# The Internet of Things (IoT): Creating Really Big Data

Martin De Saulles, Principal Lecturer in Digital Marketing, University of Brighton

Information Matters

The term, Internet of Things (IoT), has been around since 1999 when brand manager Kevin Ashton at Proctor and Gamble applied RFID technology to streamline his company's massive supply chain. Since then it has grown to encompass the deployment of Internet-connected sensors and trackers across a range of industries and business processes. Essentially, it is an evolution of closed, proprietary telemetry systems that go back to the 1970s. On an industrial scale it includes connected sensors to track the wear and tear of a jet engine and water quality sensors to measure the safety of drinking water. At the city level it includes initiatives such as the AirSensa project which is installing 10,000 air quality sensors around London, each of them providing accurate, street-level data in real time for third parties to analyse. Individually many of us are already contributing data to the IoT via smartphone apps or devices such as Fitbit that track our movements, exercise regimes and health status. Google's Nest thermostat is a good example of how everyday household devices are being connected to allow the remote monitoring and control of domestic lighting and temperatures. Google's announcement in late May of its Brillo operating system for smart devices reveals its plans to extend data gathering beyond search and Android smartphones.

As these systems are rolled out and integrated into our daily lives the biggest challenge is going to be making sense of the data thrown off the myriad of devices in our pockets, houses, workplaces and cities. Cisco estimate that the number of Internet-connected devices overtook the number of people on the planet in 2008 and that by 2020 there will be 50 billion 'things' transmitting information. By 2018, they claim, the data created by IoT devices will be 277 times higher than the amount of data generated by smartphones and PCs. With a Boeing 787 generating 40 terabytes (TB) of data per hour of flight and the mining operations of a company like Rio Tinto generating up to 2.4 TB per minute it is easy to see how the IoT presents huge opportunities for companies able to create value from it all.

As with any new technology there is the danger of getting carried away with its potential for radical change. Last August, Gartner put the IoT at the top of the Peak of Inflated Expectations on its Hype Cycle of emerging technologies with Big Data heading into the Trough of Disillusionment (if you're not familiar with Gartner's Hype Cycle, this Guardian article will be useful.) However, this is not a good reason to write the IoT off as a fad that will soon pass. IoT systems are being developed and deployed and, despite some inevitable hiccups on the way, in a decade I believe the embedded connectivity of many everyday items will be the reality. The ability for cost savings at the household and industrial levels are too compelling for it to go away.

However, there are a number of issues to be resolved before that happens. At a personal level, privacy is a major concern. Much of the personal data being uploaded into the "cloud" from IoT devices is of a sensitive nature. For example:

- Health status data (smartphone fitness trackers, smart watch health monitors)
- Eating habits data (smart fridges - Yes, the mythical smart fridge does exist)
- Quality of our driving data (smart boxes connected to cars are becoming common to reduce insurance premiums, particularly for younger drivers)
- Household status data (Google's Nest thermostat is able to tell whether anyone is in the house by tracking movement)

It is not difficult to see how this data, particularly when combined with other information about our lifestyles, could be used in ways not necessarily in our best interests. Therefore, the security of how data flows from IoT devices to third parties and how secure they keep the data once it arrives is also crucial. This is of particular concern with the firmware powering many devices that, unless closely monitored, is prone to third party attacks if not updated regularly. Managing updates on a PC is probably difficult enough for most non-technical consumers so extending this across to smart fridges, door locks and thermostats, for example, is another matter altogether.

Another major challenge for IoT developers is how to make money from their initiatives. At the bottom of the value chain are the manufacturers of devices such as thermostats and fridges but the real value is not expected to be at this level. It is further up the value chain where the data is captured and analysed that the real profits are probably to be found. Google did not spend $3.2 billion buying smart thermostat manufacturer, Nest, because it saw huge profits in the hardware. Google's underlying business model is in having access to and control of massive quantities of data. Nest, for example, makes money by doing deals with energy companies to give them a degree of control over the thermostats. This allows the energy providers to micro-manage the temperatures of their customers' houses resulting in cost savings for the customers and more efficient utilisation of the grid and power generation.

Questions over who controls the data generated by the IoT and what is then done with it will be central to who makes the biggest profits. It is no coincidence that IBM, Cisco, Microsoft, Google and others are investing billions of pounds in platforms and infrastructure to manage these data flows and make sense of it in a way that allows new services to be created, many of which have not yet been thought of. Imagine going back to 1994 as the first web browsers were being launched and the Internet was just starting to take a hold as a communications and information-sharing platform. Who would have imagined that twenty years later it would be so embedded in our private and work lives? I suspect we are at about the same stage with the IoT.