

Smart networks: coming soon to a home near you

Blogpost by Rudolf Van der Berg of the OECD's [Science, Technology and Industry](#) Directorate, OECD. January 21, 2013. Available at <http://oecdinsights.org/2013/01/21/smart-networks-coming-soon-to-a-home-near-you/>

In 2017 a household with two teenagers will have 25 Internet connected devices. In 2022 this will rise to 50, compared with only 10 today. In households in the OECD alone there will be 14 billion connected devices, up from 1.7 billion today and this doesn't take into account everything outside the household and outside the OECD. All this leads to the smart world discussed in a new OECD publication, [Building Blocks of Smart Networks](#).

The OECD defines "smart" as: "An application or service able to learn from previous situations and to communicate the results of these situations to other devices and users. These devices and users can then change their behavior to best fit the situation. This means that information about situations needs to be generated transmitted, processed, correlated, interpreted, adapted, displayed in a meaningful manner and acted upon."

Smart networks are the result of three trends coming together (and all being studied by the OECD). Machine to Machine communication means devices connected to the Internet (also known as the [Internet of Things](#)). This generates "[Big Data](#)" because all those devices will communicate and that data will be processed, stored and analyzed. And to enable the analysis, [Cloud Computing](#) will be necessary, because when entire business sectors go from no connectivity to full connectivity within a few years, they will need scalable computing that can accommodate double digit growth. Underlying these trends is the pervasive access to Internet connectivity.

2012	2017	2022
2 smartphones	4 smart phones	4 smart phones
2 laptops/computers	2 laptops	2 laptops
1 tablet	2 tablets	2 tablets
1 DSL/Cable/Fibre/Wifi Modem	1 connected television	3 connected televisions
1 printer/scanner	2 connected settop boxes	3 connected set top boxes
1 game console	1 network attached storage	2 e-Readers
	2 eReaders	1 printer/scanner
	1 printer/scanner	1 smart metre
	1 game console	3 connected stereo systems
	1 smart metre	1 digital camera
	2 connected stereo systems	1 energy consumption display
	1 energy consumption display	2 connected cars
	1 Internet connected car	7 smart light bulbs
	1 pair of connected sport shoes	3 connected sport devices
	1 pay as you drive device	5 Internet connected power sockets
	1 network attached storage	1 weight scale
		1 eHealth device
		2 Pay as you drive devices
		1 intelligent thermostat
		1 network attached storage
		4 home automation sensors
Devices that are likely but not in general use		
E readers	weight scale	alarm system
sportsgear	smart light bulb	in house cameras
network attached storage	ehealth monitor	connected locks
connected navigation device	digital camera	
set top box		
smart metre		

New devices connected to the Internet may be invented, but you'll see that the table only has everyday objects you may already have, but if you replace it in the coming years, the new version will be connected. (The ever-popular, but never seen in a shop near you, Internet connected fridge doesn't make the list.) Connected lightbulbs may well be the Trojan horse of the smart home. Some companies estimate that connected lightbulbs will be the same price as normal lightbulbs five years from now. These lights will be able to dim and change color and fit in a regular socket. They can also serve as hubs, extending the communication network in the home to all devices.

Connecting machines and devices to telecommunications networks is nothing new. Even at the dawn of the Internet there were Internet connected coffee pots and coke-machines. It is the scale of the trend that forces us to pay more attention. Dutch company TomTom now has millions of GPS-navigation devices on the road, which have generated 5000 trillion data points. When systems need to be smart, the number of datapoints goes up. A dumb electricity meter can do with one reading per year. A smart meter needs a reading every 15 minutes for the electricity company, while for home automation a sampling frequency of once every 1 to 5 seconds is proposed, which could be a 31 million times increase over traditional datasets.

There are, however, challenges that need to be faced when introducing smart systems.

Human challenges. The way people interact with networks and systems may limit their use. For eHealth, smart systems can allow people to lead a normal life. However, a portable heart monitor that sends alarms every time it loses the signal or measures a false positive can have the opposite effect. Privacy and security concerns of users have prompted the Dutch parliament for example to change the rules for smart meters.

Lifecycle challenges. A car should last for 15 years. A mobile phone works for 2-4 years. Mobile phone networks move to new protocols every 15 years. Energy networks have a 15-50 year lifecycle. When a technology is introduced in a vehicle today, the first cars with that technology may reach the end of their lifecycle in 2028, the last ones in 2038. What's more, if the lifecycles of two distinct sectors meet, the effect can be even more pronounced. Think of the charge point for electric vehicles. It may have to function for 30 years or more, meaning that all vehicles in the coming 30 years will have to be compatible and that the infrastructure needs to be active for another 15 years. Today's choices for smart systems will be long-term decisions.

Business Challenges. A previous [OECD report](#) concluded that users of M2M systems that make use of mobile technology are locked-in with their mobile networks. They can't change networks and when the devices go across borders they are locked in with their operators. And according to Norwegian research, as many 30% of devices can be offline for 10 minutes per day. To solve these problems the OECD advises governments to change their numbering policies, so that large scale M2M users can become independent of mobile operators and use multiple networks at the same time.

Another business challenge is that it is unclear who has the lead in the smart networks sector. For smart metering, energy companies, meter manufacturers, ICT-companies and telecom companies have all said they will lead.

Regulatory challenges. Governments will be confronted with difficult policy issues, notably concerning privacy and security. A recent review of industrial control systems of five major manufacturers showed that all five could be hacked and sometimes very easily. If companies that supply multi-million dollar systems cannot get essential elements of security correct, than how can you trust systems bought in a DIY store? Would it be possible for a hacker to turn up the airconditioning or heating in a million homes to bring down the electricity grid?

Other questions governments face are regarding access to data. Who owns the data, is it the company or the consumer? If a government collects a dataset, can it share that data for other uses?

Useful links

[OECD work on the Internet economy](#)

[OECD work on information and communications policy](#)

[OECD work on smart sensors](#)

[OECD work on smart grids](#)