Some thoughts on IoT

Geoff Huston

Chief Scientist, APNIC
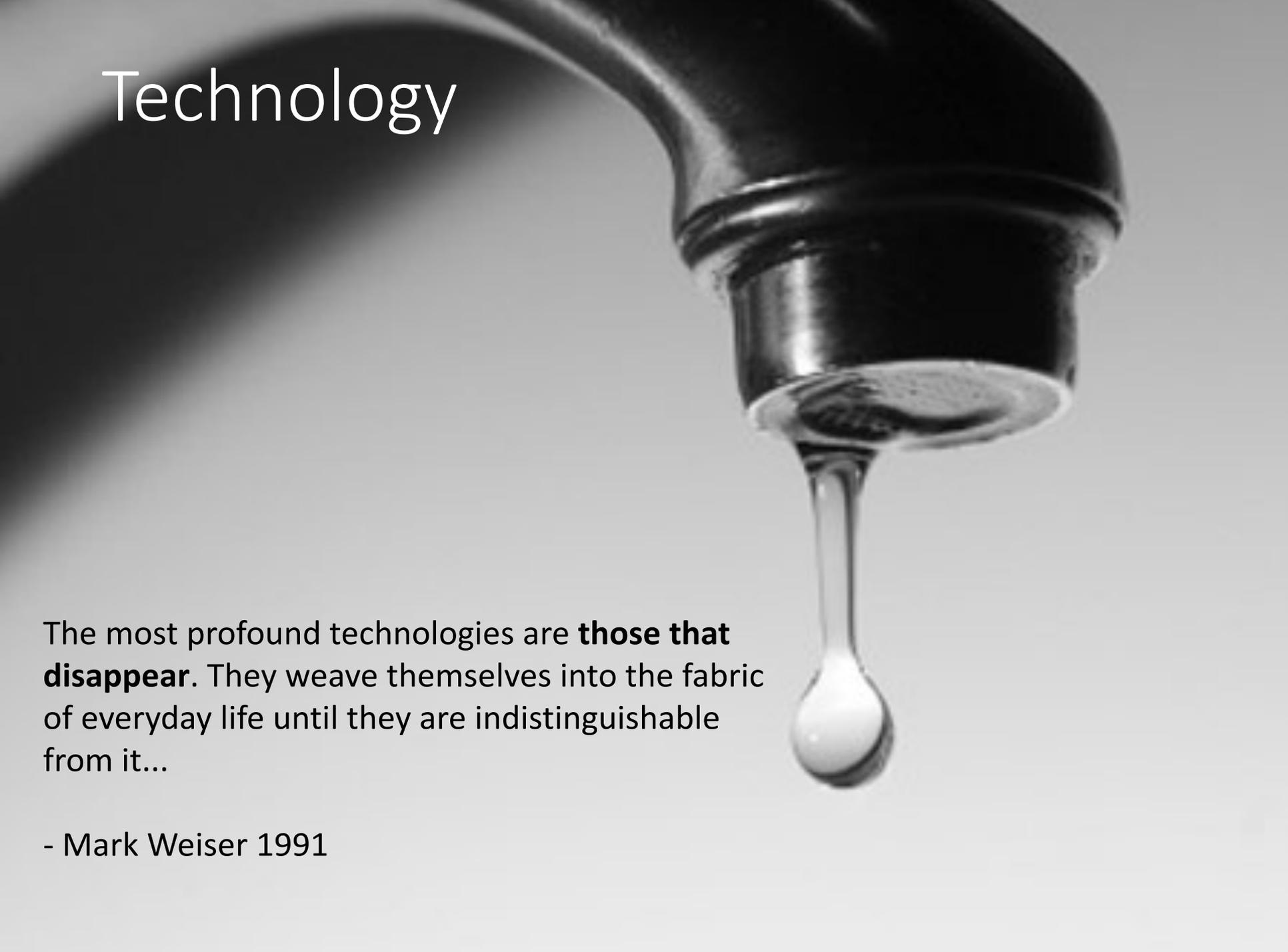
Technology

Does technology change society, or do we develop and adopt technology to address society's changes?

When Meng Tian invented the camel hair paintbrush in 250 BCE he did not invent calligraphy. He responded to a need in ancient Chinese society for more and higher quality written documents that could be produced faster

Technology

The most profound technologies are **those that disappear**. They weave themselves into the fabric of everyday life until they are indistinguishable from it…

- Mark Weiser 1991
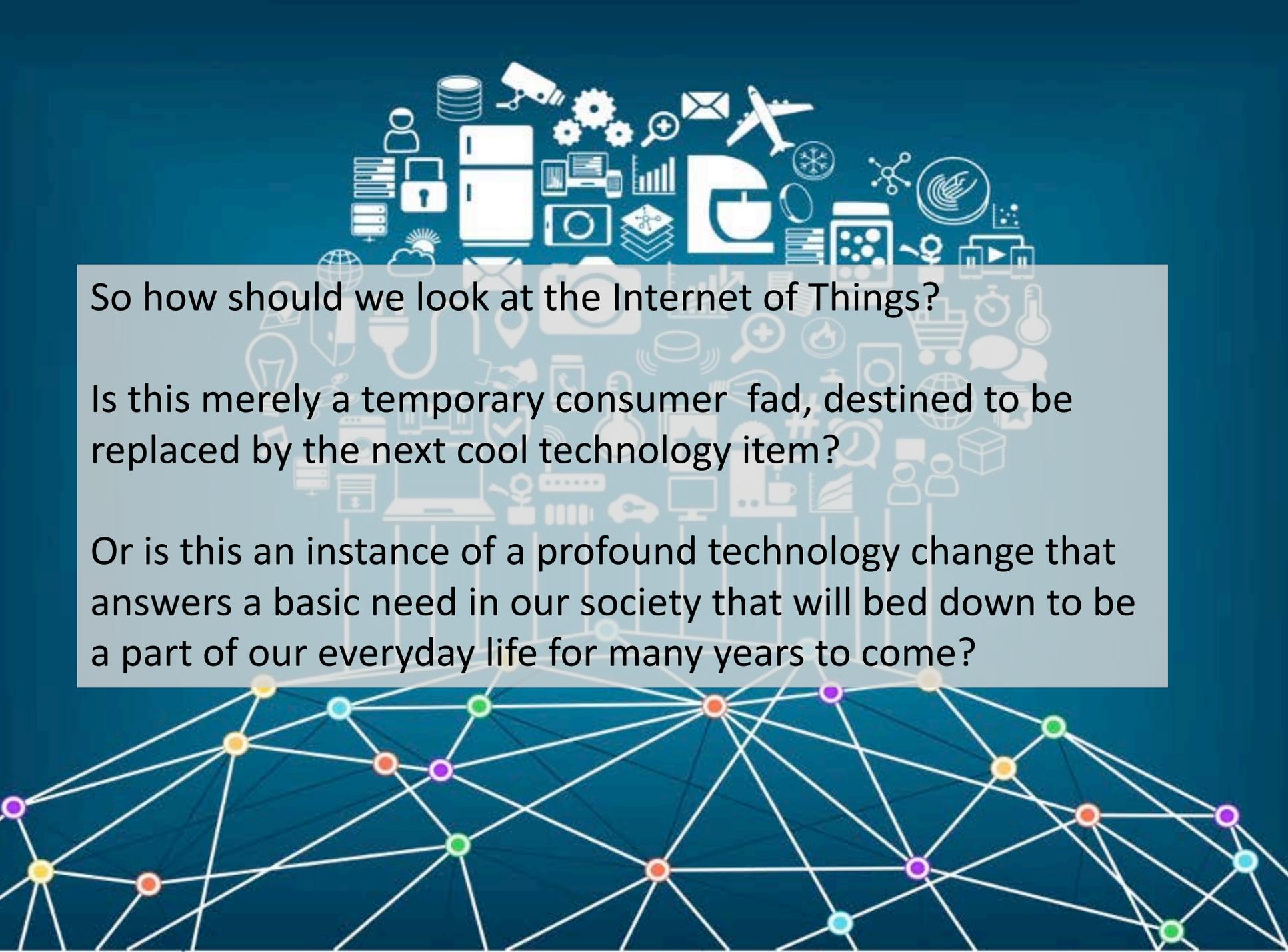
So how should we look at the Internet of Things?

Is this merely a temporary consumer fad, destined to be replaced by the next cool technology item?

Or is this an instance of a profound technology change that answers a basic need in our society that will bed down to be a part of our everyday life for many years to come?

To try and answer this, lets try and put this question into some broader context of the evolution the computer and communications enterprise

Computers were esoteric high frontier research projects
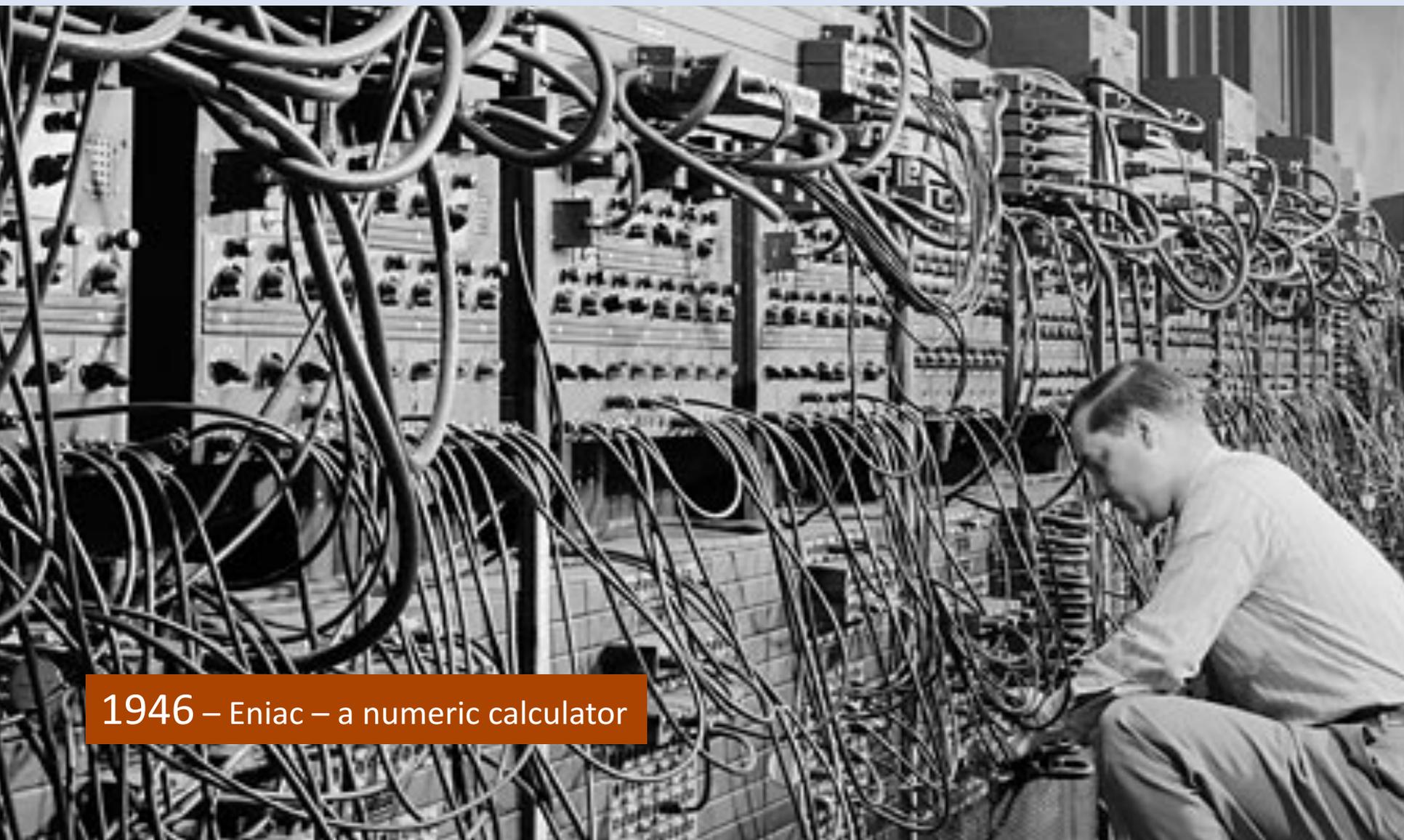
1946 – Eniac – a numeric calculator

Then they became a "must have" business tool

1964 IBM 360 – commercial computing

Extravagant statements of techno power

1976 CRAY-1 – "super" computing

But there was also the hobbyist market
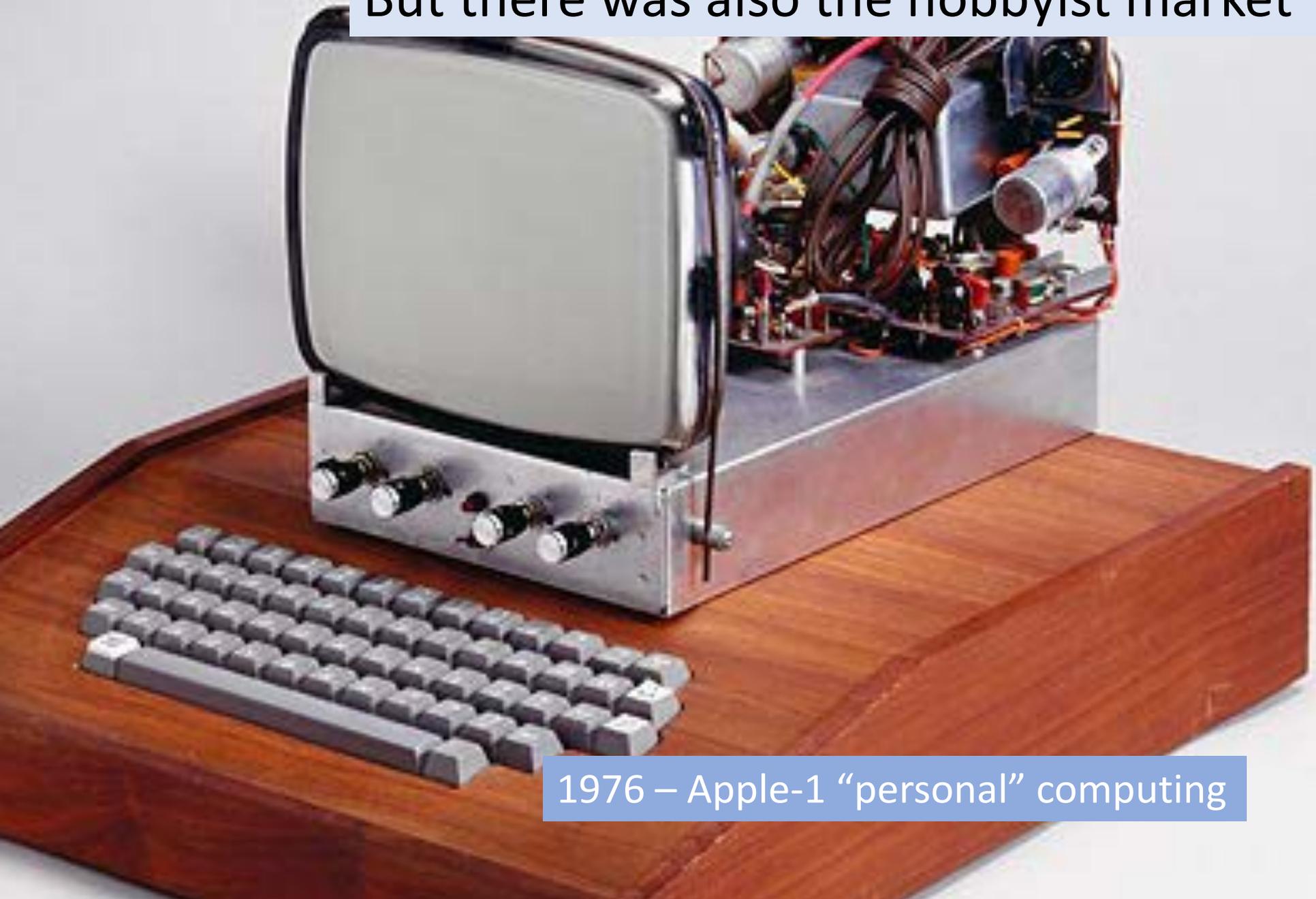
1976 – Apple-1 "personal" computing

Consumer computers as a statement of design style

1984 – Mac

From Style to Mass Marketed Luxury Item

2007 – Apple's iPhone

With desktop devices the Internet of computers was a dedicated activity

lighting

reliable power

privacy

large view screens

dedicated worktop

wired bandwidth

dedicated chair

The Internet is now anywhere and everywhere

radio connectivity

Thumb operated

hand sized

battery power

Its trivial, commonplace and blends into all our activities
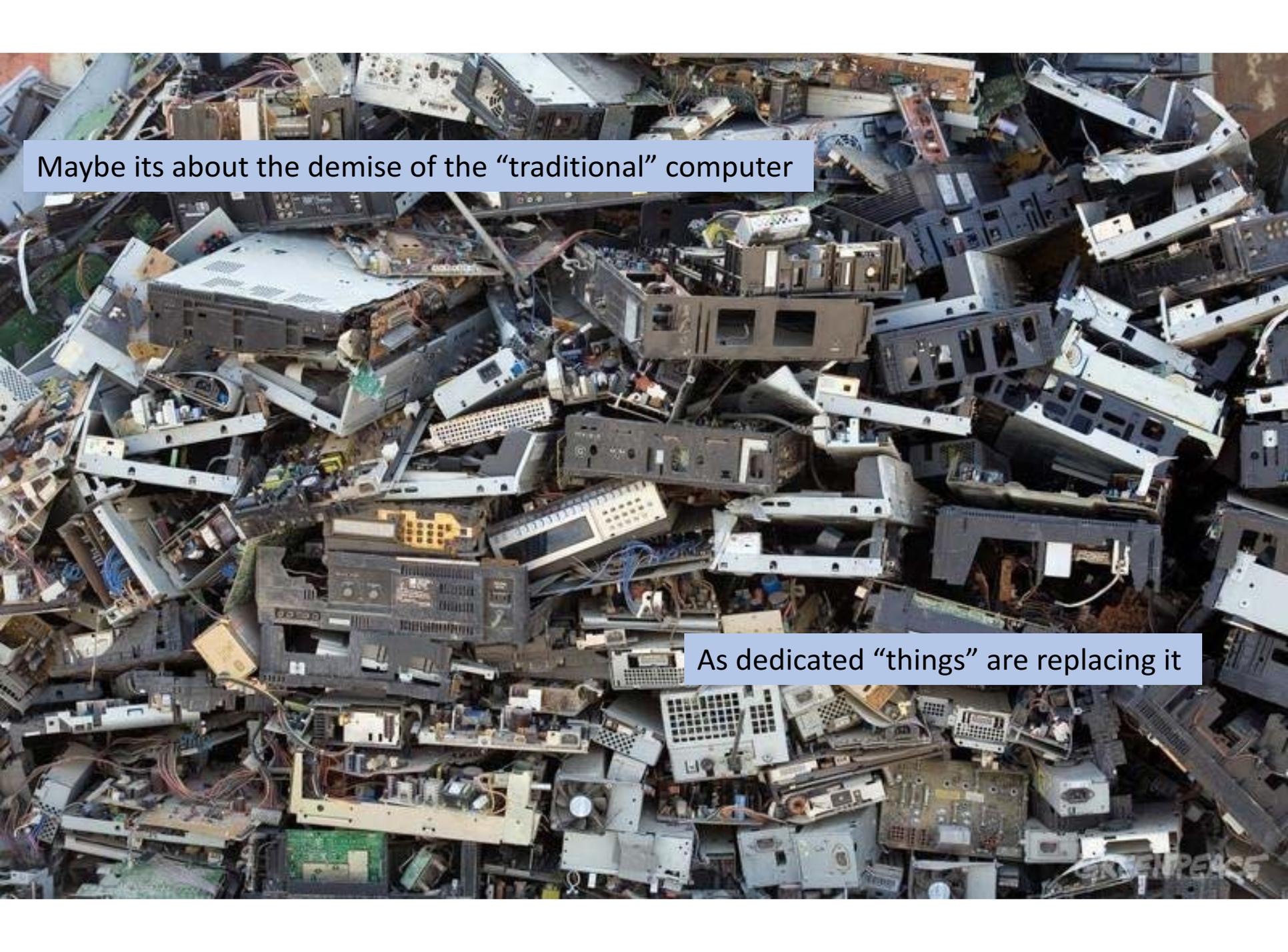
Maybe its about the demise of the "traditional" computer

As dedicated "things" are replacing it
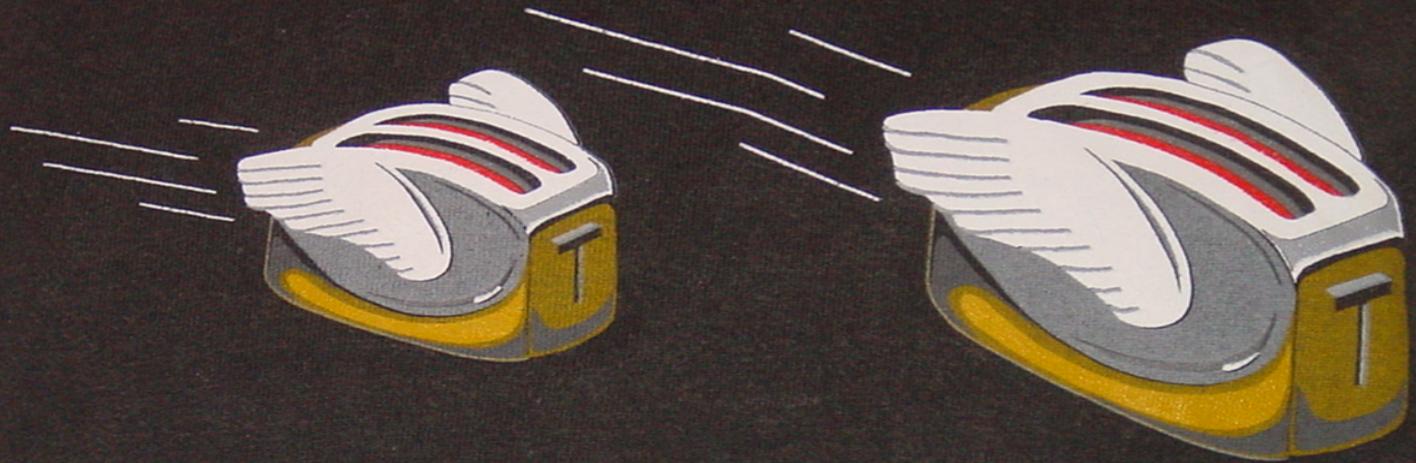
FIRST ANNIVERSARY
TOASTER NET '91

FLYING TOASTERS Artwork © 1991 BERKELEY SYSTEMS, INC.
From AFTER DARK, the Ultimate Screen Saver. Reproduced under
under license agreement by EPILOGUE Technology Corp.

John Romkey's Internet Toaster – Let them eat Toast!

This new IoT is just the old IoT

The use of microprocessors to undertake simple tasks is about as old as the Intel 4004 and the Zylogics Z80 processor chips
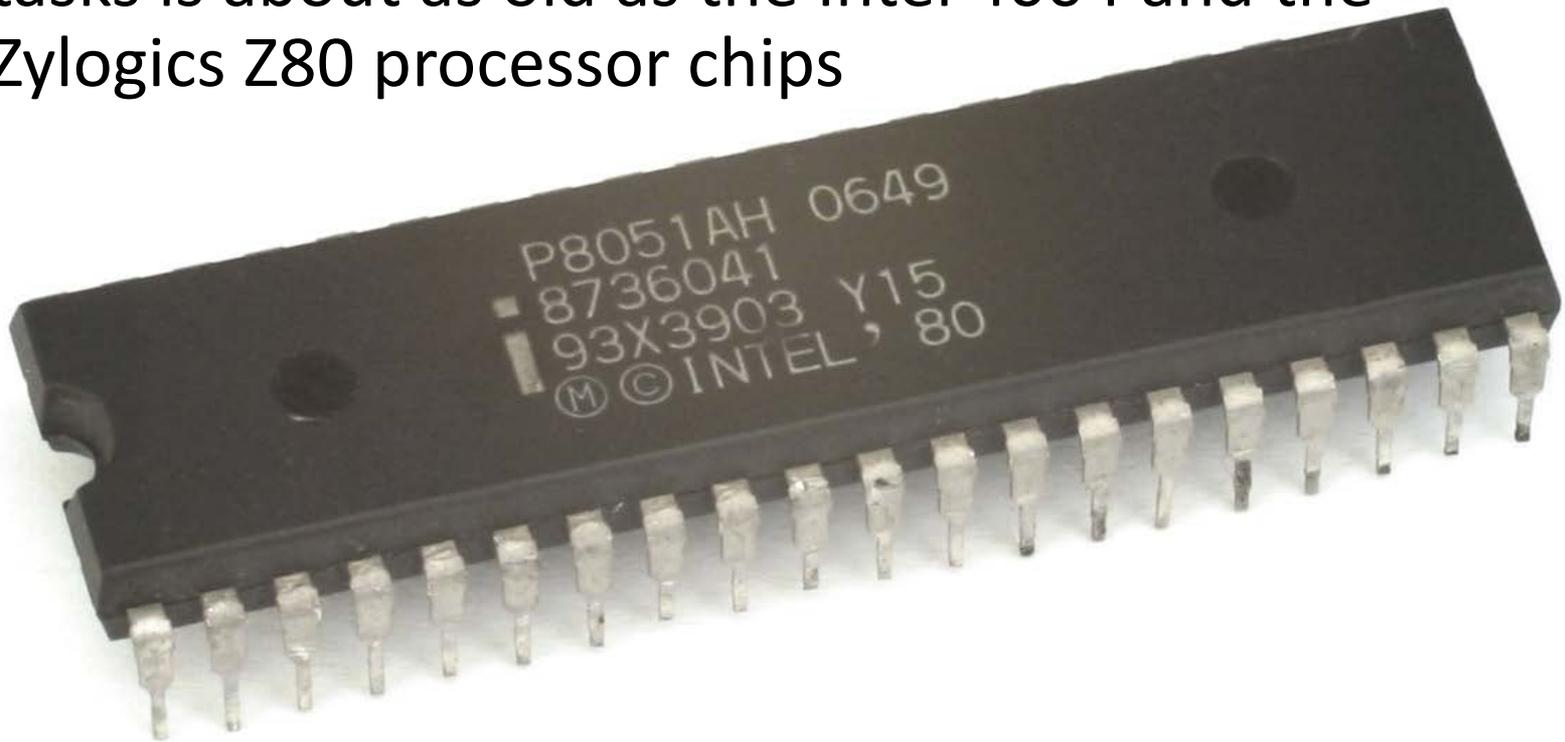
This new IoT is just the old IoT

(with new lipstick!)

And we are already living in a processing-dense world

- A modern car has around 150 – 200 microprocessor-controlled systems, from the windscreen wipers, to the entry system, to engine control and all things in between
- Many / most consumer appliances have all turned to microprocessor control
- Industrial processes, logistics and inventory control, environmental monitoring all use various forms of embedded processing

So why is IoT a hot topic today?

The Hype

Things are Your Foundation

The Internet of Things (IoT) is the heart of the digital business. You need this marriage of operational and information technology to create a business

INNOVATION AWARD HONOREES

Android Auto
The right information for the road ahead

SLEEP TECH AT CES 2017

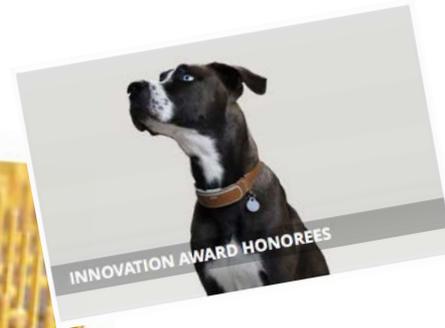For the third year in a row, the Internet of Things has dominated CES. More than 900 companies out of 3,800 at the show said they had Internet of Things products. Andrew Begin at Mirum observed that the IoT has "caught fire in a big way" and Perry Simpson at Direct Marketing predicted that the IoT will solidify "from marketing dream to full on marketing channel."

Build your connected home at the Nest Store.
Shop now ›
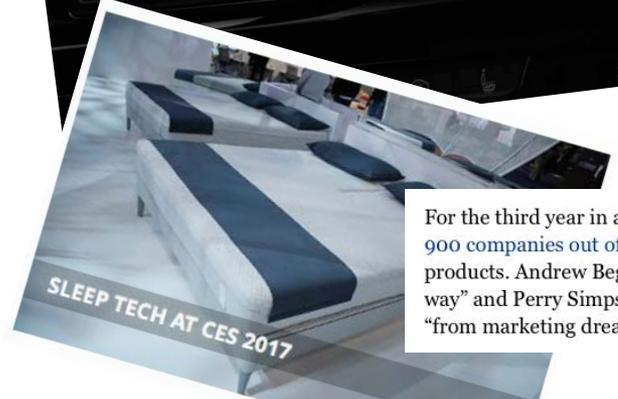
The smart home just got smarter.

With the new Home app, you can securely control all your HomeKit accessories from your favorite iOS device. Have your iPhone turn off the lights. See who's at the front door from your iPad. And even control things remotely with the help of Apple TV. The Home app makes all your connected devices work harder — and smarter — for you.

Lego Boost, on display at CES 2017, allows kids to build their own robot.

IoT is …?

- It is a generic term that encompasses a huge variety of application that have little in common other than a propensity to operate in an unmanaged environment

- Its hard to talk about the IoT in anything other than highly generic terms

Why **now**?

- Low power, high capability silicon now dominates chip fabrication plants

  Saturation of the smart device market

  Full stream silicon production volumes requires some form of consumption model

- Radio Technology: RFID, Bluetooth, WiFi, LTE
  - Improvements in AD convertors is providing range and bandwidth to radio systems
  - Protocol development provides "seamless" connectivity
  - i.e. Passports and Clothing Tags, Apple earbuds, Home controllers and similar

- Actors seeking new markets
  - 5G for SIMs and wide area mobility
  - Smart phone platform providers seeking to enter the car, home and work environments
  - Industrial and process automation seeking to expand market reach

Why **now**?

- Because we have saturated our traditional markets for technology and the production capacity is being redirected to new opportunities
  - PC sales volumes plummeting
  - Smartphone sales are now peaking
  - The computer technology industry is seeking to use its existing capability to provide new product to high volume markets
  - Which means looking at low unit margin very high volume opportunities by adding "smart" network centric interfaces and controllers to existing devices and functions

The opportunities

- "smart" lighting - e.g. Philips
- "smart" home appliances and networks - e.g. Miele
- "smart" power management
- "smart" labels for retail
- "smart" traffic control
- "smart" image analysis
- "smart" video surveillence
- Almost anything else that uses the word "smart"

The Variety of Life *IoT*

It's a set of discrete applications that have highly divergent requirements:

- Radius of connectivity varies from mm to kilometers
- Bandwidth varies from bits to gigabits per second
- Data volumes vary from bytes to petabytes
- Connectivity models may be push or pull
- Connectivity may be ad-hoc relays to dedicated wired
- Transactions may be unicast, multicast or anycast in nature
- Applications include sensing and reporting, command and control, adaptation and interfacing

There is little that these environments have in common, except maybe a common underlying gene pool!

The IoT Gene Pool

Unix

- Its small, its ubiquitous, its well understood, its cheap, its open source without onerous IPR constraints, it has a massive set of application libraries
- Customised micro kernels are risky, expensive and rarely necessary

IP

- Its small, its ubiquitous, it scales, its well understood, its cheap, its open source without onerous IPR constraints, and everyone speaks it!
- But which IP?

IPv4 and IoT

- The "conservative" option for IP in this environment
  - Ubiquitous support across the entire deployed Internet
  - Well understood protocol behaviour
  - Widely available APIs

  Of course it should also be useful to factor in NATs in IPv4:
- Push model where the "thing" pushes data to a rendezvous point rather than a constant pollable model of "pull" access
- "pull" and "feeder" models work behind NATs using relays and/or ALGs split the primary feed from the propagation of the data

IPv6 and IoT

- It's the "killer app" for IPv6

- But the numbers suggest otherwise:
  - 7B connected "devices" on today's IPv4 Internet, plus a further 7B conventional PC and smart devices
  - 2.8B announced IPv4 addresses
  - 1.3B "used" IPv4 addresses
  - We can probably push this model harder!

"Thing" Behaviour

Pull:

- Device is always connected and interrogated by external agents
  - A model of polling or feed subscription where the device maintains information that can be polled by an external agent
  - This requires an public IP address + Port
  - It also requires a highly robust core implementation that is resistant to attack
  - It also requires some considerable thought on the authorization model
    - Device is configured to authorize users and/or
    - Device uses a third party auth server
  - Commonly seen in web cams and other continuous monitoring applications (though it's not necessarily required)

Pull vs Push

Push:

- Intermittedly connected and interrogated via external agents
  - Device pushes data to some data collection agent
  - Limited connection requirement
  - This behaviour NAT "friendly" as the device is the client and the collection point is the server
  - External access via the data collection agent, not the device
  - Does not require dedicated addressing outside of the local context
  - This limited access model facilitates defensive measures, including encrypted communications to the device's agents and preventing all third party connections
  - And such devices probably should be behind a NAT in any case! (e.g. cameras)

Security

Seen at NANOG 69…

The S in IoT is for Security. [1]

Security

Interesting ...

"At last count I have about 43 devices on my LAN, with less than a third running an OS that I can actually interact with. The rest are embedded systems that get updated (hah!) by the vendors at their whim. Easily two-thirds would 'phone home' to somewhere at various times. About 7 have external access without explicitly setting port-forwarding.

Of course, my router monitors and reports on all outbound traffic – but do I actively look at it? I should. But I don't. And of course everything we value on our LAN we protect and encrypt end-to-end and at-rest as the LAN is actually occupied by foreign devices with unknown network capability... sure we encrypt absolutely everything..."

An Internet of ~~Stupid~~ *insanely* Stupid Things

We keep on seeing the same stupidity again and again:

- Devices with the telnet port open

- Devices with open DNS resolvers on the WAN side

- Devices with open NTP / SNMP / chargen etc

- Devices with the same preset root password

- Devices using vulnerable libraries that are susceptible to root kit exploitation

The Internet of Stupid Things

- How do you perform field upgrades of otherwise neglected and unmanaged devices

- What's the economics of incenting field upgrades from the manufacturer?

- Who is responsible for broken "things"?

The Internet of Stupid Things

Is this stupidity even avoidable?

- The bleak picture is maybe not!
- In a price sensitive market where system robustness and quality is largely intangible where is the motive to maintain high quality code?
- How can a consumer tell the difference in the quality of the software, in term of its robustness and security of operation?

high clockspeed industry + commodity components + low margin = market failure for IoT Security

Privacy

Samsung SMART TV
TV has never been this Smart

Privacy

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel | Mo

NEWS

Home | Video | World | Asia | UK | Business | Tech | Science | Magazine | Entertainmen

Technology

Not in front of the telly: Warning over 'listening' TV

9 February 2015 | Technology

< Share

Samsung said personal information could be scooped up by the Smart TV

Samsung is warning customers about discussing personal information in front of their smart television set.

The warning applies to TV viewers who control their Samsung Smart TV using its voice activation feature.

When the feature is active, such TV sets "listen" to what is said and may share what they hear with Samsung or third parties, it said.

Privacy campaigners said the technology smacked of the telescreens, in George Orwell's 1984, which spied on citizens.

Samsung S

Samsung SMART TV
TV has never been this Smart

Some things you can count on…

- The volumes are already huge, and they're growing
  - "Things" already outnumber everything else on the Internet
- Security is an unachievable word!
- Privacy is now an historical concept
- Digital pollution is pervasive and we now have an internet that is a largely chaotic and hostile environment

And some things we can't tell

- Will we standardize this area or will it be a diverse set of mutually incompatible devices?

- Will the market consolidate to be dominated by a small number of providers and their pseudo-open proprietary architectures?

- When will the IoT embrace IPv6?

- Will the IoT market ever discriminate on quality and rebustness?

- How do we manage the risk of coercion of these devices?

And some things we can't tell

- How bad can it get?

It's a tough problem...

"The market can't fix this because neither the buyer nor the seller cares.

The owners of the webcams and DVRs used in the denial-of-service attacks don't care. Their devices were cheap to buy, they still work, and they don't know any of the victims of the attacks.

The sellers of those devices don't care: They're now selling newer and better models, and the original buyers only cared about price and features.

There is no market solution, because the insecurity is what economists call an externality: It's an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution."

https://www.schneier.com/blog/archives/2017/02/security_and_th.html

Thanks!