See your free credit score in 2 minutes.

Credit Karma™ Completely Free Credit Score • No Credit Card Required

See My Score

The State of Tech 2016

The Internet of Things is already here—just not the way you expected (http://kernelmag.dailydot.com/issue sections/headline-story/15404/state-of-internet-

of-things-2016/)

By AJ Dellinger on January 3rd, 2016

This was supposed to be the Year of the Internet of Things. In fact, it was the third year in a row that was going to mark the arrival of the connected home, according to everyone from experts at the Massachusetts Institute of Technology to industry leaders like Cisco.

Despite missing the mark in 2013, and 2014, 2015 was for sure going to be when Internet of Things (http://kernelmag.dailydot.com/issue-list/the-internet-of-things/) (IoT) took over, according to the hype generated at the Consumer Electronics Show that kicked off the year. During the Samsung keynote at last year's event, company CEO and president Boo-Keun Yoon declared (http://www.zdnet.com/article/ces-2015-samsung-internet-of-things/) that the Internet of Things "is not science fiction anymore; it's science fact." By the time the ball dropped to mark the arrival of 2016, you were supposed to have a home full of Internet-enabled appliances that would cater to your every need.

As it turns out, your microwave probably won't know what time it is if you unplug it, let alone that this was the year it was supposed to be made obsolete, and your toaster still doesn't know anything about you.

Everyone is waiting for the Internet of Things to take consumers by storm. That likely isn't going to happen, but it's not because IoT isn't a big deal. It's because it's already here.

The sensors are everywhere

"There's about 3 billion more RFID tags in the world than there are smartphones," says Kevin Ashton (https://en.wikipedia.org/wiki/Kevin_Ashton). The British technology pioneer and co-founder of what used to be the Auto-ID Center at MIT sees these types of sensors, now hidden in everything from payment systems to automated toll roads to hotel keycards, as the driving force behind the expansion of the Internet of Things.

If anyone would know how IoT will proliferate, it's Ashton. He coined the term "Internet of Things" in 1997 while managing the supply chain at Procter & Gamble. It was then that he decided to start exploring uses of radio-frequency identification, widely known as RFID, to better track every aspect of manufacturing.

This communication system of batteryless computers creates unique identities for objects and allows these objects to wirelessly send information, making it nearly effortless to track just about anything. Ashton eventually helped to set industry standards for the chips, which have been adopted en masse (http://www.zdnet.com/article/82-percent-of-companies-to-use-rfid/) by large companies and have been in use by many for over a decade.

> **Imagine if owners of Samsung phones could only talk to people with other Samsung devices. That's how many IoT devices operate today.**

It took a little longer to make its way to consumers, but they have also unwittingly adopted RFID technology, along with a plethora of other sensors that are stuffed into smartphones. By 2012, smartphones replaced (http://www.pewinternet.org/files/oldmedia//Files/Reports/2012/Smartphone%20ownership%202012.pdf) cellphones as the dominant device in mobile. That put tiny information trackers in the hands of hundreds of millions of people. GPS, accelerometers, barometers, and other sensors provide a plethora of information about a user without requiring their input. Bluetooth, Wi-Fi, and cellular networks transmit it, along with Ashton's favorite invention, RFID.

"It's already ubiquitous," Ashton says of the Internet of Things. He's right, in the sense that enterprise has largely embraced the technology that enables the IoT, and smartphones and wearables are in nearly every pocket and on nearly every wrist. But expanding the network to appliances and assorted home devices around the home has proven more challenging.

What IoT is and isn't

When we think IoT, we think of things shown through the "smart house" trope (http://tvtropes.org/pmwiki/pmwiki.php/Main/SmartHouse), and companies already in the appliances business happily oblige the fantasy. Samsung invoked just about every fantasy tech invention imaginable when introducing its smartwatch, running an ad (https://www.youtube.com/watch?v=B1QIZowK-PM) for the wearable with clips from *Star Trek*, *The Jetsons*, *Knight Rider*, and *Get Smart*.

It's never going to happen, as Nest CEO Tony Fadell has pointed out. "The people who are pitching those kinds of products, it amazes me," he told *Fast Company* (http://www.fastcodesign.com/3036830/innovation-by-design/nest-ceo-tony-fadell-on-why-jetsons-esque-connected-homes-just-dont-wor) in 2014, about the idea of *Jetsons*-like connected homes. "They just don't work."

What Fadell was getting at, and what he recognized as a creator of an Internet of Things startup, is that people don't buy devices the way companies do. A corporation can afford to purchase an entire system up front—it buys a platform. Ordinary individual consumers, on the other hand, will pick up pieces here and there according to what fits their budget and needs.

The marketplace of connected devices is fractured and fragmented, filled with opportunistic companies hoping to get in on what the International Data Corporation (IDC (http://www.idc.com/)) says (http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/) will be a $7.1 trillion industry by 2020. Just as important as locking customers into companies' own platforms is locking out competitors.

> **"As long as we follow the Web 2.0 business model we will not be able to unleash the real potential of IoT."**

What that leaves for consumers is something that looks similar to the smartphone market; there are a lot of big, familiar names producing slight variations on very similar products. There's just one major difference: Imagine if owners of Samsung (http://www.dailydot.com/tags/samsung/) phones could only talk to people with other Samsung devices. That's how many IoT devices operate today.

Meanwhile, plenty of startups and "little guys," Fadell and the Nests of the world, believe they know best when it comes to getting devices onto the Internet of Things. These companies tend not to last long, generally because anything with promise gets swallowed up by bigger companies that know IoT for the warehouse but can't figure it out for the home.

That is overwhelmingly the way the market has gone, with 15 of 18 IoT startups getting acquired in 2014, according to PitchBook (https://www.hottopics.ht/stories/funding/10-iot-startups-with-the-best-exits/). Every time another kitschy connected device rakes in a couple hundred thousand bucks from crowdfunders, the countdown clock begins on which company will buy them. It might be Philips, the maker of the most popular line of connected lights, or it might be Belkin and its eclectic range of connected devices, but someone is going to swoop in and snag the potential moneymaker.

Big data, big money

The potential retail profit from connected devices—currently priced at a premium because it's the hot new thing—is nice, but the real payday comes in the form of data.

Dropcam gave the world Web-enabled cameras, and Nest brought the smart thermostat to homes; both companies were swallowed by Google. SmartThings, a company that got its start with $1.2 million of backing on Kickstarter, was bought by Samsung despite fairly dismal sales in its first year of operation.

Both companies forked over a premium for products that they believe will eventually net them new information about their customers. With Internet-enabled thermostats and outlets, Google and Samsung can track energy consumption and provide the data to energy companies who might want to advertise their services; they can feed ads from local retailers based off usage data from a smart refrigerator or coffeemaker; they can tell insurance agencies about unreported incidents caught by a connected smoke detector or home security system.

These are billion-dollar industries that would love to be able to better target potential customers, and the data is floating around inside everyone's homes. Google and Samsung, among others, are trying to capture it—and as interested as they are in selling it, they aren't all that into the idea of sharing it.

According to Valentin Heun, a Ph.D. student and member of the MIT Media Lab's Fluid Interfaces Group, companies' tight grip on user data is fracturing the market. "You generate a proprietary data silo with a trusted/dependent user base and then you either sell their data and/or you show them advertisements," he explained. "As long as we follow the Web 2.0 business model we will not be able to unleash the real potential of IoT."

As a remedy, Heun developed Reality Editor (http://www.dailydot.com/technology/mit-reality-editor-app) and Open Hybrid (http://openhybrid.org/), an app and open-source platform respectively, which work together to decentralize IoT and embrace open Internet standards by putting the data back in the hands of the device owners rather than the device makers. Three years in the making, the system communicates directly with objects instead of translating commands through the cloud.

Gerd Leonhard (http://www.futuristgerd.com/), CEO of the Futures Agency (http://thefuturesagency.com/), believes companies chasing user information "will never want less data from us, and they will find it impossible to resist the mantra of 'yes we can and so we will,'" describing it as a "huge issue looming right in front of us." In his estimation, it's an issue that will need to be addressed both on individual and regulatory levels.

Currently, protections for IoT consumers are too often absent. A 2014 study (http://www.symantec.com/connect/blogs/how-safe-your-quantified-self-tracking-monitoring-and-wearable-tech) of connected devices and services found that 52 percent didn't even provide a privacy policy to inform users what can be collected and how it can be used. It's already difficult for companies to avoid the temptation of overreaching when it comes to data; it's even harder to prevent them from crossing the line when there is no line drawn in the first place.

“The problem is similar to why oil companies were and are heavily regulated,” Leonhard says. “Data is the new oil but we have very few regulations as to who, where, when and why.”

Not everyone sees things this way, including Ashton, the man who first envisioned IoT. He views the Internet reliance of devices not as a hindrance but as the whole point in the first place.

“The beauty of the Internet of Things is the Internet,” he says. “IoT devices don’t really need to communicate with each other; they just need to get their data online—after that, everything takes care of itself.”

The future of home vulnerability

Making the Internet of Things work may be as simple as getting the devices to connect to the Web, but everything that goes online appears on a hacker’s radar (http://kernelmag.dailydot.com/issue-sections/features-issue-sections/11318/the-security-concerns-at-the-center-of-the-internet-of-things/).

Ameer Karim, general manager of IoT products and services at Symantec (https://www.symantec.com/)/Norton, believes that connected home technology will take off over the next five years. He’s right, if only because that’s what is going to be pushed on consumers; last year, Samsung’s CEO stated 90 percent of all his company’s hardware will be Internet-enabled by 2017, and every device it sells will be part of the Internet of Things by 2020.

What Karim emphasized is that with more connectivity comes more risk.

“With the prevalence of IoT devices, we expect the learning curve will be even shorter for hackers based on their growing sophistication,” he says. For the time being, hackers are focused primarily on bigger targets. But as more IoT devices go online and collect more information, there will be more motivation to exploit vulnerabilities in the systems.

While threats may not be as prevalent to the home network yet, it’s not as though they aren’t happening. IoT devices have been compromised by insecure mesh networks (https://en.wikipedia.org/wiki/Mesh_networking) created to communicate with one another. Every new item you bring into the house that connects to the Internet presents another new opening that could be exploited. Connected refrigerators have been used (http://www.proofpoint.com/us/threat-insight/post/Your-Fridge-is-Full-of-SPAM) as part of distributed denial-of-service (DDoS (http://www.dailydot.com/tags/ddos/)) attacks, kitchen appliances have been proven (https://www.defcon.org/images/defcon-15/dc15-presentations/DC-15-shalev.pdf) hackable, smart TVs cough up (http://www.rsaconference.com/writable/presentations/file_upload/ht-r08-how-hackers-are-outsmarting-smart-tvs-and-why-it-matters-to-you_copy1.pdf) user information, and even kids’ toys have compromised (http://www.dailydot.com/technology/vtech-learning-lounge-data-breach/) children’s personal information.

Ashton dismissed this danger as simply part of the connected world that we live in. “Security is something you have to address every day, not a problem that gets solved once and for all. Most systems are mostly secure. No systems are invulnerable,” he explained. The question isn’t “Is this system secure?” but rather “Is this system secure *enough*?”

“The beauty of the Internet of Things is the Internet.”

According to Ashton, the answer to that question is yes. "As [connected devices] proliferate, hackers will find and exploit vulnerabilities, and developers will create countermeasures, and so on. That's the way it always works," he says. "I don't see security or privacy concerns as big reasons to avoid adopting the technology."

The truth isn't as clear as Ashton suggests. According to a research paper (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf) published by Symantec in 2014, 20 percent of tested apps for connected devices transmitted user credentials in clear text. That leaves a considerable amount of valuable information, including passwords, simply floating in the ether to be snagged. The report also found many of the sites that house the user data are easily exploitable and could be breached by even unsophisticated attacks.

Karim says research showed that the top IoT devices most at risk of being hacked in 2015 included connected cars, point-of-sale systems, ATMs, and medical devices—"all devices with which consumers interact." There will only be more hitting the market in coming years, and locking them down should be a top priority for device makers.

No boom, but definitely no bust

The Internet of Things is definitely growing. Among self-selected experts interviewed by Pew Research (http://www.pewinternet.org/2014/05/14/internet-of-things/), 83 percent said that by 2025, IoT will have "widespread and beneficial effects on the everyday lives of the public." It just won't be due to people's ability to control their microwaves with their smartphones.

Businesses will continue to adopt the Internet of Things, and consumers will be able to benefit, whether by package-delivery notifications straight to their phones or sharing information from their Fitbits with their doctors. The $70 lightbulbs that connect to the Internet, though? They're not going to be flying off the shelves.

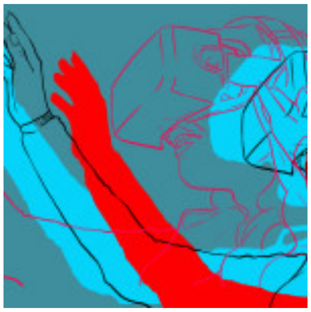
Uses for Internet-enabled appliances and accessories will become clearer once the market takes shape, either via merit or monopoly. Until that happens, though, IoT devices at home are novelty items.

Illustration by J. Longo

More from

<

(http://kernelmag.dailydot.com/issue-sections/features-issue-sections/15396/wearables-



(http://kernelmag.dailydot.cor titles/15409/editors-note-state-of-tech-2016/)The

>

OUT-OF-BAND MANAGEMENT

Always Have Your IT Accessible. Try Our Free Online Demo Today!