SWCP Portal
February 2015

Talking to your toaster in Web 3.0

An Internet of Every Thing 1

The Internet is radically changing our lives yet again. It first did so with email and webpages bringing us connections and information from around the world, and then again with interactive content and social media deepening and enriching those links.

But the revolution underway will be the biggest transformation yet, and it's called the "**Internet of Things**" (IoT). Behind this deceptively bland title is a vision of a universe where people, a wealth of data, the tools we use, even the technological landscape surrounding us are all subtly and constantly linked.

This **Internet of Things** is a dream of an almost magical world where our environments automatically mold to our needs, where data is created and shared by simple things made smarter, including the very clothes we wear, the streets we navigate, even sensors in our own bodies. All of which work together to make life easier, safer, greener, cheaper, and smarter.

IoT's a bold, breathtaking idea, but not without significant problems and serious hazards. Yet it's here already, and within a few years, will invisibly remake the world because it will join everything in it online.

The ultimate result, as Google CEO **Eric Schmidt** **predicted** recently at the Davos economic summit, is that "the Internet will disappear" into the background. With so many networked sensors and devices constantly surrounding us, "it will be part of your presence all the time." Ubiquitous Internet and an interactive environment will be the new normal.

Rooms, he said, will personalize themselves for us the moment we walk in. Since Google just **bought** Nest, a manufacturer of smart thermostats, for *$3.2 billion*, his company has a lot at stake trying to make it so.

A world of thinking, talking machines

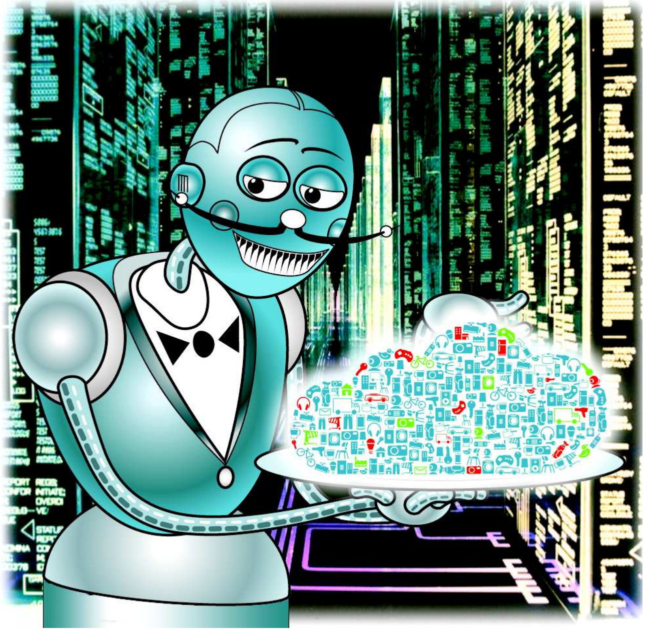
The Internet of Things can be defined as those devices with a Net connection that aren't used primarily for networking. So it's "beyond" the Internet of smartphones, laptops, PCs, servers and gateways, but extends to literally everything else, starting with office printers and faxes.

The IoT's connected smart devices will make automatic decisions; monitoring, sensing, and acting in real time on their own, and may not even have a display or buttons. Consumer applications already include smart thermostats, refrigerators, cars, appliances, alarm clocks, vending machines, and security, sound and lighting systems. But that's just the start.

At this year's **Consumer Electronics Show** in Las Vegas which highlighted the hot new tech trends, the buzz was all about IoT. Wearable devices were big, especially fitness trackers that monitor exercise, and so were smart homes and driverless cars.

While trends showcased there often take a decade to come to fruition, there's no doubt the revolution is underway. One consulting business **estimates** *12 billion* devices are online already, with *26 billion* by 2020. Other estimates call for *30*, *50*, even *212 billion* five years out, but these may be more indicative of the money-making hopes of these firms than reality.

The IoT actually began small and quietly in 1982 when students at Carnegie-Mellon University networked a **Coke-vending machine** to tell them when it was full and the sodas were cold. Yet the consumer side is less than half of the picture, for the Internet of Things is even more important to industry.



Continued on back

Continued from front

From factories to homes

In 1999, the "Internet of Things" was **coined** as a term for networked industrial supply chains. Early applications centered on computerized inventory tracking and control using RFID tags. From there, IoT quickly expanded into bookkeeping: computers collecting customer data and automatically generating bills. Sensors, high-speed links, and proprietary networks for monitoring nuclear plants, power grids, and other industrial processes soon followed.

Now the industrial version of IoT, with its clear cost-saving benefits, is far more developed than the consumer side. But the same forces drive both: smaller, smarter processors and batteries, widespread wireless connections, Cloud computing, and Big Data.

With so many gizmos online, locating them is the first challenge. By 2008, the number of linked devices surpassed the human population. The Net's addressing scheme, **IPv4**, with addresses available for half that amount, is totally inadequate to handle the astronomical numbers involved. But the recent adoption of **IPv6** gives an almost infinite supply of addresses.

Unfortunately, that's the *only* problem that's even come close to being solved so far. Most security and privacy challenges are dauntingly complex. But if they aren't solved adequately, the dream could easily turn into a real-world nightmare.

Problems and perils

The benefits of IoT are almost unimaginable, partially because they add on to each other. Smart buildings are more comfortable and also save energy; smart traffic systems would cut commuting time, save gas and lives, collect tolls on the fly, and end traffic jams.

On a more intimate level, wearable medical sensors could monitor your physical health, linked so that your doctor is automatically notified of changes and also to sensors in your medicine cabinet, bathroom scale, and refrigerator. Your prescriptions will be kept up to date, and timely reminders could be sent to your phone the moment you walk into a store.

Networking giant **Cisco Systems**, who stand to make a huge fortune, confidently **predicts** opportunities amounting to *$1.9 trillion* for business and governments worldwide by 2022. This prospect has inspired a number of industry associations and joint efforts, but few have generated anything useful yet.

One significant problem is **lack of standards and protocols**. There's no agreement on how all these vastly different machines should communicate and interact. Older linked devices are not updateable, or have once-useful features that invite abuse.

By far, the biggest headaches facing IoT are **security and privacy questions**. One **report** from the consumer show indicated that most developers were already engaged in consumer IoT projects, but not many were actively involved with those issues. Few were concerned with the kind of data that wearable monitors gather, how it was used, or who had access.

This apparent nonchalance is even more striking in devices **already in use.** LG TVs, for instance, along with your DVR and cable box, may track your viewing habits. Kitchen appliances could tell burglars your schedule and a *refrigerator* has already been hacked to send out malicious emails. Home security and baby monitoring cameras can and have been hacked and some even send their signals out unencrypted.

Other appliances, like washers and dryers, are vulnerable; smart thermostats can have settings changed by the utility. Vital medical devices, implants like pacemakers, insulin pumps, and also hospital equipment, could be attacked with murderous intent.

In fact, **several years ago**, former CIA Director Petraeus gloated over the possibilities of using TVs, car navigation systems, and smart homes for spying. While being watched by your gaming console or having your heart hacked is bad enough, the stakes involved in industrial exploits are infinitely higher.

Since the **Stuxnet** exploit against Iran, it is now common knowledge that computer viruses can now destroy physical machines. And in the code of that virus, hackers were given an example of just how to wreck industrial processors over the Internet.

Blackmail attempts against powergrids have already happened. **Cyberwar** can now not only wreck the financial system but the actual infrastructure too.

Too much of a good thing?

Even if all these challenges are successfully met, what then? Will you have to argue with your toaster if the bathroom scale tells it you've been eating too much? Striking a sane balance may not be easy but the advantages are too great to ignore – even if *real* privacy offline becomes rare and priceless.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994
505-243-SWCP (7927) ⦿ **SWCP.com** ⦿ **Help@swcp.com**
5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**

Click on blue terms in PDF file to open links.