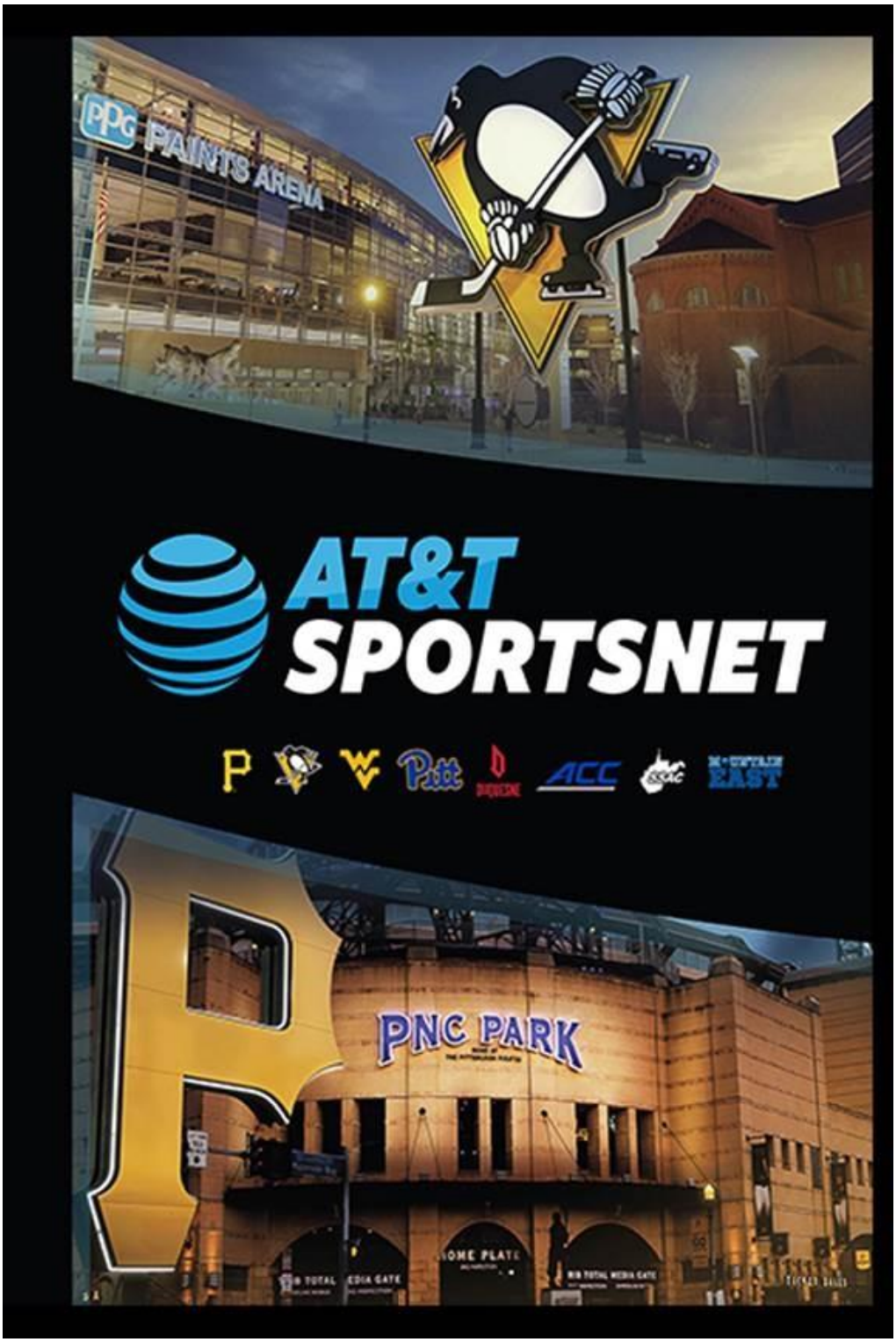

BCAP NewsClips

January 28, 2020

Washington Post
Facebook will now show you exactly

Six years ago, on January 12th 2014, I wrote a Monday Note titled Internet of Things: The "Basket of Remotes" Problem. As I saw it then, there were two Internet of Things: A thriving, professional version for

how it stalks you – even when you're not using Facebook (subscription required)

Ars Technica
Hackers target NFL teams on Twitter ahead of Super Bowl

CNBC
Congress urges Google to act against 'dangerous climate of misinformation' on YouTube

Business Wire
Comcast Acquires Blueface; Global Provider of Unified Communications as a Service (UCaaS) to Complement Comcast Business Solutions

Ars Technica
Maryland bill would outlaw ransomeware, keep researchers from reporting bugs

IHeartRadio Music News
The Internet Can't Get Enough Of Google's New Black History Commercial

Pennlive
Tickets available to see VP Pence, Kellyanne Conway, Betsy DeVos at Cumberland County event

industry and a less mature version for consumers. This is still the case today as the Industrial IoT continues to prosper [as always, edits and emphasis mine]:

"The Industrial IoT is alive and well. A gas refinery is a good example: Wired and wireless sensors monitor the environment, data is transmitted to control centers, actuators direct the flow of energy and other activities. And the entire system is managed by IT pros who have the skill, training, and culture — not to mention the staff — to oversee the (literal) myriad unseen devices that control complicated and dangerous processes."

As for the Consumer version with its promise of intelligent homes with connected appliances — now with the added frisson of Artificial Intelligence — very little progress has been made in the past six years:

"For consumers, technology should get out of the way — it's a means, not an end. Consumers don't have the mindset or training of IT techies, they don't have the time or focus to build a mental representation of a network of devices, their interactions and failure modes. […]

How to represent in one's mind a home network of IoT objects that connect the heating and cooling systems, security cameras, CO and fire sensors, the washer, dryer, stove, fridge, entertainment devices, and under-the-mattress sleep monitoring pads. This may be an exaggerated example, but even with a small group of objects, how does a normal human configure and manage the network?"

At the time, early 2014, there was no answer to the management question, hence the real and figurative recourse to a basket of remotes, to isolated, non-integrated controls for each device. One remote for the TV, another for the heating/cooling system, and so on.

Admittedly, managing your consumer IoT is, six years later, a little bit easier. Thermostats have some intelligence and can be controlled from a smartphone; among other competing solutions Apple's HomeKit and the Home app provides building blocks for tech-savvy users to control lights, power outlets, doors, cameras, and the like, all now accessible through Siri commands. I see convincing examples… at the hands of expert software engineers. But how many normal humans can develop a smarthome system, let alone maintain it when bugs, software updates, or security issues arise?

There is more. We're now seeing problems and issues that we didn't anticipate in 2014. Sonos, the popular smart audio manufacturer, provides a good, publicized example.

First, there was the justifiable objection to the company's Recycle Mode, part of its hardware Trade Up program. You could get a discount on a new Sonos device if you submitted your old one to a software procedure that permanently disabled it after which you would take it to an e-recycling facility. According to Sonos…

"Taking your device to a local certified e-recycling facility is the most environmentally friendly means of disposal"

Protesters objected that the company's claim, which has since been removed from their website, was disingenuous. Is permanently

disabling an otherwise good device — a device that you could have given to a friend or family member — an environmentally sound move? Ah, but that was the condition to get a 30% discount on a newer one.

The Sonos story gets better (meaning worse).

The company recently announced that, in May 2020, it would stop providing software updates to certain older devices. That didn't go over well and, soon, Sonos' CEO partially apologized, confirming that while older products wouldn't get updates, older products would get bug fixes and security patches for "as long as possible".

But I'm not here to pile on Sonos. Instead, let's use the company as an example of a much broader IoT problem.

Consider the hundreds of IoT devices that will control our smartest smarthomes, everything from controlled plugs in the walls, to smart lightbulbs, bridges between Zigbee, Bluetooth, and Wifi networks. Who will administer the inevitable software updates, and with what security guarantees? There's no one-size-fits-all standard for the IoT wireless network, for reasons of power and cost. You come home at the end of the day and your smart lock tells your phone or watch to wait because it has to download and install new software.

Sooner or later — sooner if you let marketeers dictate the pace — obsolescence will strike the hardware of our microprocessor-controlled Things. Someday, you might have to rip out all your AC plugs from the sheetrock in your home. Why? Thanks to the workings of Moore's Law, new plugs are so much more powerful and secure. And, as the manufacturer apologizes from a distant country, your old ones can't be updated because the new and improved software release won't work on a five-year-old microprocessor.

Today, grafting a microprocessor and a Wi-Fi radio onto a power plug is child's play (and a dollar) for the engineers of an appliance maker. Smartplugs that work with Alexa or Google Assistant are plentiful and inexpensive on Amazon, going for as low as $19.98 for a two pack. What will happen when these plugs need updates for bugs and security patches, or when the manufacturer wants to force us to buy a newer, more capable model? This will happen to smart bulbs, locks, cameras, thermostats, dishwashers…

And this is just the beginning of the Consumer IoT fun. The ongoing adoption of 5G technology will bring improvements and another layer of disorganization.

I'm hardly hostile to technology, to the contrary. My professional life in the tech world — more than 50 years — has been enormously fun, I've met remarkable individuals and have seen unimaginable advances such as supercomputers in our pockets. But I now wonder. It was one thing to fight a cranky operating system or application on one's laptop. It created a culture, a folklore. Managing the dozens of devices in a smarthome is a set of tasks for which we are ill-prepared, it's not more of the same.

Nor are we prepared for what happens to our privacy when the IoT devices that share information about our activities become "required" by market forces or, worse, mandated by new laws and regulations.

Imagine what marketers — and government agencies — could do with such information. And pause. There is no could, it will happen, there's too much "stored value" in these network of connected devices, the appetites will be too strong.

The good news, sort of, is that the development of completely computerized smarthomes will progress at a much slower pace than what we enjoyed for smartphones.

More good news is the growing interest in protecting our privacy, at least in reasonably democratic regimes. The slow pace of consumer IoT — and the inevitable bad examples from autocratic countries — might conspire to help devise ways for the Rest Of US to remain in charge. – ***Monday Note, Jean-Louis Gassée***