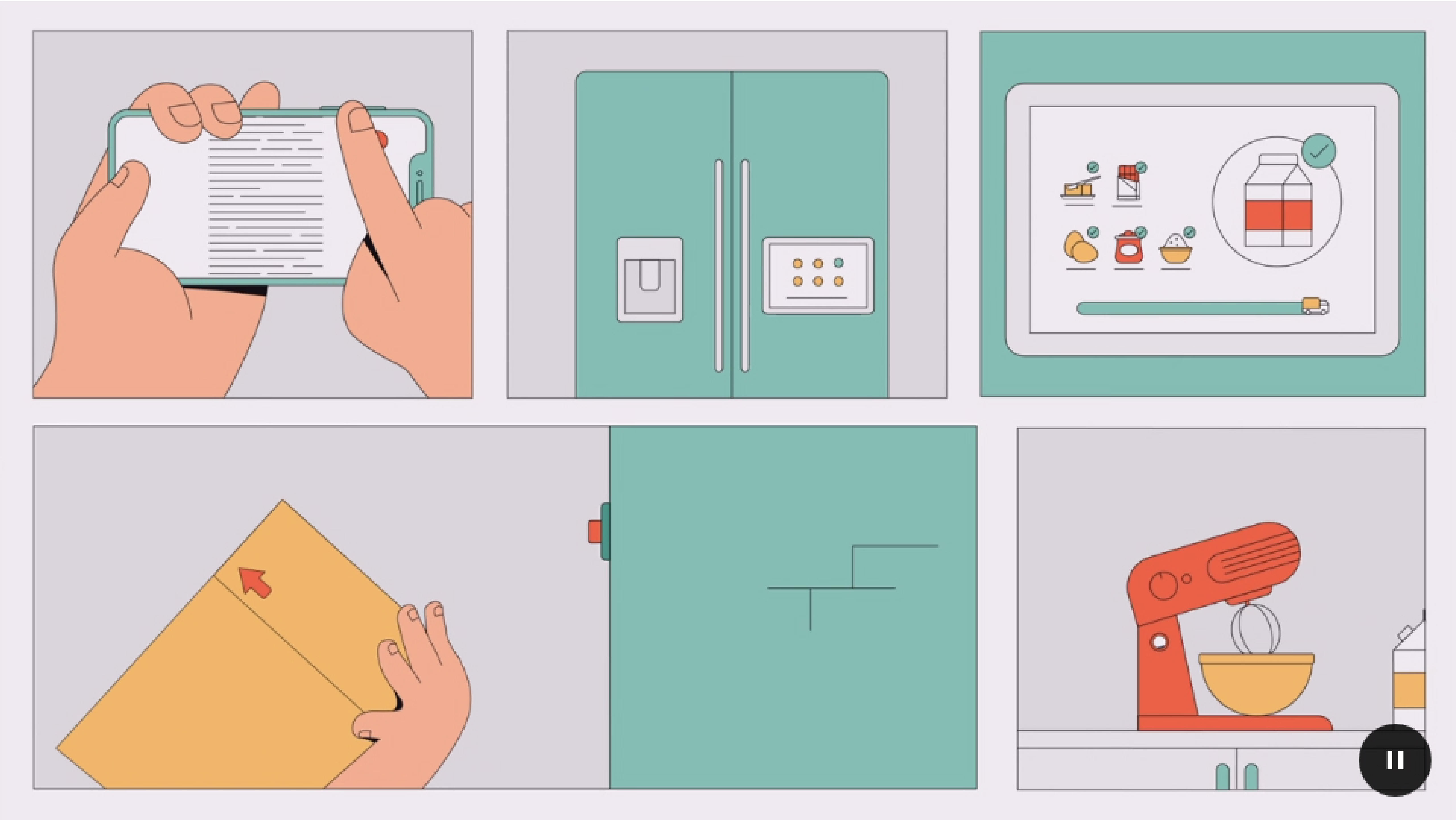


ILLUSTRATION: RADIO

ARIELLE PARDES GEAR 09.11.2020 07:00 AM

The WIRED Guide to the Internet of Things

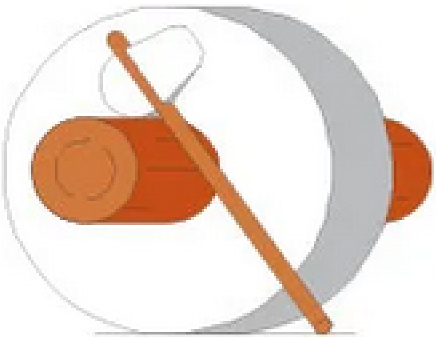
What you need to know about the promise (and peril) of networked lightbulbs, ovens, cameras, speakers, and, well ... everything.

https://www.wired.com/story/wired-guide-internet-of-things/

HOW MANY ENGINEERS does it take to change a lightbulb? Depends on whether or not that lightbulb is connected to Wi-Fi.

Lightbulbs, along with refrigerators, coffee makers, microwave ovens, baby monitors, security cameras, speakers, televisions, and thermostats have, in the past few decades, transformed from ordinary objects into conduits for the future. Embedded with sensors that see, hear, and touch the world around them, they can turn physical information into digital data. Collectively, these devices—and there are billions of them around the world—make up the “internet of things.”

Just about anything with network connectivity belongs to the internet of things. In the "smart home," these internet-enabled gadgets liberate us from our chores, give us back some of our time, and add a dash of novelty to ordinary experiences. (*"Alexa, turn on the disco lights."*) But the internet of things is about more than just using your voice to preheat the oven or using your phone to turn off the lights. The real promise of the internet of things is making our physical surroundings accessible to our digital computers, putting sensors on everything in the world and translating it into a digital format. Internet-connected objects could be the key to unlocking predictions about everything from consumer behavior to climate events, but those same objects could invite hackers into personal spaces and leak intimate data. Depending on who you ask, the growing internet of things either represents the promise of technology—the thing that will reinvent modern life as we know it—or that which will be our technological undoing.



The History of the Internet of Things

The dream of a sensory computer as the centerpiece of the smart home has occupied the popular imagination for at least half a century. Sci-fi writers like Ray Bradbury and television shows like *The Jetsons* brought the automated house to life, and inventors began creating prototypes for exhibitions around the world, showing off ideas for self-cleaning homes and furniture that could move itself around for its occupants.

The net benefit of these gizmos was, for the most part, liberation from housework. At the 1959 American National Exhibition in Moscow, Whirlpool created an exhibit called the "Miracle Kitchen"—a futuristic display meant to show what life in capitalist America was like. It included a dishwasher that cleared the table and a proto-Roomba to sweep the floors. "In America, we like to make life easier for women," Richard Nixon said to Nikita Khrushchev, the President of the Soviet Union, in an apparent jab on the showfloor.

Most of the early smart home inventions used automatic controls, making it possible to turn something or off without lifting a finger. But they didn't connect to anything else, and their functionality was limited. That would begin to change in 1983 when ARPANET, the earliest version of the internet, adopted the internet protocol suite (also known as TCP/IP). The protocol set standards for how digital data should be transmitted, routed, and received. Essentially, it laid the groundwork for the modern internet.

IoT Through the Years

1990
John Romkey creates the first IoT device: a toaster that he controls with his computer

1999
Kevin Ashton coins the term "internet of things" to describe the eyes and ears of a computer

2000
LG introduces its first connected refrigerator with a $20,000 pricetag

2008
The world's first IoT conference is held in Zurich, Switzerland

2010
Tony Fadell founds Nest, maker of the smart thermostat

2013
Oxford Dictionary adds the term "internet of things"

2014
Amazon introduces the Echo speaker, along with the Alexa voice assistant—a new way to control the smart home

2016
The Mirai botnet infects over 600,000 IoT devices with malware

2020
The number of internet-connected devices, by some estimates, exceeds 20 billion

The first internet-connected "thing" to make use of this new protocol was a toaster. John Romkey, a software engineer and early internet evangelist, had built one for the 1990 showfloor of Interop, a trade show for computers. Romkey dropped a few slices of bread into the toaster and, using a clunky computer, turned the toaster on. It would still be a decade before anyone used the phrase "internet of things," but Romkey's magic little toaster showed what a world of internet-connected things might be like. (Of course, it wasn't fully automated; a person still had to introduce the bread.) It was part gimmick, part proof of concept—and fully a preview of what was to come.

The term "internet of things" itself was coined in 1999, when Kevin Ashton put it in a PowerPoint presentation for Procter & Gamble. Ashton, who was then working in supply chain optimization, described a system where sensors acted like the eyes and ears of a computer—an entirely new way for computers to see, hear, touch, and interpret their surroundings.

As home internet became ubiquitous and Wi-Fi sped up, the dream of the smart home started to look more like a reality. Companies began to introduce more and more of these inventions: "smart" coffee makers to brew the perfect cup, ovens that bake cookies with precision timing, and refrigerators that automatically restocked expired milk. The first of these, LG's internet-connected refrigerator, hit the market in 2000. It could take stock of shelf contents, mind expiration dates, and for some reason, came with an MP3 player. It also cost $20,000. As sensors became cheaper, these internet-connected devices became more affordable for more consumers. And the invention of smart plugs, like those made by Belkin, meant that even ordinary objects could become "smart"—or, at least, you could turn them on and off with your phone.

Any IoT system today contains a few basic components. First, there's the *thing* outfitted with sensors. These sensors could be anything that collects data, like a camera inside a smart refrigerator or an accelerometer that tracks speed in a smart running shoe. In some cases, sensors are bundled together to gather multiple data points: a Nest thermostat contains a thermometer, but also a motion sensor; it can adjust the temperature of a room when it senses that nobody's in it. To make sense of this data, the device has some kind of network connectivity (Wi-Fi, Bluetooth, cellular, or satellite) and a processor where it can be stored and analyzed. From there, the data can be used to trigger an action—like ordering more milk when the carton in the smart refrigerator runs out, or adjusting the temperature automatically given a set of rules.

Most people didn't start building an ecosystem of "smart" devices in their homes until the mass adoption of voice controls. In 2014, Amazon introduced the Echo, a speaker with a helpful voice assistant named Alexa built in. Apple had introduced Siri, its own voice assistant, four years prior—but Siri lived on your phone, while Alexa lived inside the speaker and could control all of the "smart" devices in your house. Positioning a voice assistant as the centerpiece of the smart home had several effects: It demystified the internet of things for consumers, encouraged them to buy more internet-enabled gadgets, and encouraged developers to create more "skills," or IoT commands, for these voice assistants to learn

The same year that Amazon debuted Alexa, Apple came out with HomeKit, a system designed to facilitate interactions between Apple-made smart devices, sending data back and forth to create a network. These unifying voices have shifted the landscape away from single-purpose automations and toward a more holistic system of connected things. Tell the Google Assistant "goodnight," for example, and the command can dim the lights, lock the front door, set the alarm system, and turn on your alarm clock. LG's SmartThinQ platform connects many home appliances, so you can select a chocolate chip cookie recipe from the screen of your smart fridge and it'll automatically preheat the oven. Manufacturers bill this as the future, but it's also a convenient way to sell more IoT devices. If you already have an Amazon Echo, you might as well get some stuff for Alexa to control.

By 2014, the number of internet-connected devices would surpass the number of people in the world. David Evans, the former chief futurist at Cisco, estimated in 2015 that "an average 127 new things are connected to the internet" every second. Today, there are over 20 billion connected things in the world, according to estimates from Gartner. The excitement around the brave new internet-connected world has been matched with concern. All of these objects, brought to life like Pinocchio, have made the world easier to control: You can let the delivery man in the front door, or change the temperature inside the house, all with a few taps on a smartphone. But it's also given our objects—and the companies that make them—more control over us.

The internet of things brings all the benefits of the internet to items like lightbulbs and thermostats, but it brings all the problems of the internet, too. Now that people have their speakers, television sets, refrigerators, alarm clocks, toothbrushes, light bulbs, doorbells, baby monitors, and security cameras connected to the Wi-Fi, nearly every device in the house can be compromised, or rendered useless. Consider the whims of internet connectivity: When your Wi-Fi goes down, so do your devices. Router problems? That means you can't turn on the heat with your smart thermostat, or unlock your smart door lock. Things that used to be easy become potentially faulty, if not impossible, when they require an Alexa command or a smartphone control rather than a physical button. Many of these devices also run on proprietary software—meaning, if their manufacturer goes bunk, gets sold, or stops issuing software updates, your clever little gadget becomes a useless hunk of plastic.

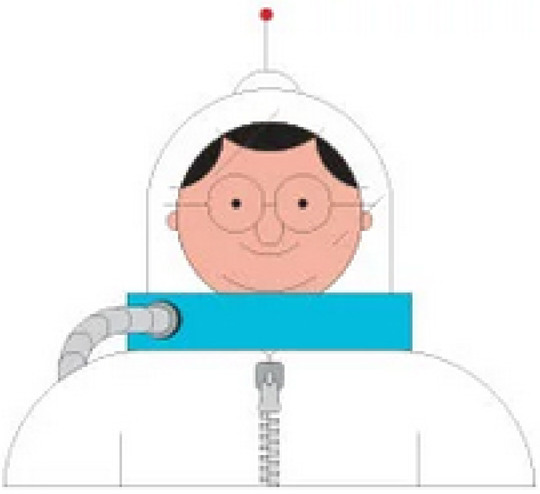
Risk of bricking aside, connecting things to the internet also leaves those objects, and everything else on your Wi-Fi network, more vulnerable to hackers. Laura DeNardis, in her recent book *The Internet in Everything*, has called this threat to cybersecurity the greatest human rights issue of our time. The risk isn't just that some prankster breaks into your smart washing machine and upsets the spin cycle, or that your Nest camera gets hijacked with a message to subscribe to PewDiePie's YouTube channel. (Yes, that really happened.) A hacked smart lock means someone can open your front door. Hack into enough smart water heaters and you can send a city into a massive blackout. And one vulnerable device can compromise the whole network. As WIRED's Lily Hay Newman points out, "IoT devices have been conscripted into massive botnets, compromised for nation-state reconnaissance, hacked to mine cryptocurrency, and manipulated in assaults on power grids."

The threat to internet-connected devices comes not just because they're connected to the internet, but because device manufacturers have not always designed their products with security as a priority. In 2016, malware called Mirai exploited these kinds of vulnerabilities in over 600,000 IoT devices to create a massive distributed denial of service (DDoS) attack. The following year, an attack called Krack infected nearly every internet-connected device connected to Wi-Fi. The attack was crippling and difficult to defend against, in part because the internet of things runs on so many disparate operating systems. When a phone or a computer gets hit with a virus, software makers are generally quick to issue a patch. But things like routers or internet-connected doorbells don't usually receive software updates needed to protect against vulnerabilities, and many of them weren't built with the same kind of security protocols as computers. After the Krack attack, one security researcher predicted that we would still "find vulnerable devices 20 years from now."

The threat of hacks on internet-connected devices remains a big problem, both for companies and for consumers. In 2014, hackers stole credit card information from 40 million Target customers after breaching the corporate network. How did they get in? A malware email was sent to Target's HVAC vendor, which had been given remote access to Target's network. When the vendor clicked the email, hackers had remote access, too. In 2019, Amazon faced a $5 million class action lawsuit from customers who alleged that their internet-connected Ring doorbells had been left open to cyberattacks. Those customers shared stories of hackers who, through their doorbells, harassed them and demanded ransom money. (The company denied blame, claiming instead that it was the customers' fault for using weak passwords.)

These security breaches inspired California's IoT Security Law, the first law of its kind to raise the security standards on IoT device-makers. The law, which applies to any device with the ability to connect to the internet, mandates a series of cybersecurity checks in the product's development and design. For now, those requirements are fairly simple—better authentication and password management, basically—but it's an important first step in regulating the security of internet-connected devices. In 2019, Oregon followed California's lead with its own IoT security law, which mandates that manufacturers build "reasonable security features" into their IoT devices.

Then there's the question of privacy. If cameras and microphones are studded around your home, they are definitely watching and listening to you. Everything in the internet of things collects data—and all that data has value. In a recent study, researchers found that 72 of the 81 IoT devices they surveyed had shared data with a third party unrelated to the original manufacturer. That means the finer details of your personal life—as depicted by your smart toothbrush, your smart TV, or your smart speaker—can be repackaged and sold to someone else. Google and Apple both admitted, in 2019, that the recordings captured by their smart speakers are reviewed by contractors, including awkward and intimate snippets of audio. Amazon has partnerships with over 400 police departments, who use the footage from its Ring doorbell cameras to keep watch on neighborhoods. An ever-expanding internet of things doesn't just have consequences for personal privacy. It can create a network of computer eyes and ears everywhere we go.



The Future of the Internet of Things

One day, the internet of things will become the internet of *every*thing. The objects in our world might sense and react to us individually all the time, so that a smart thermostat automatically adjusts based on your body temperature or the house automatically locks itself when you get into bed. Your clothes might come with connected sensors, too, so that the things around you can respond to your movements in real time. That's already starting to happen: In 2017, Google announced Project Jacquard, an effort to create the connected wardrobe of the future.

In 2018, there were 23 billion connected devices, according to market data from Statista. By 2025, forecasters believe there will be more than 75 billion. Part of that explosion comes from people getting more comfortable with an always-on, data-collecting device that sits in their living room. But it also comes from product-makers dreaming up new things to connect to the internet. This vision extends far beyond your home, and even your clothes. You'll also have smart offices, smart buildings, smart cities. Smart hospital rooms will have sensors to ensure that doctors wash their hands, and airborne sensors will help cities predict mudslides and other natural disasters. Autonomous vehicles will connect to the internet and drive along roads studded with sensors, and governments will manage the demands on their energy grids by tracking household energy consumption through the internet of things. The growth of the internet of things could also lead to new kinds of cyberwarfare; imagine a bad actor disabling every smart thermostat in the dead of winter, or hacking into internet-connected pacemakers and insulin pumps. It could create new class systems: those with robot maids, and those without. Or, as Ray Bradbury described in one short story from 1950, all the people might disappear—but the smart homes, preparing meals and sweeping the floors, will live on.

If we're going to get there—whether we like "there" or not—we're going to need faster internet. Enter: 5G. Crazy-fast internet speeds have long been overpromised and undelivered, but these days, you can see real 5G if you squint. In 2020, as the coronavirus pandemic sent daily work and life into cyberspace, the FCC accelerated its timeline for improving existing internet infrastructure. That could have happy consequences for remote work and school, but might also speed up the possibilities for other internet-enabled devices. China, which is much closer to adopting the 5G standard nationwide, has this year begun testing things like 5G-powered robots in hospital wards to protect doctors from contagious diseases, like the novel coronavirus. Even without 5G, the internet of things supported health care this year. Researchers used the GPS in mobile phones to track the spread of the virus, public health workers used sensors to monitor patients under quarantine, and doctors used internet-connected devices, like drones and robots, to deliver drugs and check on patients without risking contact.

We'll also need to keep all those devices from mucking up the airwaves, and we'll need to find a better way to secure the data that's transmitted across those airwaves. Recently, the Swiss cryptography firm Teserakt introduced an idea for a cryptographic implant for IoT devices, which would protect the data that streams from these devices. And Darpa—that's the Department of Defense's innovation arm—is also working on buffing up the security technology for the military's various IoT devices. That effort, delightfully named CHARIOT (Cryptography for Hyper-scale Architectures in a Robust Internet Of Things), aims to prototype a number of low-cost cryptography techniques to make internet-enabled devices harder to hack into. Darpa's inventions aren't just for the military: Drones, GPS, autonomous vehicles, and the actual worldwide web all came out of the agency's research projects. So if the agency can crack IoT security well enough for the military, it's likely to help your humble HomePod, too.

There are also ideas for creating a better standard for IoT devices, and plans to help them get along with each other, regardless of which company makes them or which voice assistant lives inside. However the internet of things changes the future, first they just need to work. Hey Alexa, can you help with that?