4. The IOT

What is the Internet of Things?

People have been getting excited about this idea since it was originally suggested in 1999 by technology entrepreneur Kevin Ashton, then working in brand marketing at Proctor & Gamble. He'd been researching electronic sensors and RFID tags (wireless printed circuits that allow objects to identify themselves automatically to computer systems; they're used in library self-checkouts) and, in a moment of insight, wondered what would happen if all kinds of everyday objects and machines could communicate through a standard computer network. Ashton realized his Internet of Things was a yellow-brick road to better efficiency and less waste for all kinds of businesses.

Although people sometimes talk about the Internet of Things as though it's merely an extension of smart home technology, it's actually a much bigger and more general idea. Imagine our system for monitoring the elderly transplanted to a hospital and scaled up into a kind of e-care, in which noncritical patients are routinely monitored not by nurse's observations but by remotely gathered electronic sensors, communicating their measurements over a network. Or, to take another example, what about automatically monitoring your home while you're on holiday using sensors and webcams? If it works in a house, it works anywhere: for checking and automatically restocking shelves in a supermarket, for remotely monitoring the crumbling concrete on a highway bridge, or in a hundred other places.

How does it work?

Five basic things are needed to make the Internet of Things work.

1. The thing

First, there's the "thing" itself—which could be anything from a person or animal to a robot or computer; champions of the technology have even speculated that one day the Internet of Things could extend to things as small as bits of dust. Generally speaking, the "thing" is something we want to track, measure, or monitor. It could be your own body, a pet, an elderly relative, a home, an office block, or pretty much anything else you can imagine.

2. The identifier

If we want to be able to connect things, monitor them, or measure them, we need to be able to identify them and tell them apart. It's easy enough with people: we all have names, faces, and other unique identifiers. It's also relatively easy with products we buy from stores. Since the 1970s, most of them carried have unique numbers called Universal Product Codes (UPC), printed on their packs using black-and-white zebra patterns—barcodes, in other words. The trouble with barcodes is that someone has to scan them and they can "store" only a very small amount of information (just a few digits). A better technology, RFID, allows objects to identify themselves to a network automatically using radio waves, with little or no human intervention. It can also transmit much more information.

3. The sensors

If an object simply identifies itself to a network, that doesn't necessarily tell us very much, other than where it is at a certain time. If the object has built-in sensors, we can collect much more useful information. So automatic sensors that can routinely transmit automatic measurements are another key part of the Internet of Things. Any type of sensor could be wired up this way, from electronic thermometers and thermocouples to strain gauges and reed switches.

4. The network

It makes sense for things to exist and communicate on a network the same way that computers exist and talk to one another over the Internet—using a standard agreed communication method called the Internet Protocol (IP). IP is based on the idea that everything has a unique address (an IP address) and exchanges data in little bits called packets. If things communicate using IP, or use something like WiFi to talk to an Internet-connected router, it opens up the possibility of controlling them from a Web browser anywhere in the world. That's why we're now seeing home security and monitoring systems that allow you to do things like turning your central heating on and off with smartphone apps.

5: The data analyzer

Once we're collecting masses of data, from hundreds, thousands, millions, or even billions of things, analyzing it could find patterns that help us work, move, and live much more smartly—at least in theory. Data mining the information we gather from people or car movements and optimizing our transportation systems could help us reduce travel times or congestion, for example, with major benefits for people's quality of life and the environment. Cloud computing systems (the idea of using powerful computer services supplied over the Internet) are likely to play a very big part in the Internet of Things, not least because the amount of data collected from so many things, so regularly, is likely to be enormous.

Good points and bad points

It's easy enough to see benefits from a world in which we connect, monitor, and analyze things much more intelligently. The natural world manages perfectly well without top-down organization, coordination, and control, but our human-dominated planet, packed with over 7 billion people, plagued with problems like poverty, disease, and looming environmental challenges such as climate change, probably can't afford the luxury of hapless, chaotic self-organization for much longer. The benefits of tracking and organizing things seem overwhelming to some people; even so, critics point out equally clear risks of monitoring people and things so much more closely. Do we all want our cars to be tracked at all times? Do we want grocery stores to know even more about what we're heating than they do already? Do we want our homes packed with sensors, keeping tabs on us at all times? There are all kinds of privacy, security, and ethical issues to consider before we get anywhere near the technological difficulties of building something so all-encompassing as an Internet of Things.

Photo: Privacy problems ahead? Will an Internet of Things designed for tracking and tracing things turn into a perfect tool for spying on people?