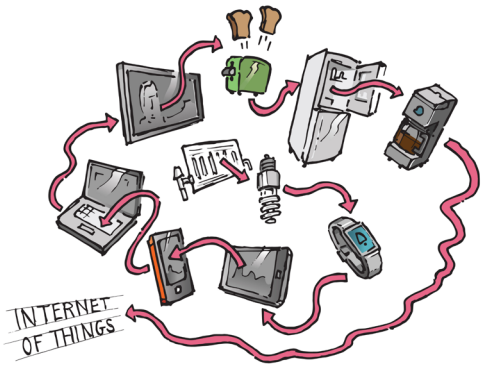
A Telco regulator's take (and our take) on the Internet of Things

February 2015

Speed read

On 27 January 2015, the same day the US Federal Trade Commission produced a report on the Internet of Things (see here for our comments on that), the UK Telco regulator, Ofcom, produced its report, *Promoting investment and innovation in the Internet of Things*.[1] Ofcom identifies some tension points to deal with, but there are more besides that it hasn't identified. We address how we see those other issues.



We explain what the Internet of Things (IoT) is here.

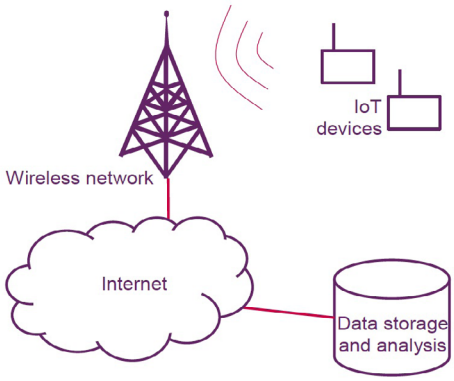
The IoT raises overlapping issues for Telco, data protection/privacy, competition and other regulation.

Take a smart meter for controlling and billing electricity use in the house (that's an IOT device replacing those meters of old with spinning dials: they can do all sorts of things at the behest of an electricity provider):

- **Telco regulation**: A new Canadian decision (reported by us here) indicates this may raise telecommunications regulation issues;
- **Data protection/Privacy regulation**: With collection of detailed personal information, and the ability to merge data from multiple sources, in tandem with big data initiatives, data protection and privacy is to the fore (see our comments here).
- **Competition law**: Smart meters, while enabling pro-competitive innovative services and also more efficient electricity consumption, can also facilitate anti-competitive outcomes such as locking-in customers to a sole supplier (the company supplying and controlling the smart meter can have bottleneck control at the single physical point, just like, say, an airport or a fibre network company). And there's overlaps into competition law issues on big data and use of aggregated information, a bit like the EU allegations against Google. (We are going to write about that soon).
- **Other regulation**: Smart meters are an example of other regulatory issues popping into the IoT space: here, electricity regulation. Smart meters are an important consideration for electricity regulators.

The Detail

What are the issues raised by Ofcom?



Ofcom sees the key components of the IoT as being, as in the diagram (above) from their report:

- IoT devices
- Wireless network including spectrum
- The Internet
- Data storage and analysis.

It's strange of Ofcom to base this only on wireless access, when fixed line access will be just as relevant. Many IoT devices are connected to fixed line.

Having got to that point, Ofcom sees the issues in its Telco regulatory space as being:

- Spectrum
- Addressing
- Network security and resilience.

A diversion to fixed line

In our view, add fixed line access as that is a major Telco regulatory focus. By the way, NZ has a twist on the generally applicable issues around fixed line regulation impacting on the IoT. Many devices – especially B2B and machine to machine – will be connected to the new UFB network at locations other than existing premises. The acronym for those locations is NBAP: Non-Building Access Point. They are outside the LFC and Chorus primary obligations as to connecting fibre to existing premises, thereby raising some issues to resolve.

Additionally, there are telco regulatory issues potentially related to the devices themselves. The recent Canadian decision on net neutrality – see here for our views on that – indicates that telco regulation may go wide enough to cover issues related to such devices. Similarly, as we point out in our views, that may be so in New Zealand, given that "telecommunications services" are broadly framed. This is an open issue and not easily resolved, but Telco regulation may prove relevant depending on the device and the underlying connectivity etc. Application of telco regulation should not automatically be ruled out if the Canadian decision is anything to go by.

But back to Ofcom's list:

Spectrum

Availability of spectrum for IoT is not yet an issue in the UK, but that may happen later. This in NZ is an issue for the Ministry not the Telco regulator.

Addressing

The huge number of devices will raise numbering and identification issues. As Ofcom points out – the same is likely in NZ – telephone numbering is not likely to be an issue, as internet numbering, increasingly on an IPv6 basis, will adequately deal with this.

Network security and resilience

What Ofcom says is a useful summary on this:

> *1.20 As the IoT develops and encompasses an increasing number of services on which citizens and consumers come to rely, it will become increasingly important to ensure that the networks delivering these services are robust and the data delivered over them is secure. This creates particular challenges as the traditional security approaches used in telecommunications may not be applicable in the high volume, low cost devices likely to be used by many IoT services. We acknowledge that industry is aware of these challenges and work is ongoing to deliver secure and robust IoT networks and services.*
>
> *1.21 Providers of networks and services are obliged under existing legislation to take appropriate measures to manage risks to security and resilience. The existing legislation does not explicitly refer to the IoT. However, to the extent that they fall under the definitions in the legislation, we believe IoT networks and services would be covered by these existing obligations.*

Data privacy and consumer literacy

Ofcom go on to identify data privacy and consumer literacy – the key focus of the FTC report, on which we reported here – as an important area, overlapping with the UK data protection regulator's remit. So, they'll work in together on this.

Competition law

Finally, joining dots with competition law, the Internet of Things, in addition to location-based challenges to competition, such as with smart meters, is part of the data explosion, and part of the big data developments. This can lead to competition and consumer welfare problems, as providers can use aggregated information not available to others, thereby creating high barriers to entry in markets. That needs to be balanced against the innovative and pro-market features possible from the Internet of Things.

What is emerging is that control of data and information is an increasingly major competition law issue.

The EU allegations against Google provide a great example of this, extending beyond the IoT. We will write about that later: should the wonderful innovation benefits of what Google is doing be curtailed by competition law? For an introduction in the meantime, see our article, *Why competition law applies to the "innovative" Internet? Lessons from Europe*.

---

1. *Promoting investment and innovation in the Internet of Things* (2015) Ofcom.

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com