – FTTH Council MENA (richard@venturateam.com)

Malcolm Dowden, Consultant, Charles Russell Speechlys LLP (Malcolm.Dowden@crsblaw.com)

David Berry, Partner, Charles Russell Speechlys LLP (David.Berry@crsblaw.com)