The New York Times | https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html

STATE OF THE ART

A Future Where Everything Becomes a Computer Is as Creepy as You Feared

By Farhad Manjoo
Oct. 10, 2018

More than 40 years ago, Bill Gates and Paul Allen founded Microsoft with a vision for putting a personal computer on every desk.

No one really believed them, so few tried to stop them. Then before anyone realized it, the deed was done: Just about everyone had a Windows machine, and governments were left scrambling to figure out how to put Microsoft's monopoly back in the bottle.

This sort of thing happens again and again in the tech industry. Audacious founders set their sights on something hilariously out of reach — Mark Zuckerberg wants to connect *everyone* — and the very unlikeliness of their plans insulates them from scrutiny. By the time the rest of us catch up to their effects on society, it's often too late to do much about them.

It is happening again now. In recent years, the tech industry's largest powers set their sights on a new target for digital conquest. They promised wild conveniences and unimaginable benefits to our health and happiness. There's just one catch, which often goes unstated: If their novelties take off without any intervention or supervision from the government, we could be inviting a nightmarish set of security and privacy vulnerabilities into the world. And guess what. No one is really doing much to stop it.

The industry's new goal? Not a computer on every desk nor a connection between every person, but something grander: a computer inside everything, connecting everyone.

Cars, door locks, contact lenses, clothes, toasters, refrigerators, industrial robots, fish tanks, sex toys, light bulbs, toothbrushes, motorcycle helmets — these and other everyday objects are all on the menu for getting "smart." Hundreds of small start-ups are taking part in this trend — known by the marketing catchphrase "the internet of things" — but like everything else in tech, the movement is led by giants, among them Amazon, Apple and Samsung.

For instance, Amazon last month showed off a microwave powered by Alexa, its voice assistant. Amazon will sell the microwave for $60, but it is also selling the chip that gives the device its smarts to other manufacturers, making Alexa connectivity a just-add-water proposition for a wide variety of home appliances, like fans and toasters and coffee makers. And this week, both Facebook and Google unveiled their own home "hub" devices that let you watch videos and perform other digital tricks by voice.

You might dismiss many of these innovations as pretty goofy and doomed to failure. But everything big in tech starts out looking silly, and statistics show the internet of things is growing quickly. It is wiser, then, to imagine the worst — that the digitization of just about everything is not just possible but likely, and that now is the time to be freaking out about the dangers.

"I'm not pessimistic generally, but it's really hard not to be," said Bruce Schneier, a security consultant who explores the threats posed by the internet of things in a new book, "Click Here to Kill Everybody."

Mr. Schneier argues that the economic and technical incentives of the internet-of-things industry do not align with security and privacy for society generally. Putting a computer in everything turns the whole world into a computer security threat — and the hacks and bugs uncovered in just the last few weeks at Facebook and Google illustrate how difficult digital security is even for the biggest tech companies. In a roboticized world, hacks would not just affect your data but could endanger your property, your life and even national security.

Mr. Schneier says only government intervention can save us from such emerging calamities. He calls for reimagining the regulatory regime surrounding digital security in the same way the federal government altered its national security apparatus after the Sept. 11, 2001, attacks. Among other ideas, he outlines the need for a new federal agency, the National Cyber Office, which he imagines researching, advising and coordinating a response to threats posed by an everything-internet.

"I can think of no industry in the past 100 years that has improved its safety and security without being compelled to do so by government," he wrote. But he conceded that government intervention seems unlikely at best. "In our government-can't-do-anything-ever society, I don't see any reining in of the corporate trends," he said.

Those trends are now obvious. It used to be difficult to add internet connectivity to home devices, but in the last few years the cost and complexity of doing so have plummeted. Today, off-the-shelf minicomputers like the Arduino can be used to turn just about any household object "smart." Systems like the one Amazon is offering promise to accelerate the development of internet-of-things devices

even further.

At a press event last month, an Amazon engineer showed how easily a maker of household fans could create a “smart” fan using Amazon’s chip, known as the Alexa Connect Kit. The kit, which Amazon is testing with some manufacturers, would simply be plugged into the fan’s control unit during assembly. The manufacturer also has to write a few lines of code — in the example of the fan, the Amazon engineer needed just a half-page of code.

And that’s it. The fan’s digital bits (including security and cloud storage) are all handled by Amazon. If you buy it from Amazon, the fan will automatically connect with your home network and start obeying commands issued to your Alexa. Just plug it in.

This system illustrates Mr. Schneier’s larger argument, which is that the cost of adding computers to objects will get so small that it will make sense for manufacturers to connect every type of device to the internet.

Sometimes, smarts will lead to conveniences — you can yell at your microwave to reheat your lunch from across the room. Sometimes it will lead to revenue opportunities — Amazon’s microwave will reorder popcorn for you when you’re running low. Sometimes smarts are used for surveillance and marketing, like the crop of smart TVs that track what you watch for serving up ads.

Even if the benefits are tiny, they create a certain market logic; at some point not long from now, devices that don’t connect to the internet will be rarer than ones that do.

The trouble, though, is that business models for these devices don’t often allow for the kind of continuing security maintenance that we are used to with more traditional computing devices. Apple has an incentive to keep writing security updates to keep your iPhone secure; it does so because iPhones sell for a lot of money, and Apple’s brand depends on keeping you safe from digital terrors.

But manufacturers of low-margin home appliances have little such expertise, and less incentive. That’s why the internet of things has so far been synonymous with terrible security — why the F.B.I. had to warn parents last year about the dangers of “smart toys,” and why Dan Coats, the director of national intelligence, has identified smart devices as a growing threat to national security.

An Amazon representative told me that the company was building security into the core of its smart technologies. The Connect Kit, the company said, lets Amazon maintain the digital security of a smart device — and Amazon is very likely to be better at security than many manufacturers of household appliances. As part of its cloud business, the company also offers a service for companies to audit the security of their internet-of-things services.

The Internet of Things Consortium, an industry group that represents dozens of companies, did not respond to an inquiry.

Mr. Schneier is painting government intervention not as a panacea but as a speed bump, a way for us humans to catch up to the technological advances. Regulation and government oversight slow down innovation — that’s one reason techies don’t like it. But when uncertain global dangers are involved, taking a minute isn’t a terrible idea.

Connecting everything could bring vast benefits to society. But the menace could be just as vast. Why not go slowly into the uncertain future?