



# ITU EXPLAINERS

## INTERNET OF THINGS

### What is the internet of things?

The term ‘internet of things’ (or, more commonly, ‘IoT’) was first coined in 1999 by a British technologist, Kevin Ashton, in an attempt to describe how devices and objects connected to the internet (‘smart things’) communicated and shared information with each other independently of humans. It can be seen as the progression from the traditional internet infrastructure, based predominantly on individuals accessing the internet through computers, to an internet based on a much larger range of devices collecting and sharing data.

In popular discourse, IoT is often seen as a means of optimising consumer products and services – by enabling, for example, central heating systems which switch on when a homeowner’s car is a few minutes away, or fridges which automatically order more milk from the supermarket when it’s running out. But, by connecting the devices and applications of larger numbers of people, it is also the subject of wider societal and structural visions. Cities could use IoT to react and adapt on the basis of actual rather than estimated behaviour – for example, by installing traffic lights which reduce congestion by adapting dynamically to the number of vehicles on the road, or by using real time crime statistics to allocate police officers more effectively.

#### **The ITU’s Definition of IoT**

The ITU itself defines IoT in one of its Recommendations ([ITU-T Y.4050](#), formerly ITU-T Y.2069) as “a global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies.” One of the notes to the definition adds that “from a broad perspective, the IoT can be perceived as a vision with technological and societal implications”. That this definition suggests that IoT can be considered as both a “global infrastructure” and a “vision” demonstrates the rather general, non-technical nature of the term.

IoT isn’t just a speculative technology, however. Devices developed today routinely carry sensors which allow them to collect data and to share it with other objects and applications, which means that many people – whether or not they know it – are already experiencing IoT in everyday life. This has led some to argue that talking of a separate, distinct ‘internet of things’ is already becoming out of date. Just as the ‘smartphone’ is now referred to as simply a phone, so the ‘internet of things’ will likely one day be simply understood as ‘the internet’. For the time being, however, the term is still widely used.

## Why is IoT being discussed at the ITU?

Given that IoT is the natural extension of the current application and use of the internet, a better question might be ‘Why is the internet being discussed at the ITU?’. There isn’t a straightforward answer to this.

The ITU has had a clear mandate, [since its inception in the 19th century](#), to set technical standards on certain forms of electronic communication, initially telegraphy, but over the years also radio, telephony, television and satellites, to ensure global interoperability. Given that much of the internet relies upon the same physical infrastructure as other electronic communications, some of the ITU’s work has an indirect link to internet-related policies. Some have argued that the ITU should also play a role in setting standards beyond the physical infrastructure and on other internet-related issues such as Internet Protocols, counterfeit devices, spam and security. In 2005 – at the World Summit on the Information Society (WSIS) – the ITU was, for the first time, given an, explicit, albeit limited, mandate to work on internet-related issues. However, the mandate was not to set standards comparable to those that it develops on other forms of electronic communications, but to facilitate certain activities which fell within the Geneva Plan of Action. Specifically, the ITU was tasked to facilitate activities under action lines C2, which aimed to support the development of information and communication infrastructure, and C6, which aimed to build confidence and security in the use of information and communication technologies.

### **The Geneva Plan of Action**

The [Geneva Plan of Action](#) is a document agreed upon at the end of the first of two events that made up World Summit on the Information Society (WSIS), in Geneva in 2003 (a further event took place in Tunis in 2005).

The WSIS itself was a UN-convened multistakeholder summit on the ‘information society’ with a particular focus on harnessing ICTs for development, and the Geneva Plan of Action comprised of a series of ‘action lines’ which aimed to advance progress on internationally-agreed development goals, such as the Millennium Development Goals, by promoting the use of ICT-based products, networks, services and applications, and helping countries bridge the global digital divide.

There are eleven action lines in total, each setting out the responsibilities of various actors. The [Tunis Agenda](#), adopted at the end of the second WSIS event, included a list of different international organisations chosen to facilitate/moderate for the action lines and their activities.

Given this remit, it's unsurprising that IoT – an ICT-related issue that is becoming increasingly prominent in global policy discussions – has attracted the attention of the ITU.

In the 2010s, a number of ITU study groups started to include IoT-related issues in their work, and in 2011, a 'Joint Coordination Activity on Internet of Things' was established to coordinate the work in these different study groups, which have since developed a number of Recommendations relating to IoT.

At the ITU's Plenipotentiary Conference in 2014, its members adopted [Resolution 197](#), which gave the organisation, for the first time, an explicit mandate to look at certain aspects of IoT. In that Resolution, ITU member states resolved "to promote investment in and development of IoT" in order to achieve certain objectives, namely, the potential benefit that IoT could bring in the fields of energy, transportation, health, agriculture, disaster management, public safety and home networks. The Resolution also gave more specific instructions to various actors within the ITU:

- The Secretary-General was "to facilitate the exchange of experiences and information with all relevant organizations and entities involved in IoT and IoT services, with the aim of creating opportunities for cooperative efforts to support the deployment of IoT" and to submit a report on the resolutions implementation at the annual ITU Council sessions as well as the Plenipotentiary Conference in 2018;
- The ITU-T Sector was mandated to continue studying IoT in its study groups, specifically on "enabling IoT as a basic enabler capable of facilitating the emergence of diverse services in the globally connected world, in collaboration with relevant sectors" and to "continue cooperation with relevant organizations (...) for exchanging best practices and disseminating information to increase interoperability of IoT services, through joint workshops, training sessions, joint coordination activity groups and any other appropriate means"; and
- The ITU-D Sector was mandated "to encourage and assist those countries which need support in adopting IoT and IoT services, by providing relevant information, capacity building and best practices to enable the adoption of IoT, through seminars, workshops, etc".

Importantly, however, the ITU has not been given a mandate to set technical standards relating to IoT, which are instead being developed by other

standards developing organisations such as the Institute of Electrical and Electronics Engineers and the Internet Engineering Task Force. This has not stopped some ITU member states from pushing for the ITU to be more heavily involved in the technical aspects of IoT. As we examine in our [Explainer on digital object architecture \(DOA\)](#), some ITU members are trying to have DOA – a particular way of managing digital information in a network environment – adopted as the global standard of managing IoT devices, and proposing that the ITU be the sole entity authorised to administer the global register of all such devices.

### **Why should human rights defenders care?**

While much data is entirely innocuous, some, either alone or when combined with other data, can reveal an enormous amount of more personal information about an individual. Data can reveal the places a person goes, the people they communicate with, their health status, what they read and look at on the internet, and even highly sensitive information such as religion, sexual orientation, gender identity or political opinions. The right to privacy includes the right to exercise control over if and how we share such personal information and so, if this information were leaked or hacked, it would be a breach of that right to privacy. In some societies, it could even put them at risk of other human rights violations, such as discrimination, persecution or violence from state or non-state actors.

Those risks, of course, already exist today, with the widespread use of internet-enabled devices like smartphones and laptops. But the move to IoT – and the radical increase in data-sharing that this will entail – magnifies these risks. As more and more devices become connected, and IoT becomes standard, it is therefore crucial that there are sufficient safeguards for individuals' right to privacy to ensure that personal data is not generated, stored or shared without their informed consent, and that such data as is stored and shared is done so securely. However, given that the ITU does not have a mandate to set standards or regulate on either privacy or data protection, it is incumbent upon the states themselves to ensure sufficient and appropriate privacy and data protection laws and policies apply when it comes to IoT, consistent with international human rights law and standards.

As well as these general concerns, were DOA ever adopted by the ITU as the global standard of managing IoT devices (and under the ITU's administration) there could be further adverse impacts upon the rights to privacy and freedom

of expression, which we examine further in our [DOA Explainer](#).

### **Where is the discussion taking place?**

Discussions around IoT are taking place in a number of forums within the ITU, primarily in ITU-T Study Group 20 ('Internet of Things, smart cities and communities'), where a range of IoT-related questions are being studied, but also:

- In ITU-T Study Group 11 ('Protocols and Test Specifications'), where question Q12/11 looks at the testing of IoT, its applications and identification systems;
- In ITU-T Study Group 17 ('Security'), where question Q6/17 looks at the security aspects of telecommunication services, networks and IoT.

It is likely that further discussions around IoT will also take place at upcoming ITU forums and events, including the Plenipotentiary Conference in October and November 2018.