**What is the Internet of Things?**

The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. Thanks to the arrival of super-cheap computer chips and the ubiquity of wireless networks, it's possible to turn anything, from something as small as [a pill](https://www.zdnet.com/article/how-sensors-enabled-eli-lilly-to-improve-the-patient-experience/)to something as big as [an aeroplane](https://www.zdnet.com/article/ten-examples-of-iot-and-big-data-working-well-together/), into a part of the IoT. Connecting up all these different objects and adding sensors to them adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without involving a human being. The Internet of Things is making the fabric of the world around us more smarter and more responsive, merging the digital and physical universes.

**What is an example of an Internet of Things device?**

Pretty much any physical object can be transformed into an IoT device if it can be connected to the internet to be controlled or communicate information.

A lightbulb that can be switched on using a smartphone app is an IoT device, as is a motion sensor or a [smart thermostat](https://www.zdnet.com/article/johnson-controls-cortana-powered-thermostat-is-up-for-preorder-in-march/) in your office or a connected streetlight. An IoT device could be as fluffy as [a child's toy](https://www.zdnet.com/article/fbi-to-parents-beware-your-kids-smart-toy-could-be-a-security-risk/) or as serious as [a driverless truck](https://www.zdnet.com/article/driverless-trucks-are-coming-but-for-now-adoption-is-in-the-slow-lane/). Some larger objects may themselves be filled with many smaller IoT components, such as a jet engine that's now filled with thousands of sensors collecting and transmitting data back to make sure it is operating efficiently. At an even bigger scale, [smart cities projects are filling entire regions with sensors](https://www.zdnet.com/article/las-vegas-announces-smart-city-plans-with-cisco/) to help us understand and control the environment.

The term IoT is mainly used for devices that wouldn't usually be generally expected to have an internet connection, and that can communicate with the network independently of human action. For this reason, a PC isn't generally considered an IoT device and neither is a smartphone -- even though the latter is crammed with sensors. A [smartwatch](https://www.zdnet.com/article/could-your-apple-watch-save-your-life-how-smartwatch-sensors-are-helping-tackle-a-dangerous-heart/) or a [fitness band](https://www.zdnet.com/product/fitbit-ionic/) or other wearable device might be counted as an IoT device, however.

**What is the history of the Internet of Things?**

The idea of adding sensors and intelligence to basic objects was discussed throughout the 1980s and 1990s (and there are arguably some [much earlier ancestors](https://innovateuk.blog.gov.uk/2017/07/03/the-history-of-internet-of-things-iot/)), but apart from some early projects -- including an internet-connected vending machine -- progress was slow simply because the technology wasn't ready. Chips were too big and bulky and there was no way for objects to communicate effectively.

Processors that were cheap and power-frugal enough to be all but disposable were needed before it finally became cost-effective to connect up billions of devices. The [adoption of RFID tags](https://www.zdnet.com/article/rfid-heralds-the-internet-of-things/) -- low-power chips that can communicate wirelessly -- solved some of this issue, along with the increasing availability of broadband internet and cellular and wireless networking. The [adoption of IPv6](https://www.zdnet.com/article/finally-ipv6s-killer-app-the-internet-of-things/)-- which, among other things, should provide enough IP addresses for every device the world (or indeed this galaxy) is ever likely to need -- was also a necessary step for the IoT to scale.

[Kevin Ashton](https://en.wikipedia.org/wiki/Kevin_Ashton) coined the phrase 'Internet of Things' in 1999, although it took at least another decade for the technology to catch up with the vision.

Adding RFID tags to [expensive pieces of equipment](https://www.zdnet.com/article/uk-hospitals-embrace-rfid/) to help track their location was one of the first IoT applications. But since then, the cost of adding sensors and an internet connection to objects has continued to fall, and experts predict that this basic functionality could one day cost as little as 10 cents, making it possible to connect nearly everything to the internet.

**How big is the Internet of Things?**

Big and getting bigger -- there are already more connected things than people in the world.

Tech analyst company IDC predicts that in total there will be 41.6 billion connected IoT devices by 2025, or "things." It also suggests industrial and automotive equipment represent the largest opportunity of connected "things,", but it also sees strong adoption of smart home and wearable devices in the near term.

Another tech analyst, Gartner, predicts that the enterprise and automotive sectors will account for 5.8 billion devices this year, up almost a quarter on 2019. Utilities will be the highest user of IoT, thanks to the continuing rollout of smart meters. Security devices, in the form of intruder detection and web cameras will be the second biggest use of IoT devices. Building automation – like connected lighting – will be the fastest growing sector, followed by automotive (connected cars) and healthcare (monitoring of chronic conditions).

**What are the benefits of the Internet of Things for consumers?**

The IoT promises to make our environment -- our homes and offices and vehicles -- smarter, more measurable, and... chattier. Smart speakers like [Amazon's Echo](https://www.zdnet.com/article/amazon-echo-the-four-hard-problems-amazon-had-to-solve-to-make-it-work/) and [Google Home](https://www.zdnet.com/product/google-home/) make it easier to play music, set timers, or get information. [Home security systems](https://www.zdnet.com/product/amazon-cloud-cam/) make it easier to monitor what's going on inside and outside, or to see and talk to visitors. Meanwhile, smart thermostats can help us heat our homes before we arrive back, and smart lightbulbs can make it look like we're home even when we're out.

Looking beyond the home, sensors can help us to understand how noisy or polluted our environment might be. Self-driving cars and smart cities could change how we build and manage our public spaces.

However, many of these innovations could have major implications for [our personal privacy](https://www.zdnet.com/article/business-must-tone-down-its-lust-for-big-data/).

**The Internet of Things and smart homes**

For consumers, the smart home is probably where they are likely to come into contact with internet-enabled things, and it's one area where the big tech companies (in particular Amazon, Google, and Apple) are competing hard.

The most obvious of these are [smart speakers](https://www.zdnet.com/article/smart-speakers-are-now-the-fastest-growing-consumer-technology/) like Amazon's Echo, but there are also smart plugs, lightbulbs, cameras, thermostats, and the much-mocked [smart fridge](https://www.zdnet.com/article/samsung-connected-home-fridge-becomes-weapon-in-mitm-attacks/). But as well as showing off your enthusiasm for shiny new gadgets, there's a more serious side to smart home applications. They may be able to [help keep older people independent](https://www.zdnet.com/article/trusense-aging-in-place-system-passively-monitors-independent-seniors/) and in their own homes longer by making it easier for family and carers to communicate with them and monitor how they are getting on. A better understanding of how our homes operate, and the ability to tweak those settings, could help save energy -- [by cutting heating costs](https://www.zdnet.com/article/origin-energy-launches-smart-home-kit-for-optimising-energy-usage/), for example.

**What about Internet of Things security?**

Security is one the biggest issues with the IoT. These sensors are collecting in many cases extremely sensitive data -- [what you say and do in your own home](https://www.zdnet.com/article/how-to-keep-your-smart-tv-from-spying-on-you/), for example. Keeping that secure is vital to consumer trust, but so far the IoT's security track record has been extremely poor. Too many IoT devices give little thought to the basics of security, like encrypting data in transit and at rest.

Flaws in software -- even old and well-used code -- are discovered on a regular basis, but many IoT devices lack the capability to be patched, which means they are permanently at risk. Hackers are now actively targeting IoT devices such as routers and webcams because their inherent lack of security makes them easy to compromise and [roll up into giant botnets](https://www.zdnet.com/article/satori-malware-code-given-away-for-christmas/).

Flaws have left smart home devices like refrigerators, ovens, and dishwashers open to hackers. Researchers found [100,000 webcams that could be hacked with ease](https://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/), while some internet-connected smartwatches for children have been found to contain security vulnerabilities that allow hackers to track the [wearer's location, eavesdrop on conversations](https://www.zdnet.com/article/security-flaws-in-childrens-smartwatches-make-them-vulnerable-to-hackers/), or even communicate with the user.

Governments are growing worried about the risks here. The UK government has published its own [guidelines around the security of consumer IoT devices](https://www.zdnet.com/article/iot-security-your-smart-devices-must-have-these-three-features-to-be-secure/). It expects devices to have unique passwords, that companies will provide a public point of contact so anyone can report a vulnerability (and that these will be acted on), and that manufacturers will explicitly state how long devices will get security updates. It's a modest list, but a start.

When the cost of making smart objects becomes negligible, these problems will only become more widespread and intractable.

All of this applies in business as well, but the stakes are even higher. Connecting industrial machinery to IoT networks increases the potential risk of hackers discovering and attacking these devices. Industrial espionage or a destructive attack on critical infrastructure are both potential risks. That means businesses will need to make sure that these networks are isolated and protected, with data encryption with security of sensors, gateways and other components a necessity. The current state of IoT technology makes that harder to ensure, however, as does a lack of consistent IoT security planning across organisations. That's very worrying considering the documented willingness of hackers to tamper with industrial systems that have been [connected to the internet but left unprotected](https://www.zdnet.com/article/ransomware-snooping-and-attempted-shutdowns-the-state-of-this-honeypot-shows-what-hackers-do-to-systems-left-unprotected-online/).

The IoT bridges the gap between the digital world and the physical world, which means that hacking into devices can have dangerous real-world consequences. Hacking into the sensors controlling the temperature in a power station could trick the operators into making a catastrophic decision; taking control of a driverless car could also end in disaster.

**What about privacy and the Internet of Things?**

With all those sensors collecting data on everything you do, the IoT is a potentially vast privacy and security headache. Take the smart home: it can tell when you wake up (when the smart coffee machine is activated) and how well you brush your teeth (thanks to your smart toothbrush), what radio station you listen to (thanks to your smart speaker), what type of food you eat (thanks to your smart oven or fridge), what your children think (thanks to their smart toys), and who visits you and passes by your house (thanks to your smart doorbell). While companies will make money from selling you the smart object in the first place, their IoT business model probably involves selling at least some of that data, too.

What happens to that data is a vitally important privacy matter. Not all smart home companies build their business model around harvesting and selling your data, but some do.

And it's worth remembering that IoT data can be combined with other bits of data to create a surprisingly detailed picture of you. It's surprisingly easy to find out a lot about a person from a few different sensor readings. In one project, a researcher found that by analysing data charting just the home's energy consumption, carbon monoxide and carbon dioxide levels, temperature, and humidity throughout the day they could work out what someone was having for dinner.

**IoT evolution: Where does the Internet of Things go next?**

As the price of sensors and communications continue to drop, it becomes cost-effective to add more devices to the IoT – even if in some cases there's little obvious benefit to consumers. Deployments are at an early stage; most companies that are engaging with the IoT are at the trial stage right now, largely because the necessary technology – sensor technology, 5G and machine-learning powered analytics – are still themselves at a reasonably early stage of development. There are many competing platforms and standards and many different vendors, from device makers to software companies to network operators, want a slice of the pie. It's still not clear which of those will win out. But without standards, and with security an ongoing issue, we are likely to see some more big IoT security mishaps in the next few years.

As the number of connected devices continues to rise, our living and working environments will become filled with smart products – assuming we are willing to accept the security and privacy trade-offs. Some will welcome the new era of smart things. Others will pine for the days when a chair was simply a chair.