

**HIGHLIGHTS:** Net neutrality inching ever closer

## Make way for the Internet of Things

01 January 2011

[Print](#) [Share](#)**It's predicted there will be 50 billion connected devices in 10 years' time, but how can carriers profit from the opportunity and what hurdles do they need to overcome? Tim Phillips explores.**

The Internet of Things (IOT) is one of those technologies that has been the Next Big Thing since long before today's big things were even small. The idea that anything could speak to anything – provided there was a reason to do so – dates back to the science fiction of the 1950s, and in reality perhaps to the Trojan Room coffee pot – the world's first webcam, which internet users in 1993 could view to see if the coffee pot in the Cambridge University Computer Library had any coffee in it.

The coffee pot was hardly sophisticated: an empty pot didn't send a message asking to be refilled, for example. While the pot was quietly advertising its emptiness to thousands, the first major hype of the IOT was grabbed by the ubiquitous – but somehow never quite commercially available – internet fridge. Intel Architecture Labs made it the centrepiece of its vision of the future video in 1998. A child sneaks a late-night snack, and the fridge wakes up his parents to tell them. Later, the same child puts an egg carton in the rubbish, which then automatically orders more eggs.

By 1999, the fridge had been announced by Electrolux. "Why should our future home be a copy of the past? Because most of us spend a lot of time at home in the kitchen, our vision at Electrolux is to provide really useful appliances that can make life easier and simpler," said Michael Treschow, CEO and president. He didn't want to put a price on the fridge, but promised that it would "revolutionise daily life."

### The intelligent doorknob

As the dotcom frenzy took hold, many things were posited as ready to be added to the network, even if there was no obvious problem that needed to be fixed. Nicholas Negroponte, head of the MIT Media Lab, predicted the intelligent doorknob. "Clearly if the doorknob could see, listen, speak, it could do a great deal more than an ordinary doorknob. If it sees me walking up to the door with my groceries, it can open the door. It might even be security-conscious and ask me my mother's maiden name," he told the BBC. The same year Watts Wacker, futurist, predicted that the next technological revolution would be the intelligent toilet.

Eleven years later, our doorknobs remain sullenly uncommunicative, and refuse to open themselves for us. Our toilets still keep their secrets to themselves. Perhaps it was simply too early, or perhaps enough of us find our door furniture is pretty much up to the job that we require from it already.

Yet, with less heady excitement than in the dotcom days, a more functional and practical attitude to machine-to-machine (M2M) communications has become apparent. Mobile operators such as Vodafone, Telenor or Sprint are beginning to report how many of their users aren't people.

There's still exuberance. Ericsson predicts that there will be 50 billion connected devices by 2020 – seven for everyone on the planet – and that seven billion mobile devices will be used by 2015. Many of the people making the most optimistic claims for the IOT have the largest financial incentive to do so – China Unicom, for example recently claimed that M2M will be a source of new subscribers as China's cities reach mobile saturation. "We need to develop new services and new revenue streams," says Dr Zhang Zhijiang, the head of the company's research institute, human-to-machine and machine-to-machine are the new source of subscribers." Yiru Zhong, Frost & Sullivan's ICT analyst, Europe, points out that China is already talking about a national plan for the Internet of Things.

### M2M and mobile data

The mobile industry is excited by the potential size of a market which appears to multiply the population of the planet many times. "Voice is a commodity service that's already a zero-sum game. Mobile data is an interesting story with some room for business model flexibility round smartphones and packages," says Andy Zimmerman, global managing director of mobility services for Accenture. "M2M is the next new growth story for mobile operators. We're starting to see the end game for mobile data revenues in two to three years' time. But M2M has the potential to be far bigger than the current telco market."

As the IOT develops, then it will become so much part of our lives that we cease to think of it as separate to the Things themselves. "The IOT comprises a digital overlay of information over the physical world. Objects and locations become part of the IOT in two ways. Information may become associated with a specific location using GPS coordinates or a street address. Alternatively, embedding sensors and transmitters into objects enables them to be addressed by internet protocols," explains a Hammersmith Group report, *Network Objects and Smart Devices*, from February 2010 on the IOT applications that already exist.

The public discovered in the late 1990s that existing electronic devices contained computer chips that controlled their operation (and could cause them to cease to operate on January 1 2000). If the Millennium Bug had a positive effect, it might be that we are now comfortable that our machines, devices and even clothes collect, contain and occasionally transmit data. The fact that computers help cars to brake, that price tags contain RFID tags and that washing machines contain little computers is old news.

**The Hammersmith Group report quotes Georgetown University professor of communication, culture and technology Michael Nelson, formerly director of internet technology at IBM, who believes that the potential for the IOT is unlimited – as long as you stop thinking about it as a discrete market.**

**HIGHLIGHTS:** Net neutrality inching ever closer

**"Trying to determine the size of the IOT is like trying to calculate the market for plastics, circa 1940. At that time, it was difficult to imagine that plastics could be in everything. If you look at information processing in the same way, you begin to see the vast range of objects into which logic, processors or actuators could be embedded."**

**Public acceptance**

An example of the simple yet powerful application of M2M communication is demonstrated by Tekvet, which has been commonplace in farming since 2003. The system uses a sensor in the cow's ear which can broadcast data over a range between 100m and 200m. A monitoring system can do a simple job, such as taking a core temperature, and so alerting the farmer by text message when one of the animals is sick. It can do the simple job of keeping track of the cows in real time. The sensors, based on RFID tags, cost a few dollars and can be re-used.

More complex systems developed more recently can report on advanced information, even alerting the farmer when a cow is about to give birth, transmitting up to 200Mb of data per year, per cow.

On the other hand, while the potential is seemingly limitless, it is not guaranteed that the IOT will easily be accepted by the public. Animals and machines don't care if their information is being transmitted. Today's consumer applications may be just as hard a sell as the intelligent doorknob proved to be a decade ago.

One of the problems is the selling point of the IOT itself: automation. Smart metering, for example, is often posited as one of the natural applications of the Internet of Things. Meters that not only report exactly the information we are using, but help to optimise not just our bills, but also the provision and transmission of power, are a wonderful concept. But it's a concept that didn't go down well with the residents of Bakersfield, California – one of the testing grounds for smart meters.

In November 2009, Pacific Gas & Electric "paused" installing smart meters when it was sued by Bakersfield resident Pete Flores. He claimed that since PG&E installed a smart meter, he was overcharged and his bill rose for \$200 a month to \$500 to \$600 a month. Other residents joined in a class action suit. It quickly became apparent that these smart meters were not faulty – but they were using variable pricing, which was boosting the cost of air conditioning among other things. Users who were accustomed to paying flat rates were unused to managing their electricity consumption to take advantage of off-peak times, and to reduce it during peak times. M2M communication was working perfectly from the point of view of the machines, but sub-optimally for the bill payer.

"The customer has to trust that the utility is installing devices that will make their service better, that the utility will keep their data private and safe, and that the smart meters will help them save money," comments Katie Fehrenbacher, editor of green technology blog Earth2Tech. "Smart grid technology and smart meters don't represent new or risky or bleeding-edge technology. They use the same type of information technology – wireless networks, silicon, software – that controls our cell phones, computers and internet... It's just being used in a new industry: electricity."

**Security and privacy**

The opposition to smart meters has not slowed in 2010 in California. What should have been a bonus for both provider and consumer has been, in this area at least, a PR problem. While consumers may have to become accustomed to M2M technologies that in their lives, in the short term they might take time to become accustomed to an Internet of Things that changes the way they are expected to behave. This worry is only increased if consumers feel that their security and privacy is compromised: an internet fridge that does our shopping is benign. An internet fridge that tells our doctor if we're eating the wrong products sounds intrusive. An internet fridge that informs the government if there are more people living in the house than are paying tax is, at best, creepy.

A potentially more damaging innovation is the potential of the IOT to damage from computer worms. In June 2010, Stuxnet "the most refined piece of malware ever discovered" in the words of Alan Bentley, a senior vice president at security firm Lumension, was discovered in the wild. Apparently targeted at Iran's Bushehr Nuclear Power Plant, the worm – designed to reprogram industrial systems – seems to have had no effect; but Kaspersky Labs concluded that such a coordinated attack was possible only with "nation state support". Whether or not it was an early example of cyber warfare, the worm raises the question of whether M2M communication will be vulnerable to attack in the same way as the human-to-human internet has been. In this way, the IOT either forms a new threat to our security, or offers a valuable opportunity for carriers to develop and sell value-added security services; it depends on where you stand.

**How to grasp the opportunity?**

Nevertheless, the sheer number of opportunities the IOT offers means it is impossible to ignore as a category – even if the way in which carriers grasp the opportunity (and the revenues they make from it) are still undecided. Gartner predicts that, by the end of 2012, sensors in the IOT will generate 20% of non-video internet traffic. Yet the nature of this traffic, and the low value of the information in it, will restrict the revenue opportunity for a carrier that is only interested in moving the packets of data.

Sprint, Vodafone, Orange, Telefonica and Telenor are building dedicated M2M businesses. Other operators are partnering with specialists: Jasper Wireless, for example, in which KPN bought a stake in 2010. Jasper Wireless helps M2M value-chain partners to bundle connectivity with their applications and devices. It's partners include AT&T, Rogers, KPN, Telcel and Vimpelcom already, and it has promised announcements regarding new partners in Asia-Pacific.

**HIGHLIGHTS:** Net neutrality inching ever closer

The question for operators who decide they want to move the data from our new intelligent toilets (for example): is the size of the opportunity in terms of network nodes equivalent to the revenue from it? This may guide how much, in the short term, of their resource they dedicate to helping create the IOT. "There is no immediate surge in traffic demand associated with M2M. Data transfer rates are still low and traffic is batched rather than real-time... not all connections will yield the same level of ARPU depending on whether they have always-on connectivity or send data in batch mode, and the value of the data they are transmitting. Smart metering, for example, will just involve data rather than video and can be sent off-peak across the network," warns Zhong.

**Profit in the application**

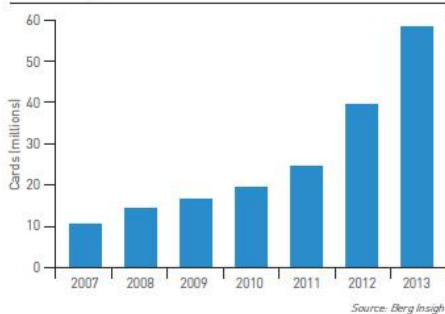
Fabio Mungo, CTO for Accenture Mobility Operated Services, Accenture's managed platform for mobile data application development and hosting, points out that connectivity with Things on the internet offers big numbers of nodes and low value per connection for carriers: unless they create a some kind of partnership with the high-value aspects of the business, the benefits are marginal.

"If you analyse the way value is distributed across the M2M value chain, the connectivity component accounts for 10% to 15% of the total value." He says that, to extract more value for themselves, telcos will need to move into vertical market segments, such as healthcare, fleet management and telematics. The problem: this is not the business that most carriers are in. "The integration of vertical applications with end users and third-party infrastructure needs deep industry knowledge and systems integration expertise. Most carriers are in no position to offer this," Mungo says.

The profit is in the application and not the connection. It is also likely to be in areas where no one will complain. Just as cows do not complain that a sensor in the ear is invading their privacy, so industries where surveillance is mandatory or efficient, rather than intrusive, will embrace M2M communication sooner. We may balk at having our personal data examined by an intelligent toilet, but we wouldn't mind the sewage company monitoring combined data to optimise its efficiency.

In the short term, vertical markets driven by regulation, and needing high-quality, high-volume data will drive revenues. "Once we see M2M widely used in surveillance applications such as the oil pipeline security or in healthcare, the need to support constant video streams will become significant and customers will be prepared to pay for high-quality, real-time visual information. This will give the wholesale community the opportunity to supply higher margin, class of service connectivity," says Zhong. "I can't see that consumer devices such as e-readers or digital photo frames will have higher revenue-generating ability than market sectors that are driven by regulatory requirements."

**Figure 1 Active wireless M2M SIM-cards in Europe**



**Figure 2 Possible barriers to M2M market growth (average score out of four)**

