Everything connected

50 billion – SIM cards in use by 2025
80% – new mobile connections occurring in Africa and Asia

Everything connected

Over 1 trillion sensors are connected to multiple networks: everything that can benefit from a connection has one. We deliver 10,000x more data 100x more effectively but are concerned about the security of the information that flows.

By 2025, there will be over 50bn SIM cards in use, we will have digitized all of our archives, and new information will be being created at such a rate that some see us doubling the volume of our total data set every month. Much of this data will come from machines, talking to each other as well as to us - by the end of the decade, pretty much everything that can have a connection, will have one. IBM sees that the Internet of Things (IoT) is bringing over 1 trillion sensors into the world, all connected to each other and multiple networks. This digitization of the world has the potential to provide us with previously unknown levels of information and insight; equally it could open the doors to unpredicted risk.

Today there are over 3.3bn of us connected to the Internet globally and we are currently adding another billion every three years. In 2014 China already had over 640m Internet users, the US had 280m and India 240m. With over 40% of the population connected, the general view is that within the decade pretty much all of us will have the capacity to be online, wherever we may be. Smartphones and other devices will be a primary driver of change; with 2.6bn smartphones already in use, Ericsson sees that there will be 6bn by 2020. Indeed, Ericsson and other big mobile technology network firms such as Nokia and Huawei are investing heavily in broadening the reach and performance of their networks. They are planning for a doubling of data traffic per user every 18 months to a point where each of us can access 1GB of information every day. Facebook and Google are looking at vast fleets of balloons and drones to bridge the digital divide and provide connectivity to those currently without coverage. With Africa and Asia accounting for over 80% of new connections,

total mobile subscriptions by 2020 are now expected to number over 9 billion.

As of 2015, some countries were already very connected. In terms of the number of devices per capita, Germany, Sweden, the Netherlands, Switzerland and the US had already passed the 20 threshold, Denmark was over 30 and South Korea was touching 40. Fast accelerating up the tables was China with 6 devices per capita but India had less than 1. Given the investments taking place looking ahead, a global average of just over 10 devices per capita by 2020 certainly seems credible.

While 10 per capita is a handy number, increasingly these devices will not be owned or used by us. The vast majority, maybe 30 to 40 billion of them, will be embedded in machines. Cars, fridges, traffic lights, containers, robots and even surgical equipment will all be connected, creating, accessing and using data. Most of the digital information will be stored in the cloud with users expecting instant access anywhere anytime and thus testing the physical limits of networks. Networks will have to become programmable to create capacity on demand, heralding the advent of self-optimizing and cognitive networks able to handle complex end-to-end optimization tasks autonomously and in real time.

All of us will have the capacity to be online, wherever we may be.

Certainties
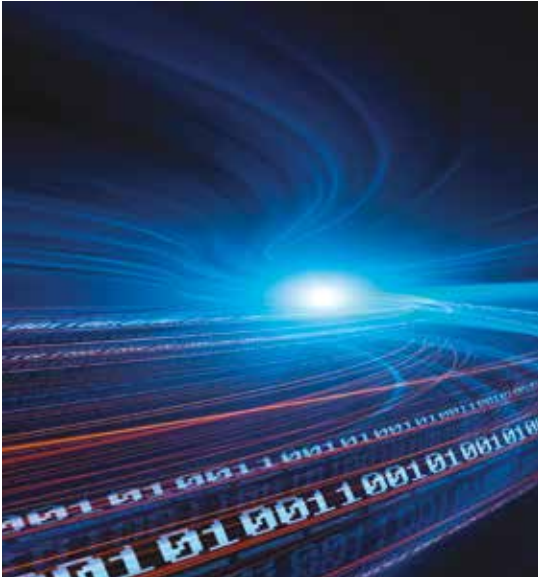
The concept of interconnected networks of physical objects, machines, buildings, infrastructure and devices is a focus for many such as Cisco and IBM as part of the vision for a Smarter Planet. Although progress has not been as rapid as some thought, the direction of travel is still clear. Everything that can benefit from an Internet connection will, by 2025, probably have one, be that fridges, toasters, driverless trucks or pallets. The large amounts of data generated from diverse locations will be aggregated very quickly, thereby increasing the need to better index, store and process such data.

One critical factor is how all these newly connected things connect to one another. Too many standalone IoT gadgets not taking into account the wider context, and digital ecosystems they exist within, is a concern. Without interoperability of technologies, products and ecosystems, these products will remain separate islands.

There is however arguably even more data to be generated from passive tags and sensors. Miniature sensors that can be put anywhere – on food, in clothing, within packaging, inside components, in animals and pretty much anywhere we like – and which can be activated by a multitude of different energy waves from a reading device, can provide location, temperature, orientation, movement or biological information to be remotely read, hundreds at a time. IBM sees that within the decade we could have 1 trillion passive tags and sensors connected to multiple networks. Nokia's view is that by 2025 we will have 10,000x more data being provided to us and between machines 100x more effectively. The knock on challenge will be the need to make sense of the information that flows.

Whether or not we choose to access and hopefully make use of these vast amounts of data and information will, though, be our choice and not a consequence of location, income or education.

A global average of just over 10 devices per capita by 2020 certainly seems credible.

6

While the benefits are lauded in terms of the opportunities to improve efficiency, reduce waste and find out new things that were previously unknown, there are concerns about the risks of everything being connected. Some argue that we are jumping into connecting everything without thinking through all of the consequences, especially as some of the data protection on some devices is very low. People point out that a connected kettle, for example, could become the back door to your Wi-Fi network that bypasses all passwords and so an open door to your personal data.

We could have 1 trillion passive tags and sensors connected to multiple networks.

When everything is connected, not just kettles and laptops but power stations, traffic systems and medical devices, then the concerns shifts from privacy to security. Cyber attacks are already happening on a regular basis targeting not just databases but also machines and systems. Security services and consultancies are already busy monitoring, repelling and recovering systems from being hacked and hijacked. As we move forward with everything being linked online, the potential for harmful hacks rises significantly. This is especially true of the billions of passive tags and sensors that don't have the power to support high levels of encryption. So while everything being connected has lots of upside, there is clearly also some risk.

A connected kettle, for example, could become the back door to your Wi-Fi network.

Related insights

Autonomous transport

The shift to fully autonomous transport is an evolution via truck platoons on highways and small urban delivery pods. Connected cars create the network and test the technologies for the eventual revolutionary driverless experience.

Built-in flexibility

The path to a connected, accessible and distributed infrastructure is fraught with complex, costly and risky issues: Upgrading and repurposing systems to make them more open plus on-going maintenance need significant resources.

Ethical machines

Automation spreads beyond trading and managing systemic risk. As we approach technology singularity, autonomous robots and smarter algorithms make ethical judgments that impact life or death.

The increasing value of data

As organisations try to retain as much information about their customers as possible, data becomes a currency with a value and a price. It therefore requires a marketplace where anything that is information is represented.