IoT (Internet of Things)

Internet governance series of webinars

Ms Desiree Miloshevic, Senior Public Policy and International Affairs Advisor in Europe for Afilias

28th November 2013 – Webinar

IoT Agenda

▶ Defining the word "IoT"; History and people involved

▶ How close are we to a broader commercial adoption of this concept?
   ▸ IoT examples from the real world; IoT and Namespace

▶ What are the issues surrounding the Internet of Things?
   ▸ Cloud storage a major player in the IoT space

▶ What impact will the Internet of Things have on IG?
   ▸ Privacy; Security; Does IoT require different regulation?

▶ What Next? Who's working on what?

▶ Questions & Answers

Defining the word "IoT"

> The Internet of Things (or IoT for short) refers to uniquely identifiable objects and their virtual representations in an Internet-like structure.

- "Internet of Things"
  - Isn't everything connected to the Internet a "thing?"
    - Yes – This is just a buzzword
    - No – There's a whole new class of "things" – not defined

- IoT encompasses a whole new world of connections

- There's more than one definition of IoT
  - Wikipedia has at least six definitions today
  - This is still uncharted territory

- … IoT is "a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities"

https://en.wikipedia.org/wiki/Internet_of_Things

Ms Desiree Miloshevic - @Des
28 November 2013

IoT – Oxford Dictionaries - 2013

Definition of **Internet of things** in English

noun

a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data:

if one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security

★ siliconrepublic®

Digital Life

Oxford Dictionaries online now includes selfie, phablet and digital detox

28.08.2013

Tech terms 'selfie', 'phablet', 'digital detox' and 'internet of things' have now taken their place in the Oxford Dictionaries online, joining 'omnishambles', the word the Oxford English Dictionary voted as its word of the year last year.

Oxford Dictionaries online defines its new tech terms:

Selfie: a photograph that one has taken of oneself, typically one taken with a smartphone or webcam and uploaded to a social media website.

Phablet: a smartphone having a screen which is intermediate in size, between that of a typical smartphone and a tablet computer.

Oxford Dictionaries online now includes selfie, phablet and digital detox

Digital detox: a period of time during which a person refrains from using electronic devices, such as smartphones or computers, regarded as an opportunity to reduce stress or focus on social interaction in the physical world.

Internet of things: a proposed development of the internet in which everyday objects have network connectivity, allowing them to send and receive data.

Omnishambles is defined as "a situation that has been comprehensively mismanaged, characterised by a string of blunders and miscalculations". Oxford Dictionaries online credits the British satirical TV series *The Thick of It* as the first user of the word.

Ms Desiree Miloshevic - @Des
28 November 2013

IoT – History and the people involved

▶ **Peter Cole @ University of Adelaide**
  ▶ Founder Integrated Silicon Design – pioneering RFID research 1984

▶ **Kevin Ashton @ Auto-ID Center at MIT**
  ▶ RFID Journal, That 'Internet of Things' Thing" 1999

▶ **Rob van Kranenburg @ Institute of Network Cultures**
  ▶ The Internet of Things. A critique of ambient technology and the all-seeing network of RFID 2008

▶ **Jari Arkko @ Ericsson Research (current IETF Chair)**
  ▶ Building the Internet of Things 2011

http://www.rfidjournal.com/article/view/4986

Ms Desiree Miloshevic - @Des   28 November 2013

IoT – An example scenario

▶ **Classic IoT example – paradigm shift in supply chain**

1) You run out of milk (or the date expires)
2) Your refrigerator orders fresh milk from the supermarket

Christopher Mims
August 23, 2011

Do We Really Need an Android-Powered Fridge?

The worst thing about "smart" appliances isn't that they're redundant. It's that they missed an opportunity to become part of the Internet of Things.

The Register

Data Centre   Software   Networks   Security   Policy   **Business**   Jobs

Financial News   Small Biz   CIO   Media

BUSINESS > MEDIA

Fridges to be hit by Net viruses

ILoveYou will turn your milk sour

By Linda Harrison, 21st June 2000

Neutralize advanced malware

Fridges and household appliances may be the future victims of PC-related bugs.

Russian anti-virus company Kaspersky Lab is warning that in a few years Internet-connected microwaves and freezers will be prime targets for virus creators.

DOCTOR FUN   4 June 2003

The brave new world of IPv6

IoT – Hype; just like the "Cloud" hype

Positive press

BUSINESS INSIDER — Tech · Finance · Politics · Strategy · Life · Entertainment · All

TECH

More: Mobile · Internet of Things · Consumer Electronics · Business Growth

Here's Why 'The Internet Of Things' Will Be Huge, And Drive Tremendous Value For People And Businesses

EMILY ADLER   NOV. 22, 2013, 5:51 PM   93,940   28

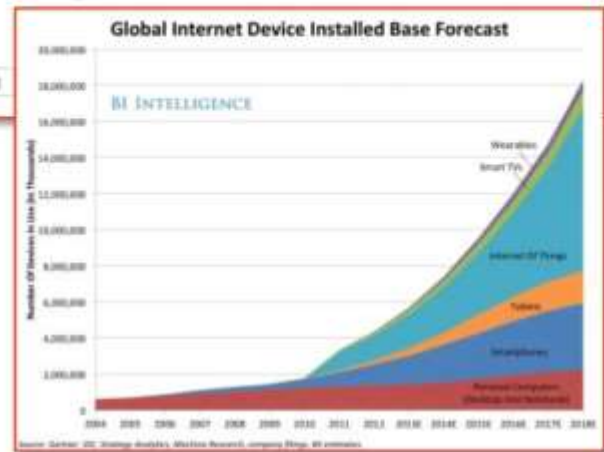Recommend 968   Share 1,728   Tweet 1,520   +1 311

Global Internet Device Installed Base Forecast

BI INTELLIGENCE

The Internet Of Things Will Be Huge—Just Not As Huge As The Hype

Various reports claim the Internet of Things will boost the global economy by trillions of dollars. Don't believe them.

Brian Proffitt on November 08, 2013
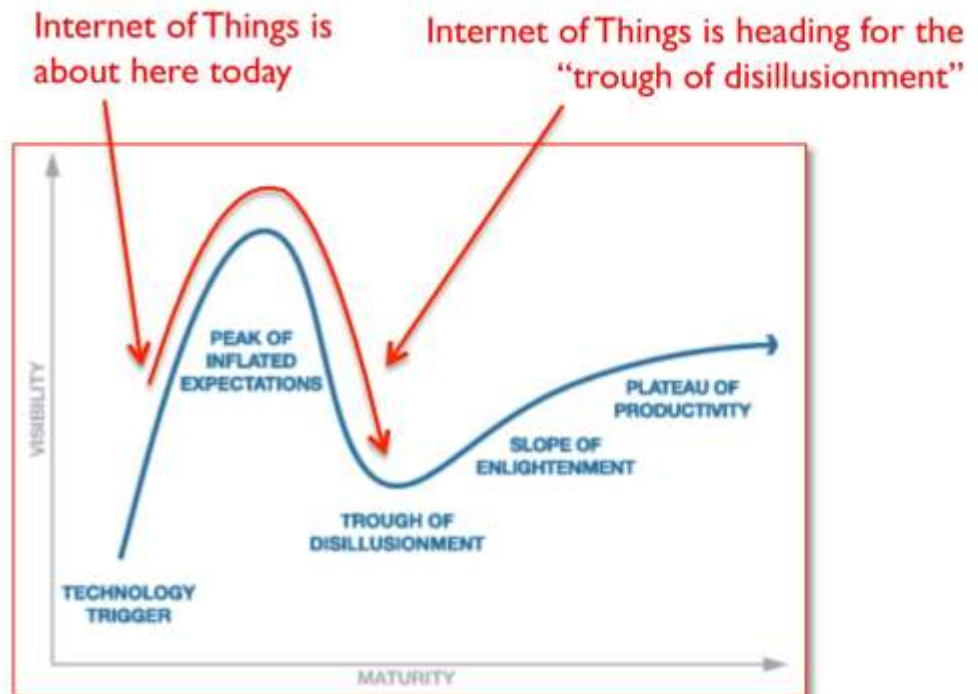
Negative press

IoT – Hype; defining where we are today

- ## Use the Gartner "Hype Cycles" graph
  - ### We have very high expectations yet no practical productivity

Gartner Hype Cycles

Interpreting Technology Hype

When new technologies make bold promises, how do you discern the hype from what's commercially viable? And when will such claims pay off, if at all? Gartner Hype Cycles provide a graphic representation of the maturity and adoption of technologies and applications, and how they are potentially relevant to solving real business problems and exploiting new opportunities. Gartner Hype Cycle methodology gives you a view of how a technology or application will evolve over time, providing a sound source of insight to manage its deployment within the context of your specific business goals.

Internet of Things is about here today

Internet of Things is heading for the "trough of disillusionment"

PEAK OF INFLATED EXPECTATIONS

VISIBILITY

PLATEAU OF PRODUCTIVITY

SLOPE OF ENLIGHTENMENT

TROUGH OF DISILLUSIONMENT

TECHNOLOGY TRIGGER

MATURITY

Gartner Hype Cycle: Each Hype Cycle drills down into the five key phases of a technology's life cycle.

IoT – Real world examples

Ms Desiree Miloshevic - @Des

28 November 2013

http://www.iotlist.co/

IoT – Real world examples – Home

- ## Home Automation
  - Power socket control (turn on anything)
  - Full heating / cooling control
  - Smoke detector
  - Garden watering

- ## All providing access from anywhere
  - Data uploaded to the "cloud"
  - Status available from anywhere
  - Control available from anywhere

- ## No unified protocol
  - No industry WebAPI standard

Ms Desiree Miloshevic - @Des

28 November 2013

IoT – Real world examples – Health

▸ **Health monitoring**

    ▸ Heart Rate monitor

    ▸ Exercise (for health insurance reasons?)

▸ **Actively adjusting your health**

    ▸ Insulin pumps remotely adjustable by doctor

    ▸ Pacemaker monitoring and adjustment

▸ **Now think about the security issues**

    ▸ Specific (health related) data uploaded

    ▸ Potentially arbitrary data uploaded

The pacemaker story ...

HOME PAGE | MY TIMES | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times

Business

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

MEDIA & ADVERTISING | WORLD BUSINESS | SMALL BUSINESS | YOUR MONEY | DEALBOOK | MARKETS | RESE

A Heart Device Is Found Vulnerable to Hacker Attacks

By BARNABY J. FEDER
Published: March 12, 2008

To the long list of objects vulnerable to attack by computer hackers, add the human heart.

The threat seems largely theoretical. But a team of computer security researchers plans to report Wednesday that it had been able to gain wireless access to a combination heart defibrillator and pacemaker.

They were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal — if the device had been in a person. In this case, the researcher were hacking into a device in a laboratory.

The researchers said they had also been able to glean personal patient data by eavesdropping on signals from the tiny wireless radio that Medtronic, the device's maker, had embedded in the implant as a way to let doctors monitor and adjust it without surgery.

nakedsecurity

Award-winning news, opinion, advice and research from SOPHOS

malware   mac   facebook   android   vulnerability   data loss   privacy   more...

Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking

by Lisa Vaas on October 22, 2013 | 1 Comment
FILED UNDER: Celebrities, Data loss, Denial of Service, Featured, Malware, Security threats, Vulnerability

Former US Vice President Dick Cheney's doctors disabled his pacemaker's wireless capabilities to thwart possible assassination attempts, he said in an interview with CBS's "60 Minutes" that aired on Sunday.

Cheney's heart problems were bad: between 1978 and 2010, he suffered five heart attacks, underwent quadruple bypass surgery, and had a pump implanted directly to his heart. A defibrillator was implanted to regulate his heartbeat in 2007.

Cheney told his 60 Minutes interviewer, CNN Chief Medical Correspondent Dr. Sanjay Gupta, that at the time of the pacemaker implant, he was concerned about reports that attackers could hack the devices and kill their owners:

RT   QUESTION MORE.   LIVE

News | USA | Russian politics | Business | Op-Edge | In vision | In motion

Hacker dies days before he was to reveal how to remotely kill pacemaker patients

Published time: July 26, 2013 15:07
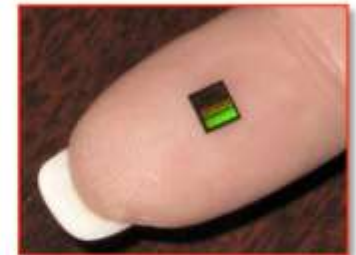Edited time: July 27, 2013 09:00

IoT – Why namespace matters?

▶ **RFID (Radio Frequency ID)**

  ▶ Electronic tags attached to items; enabling tracking

  ▶ Great for clothes, pets, box shipping/tracking

▶ **UPC (Universal Product Code)**

  ▶ On nearly all products

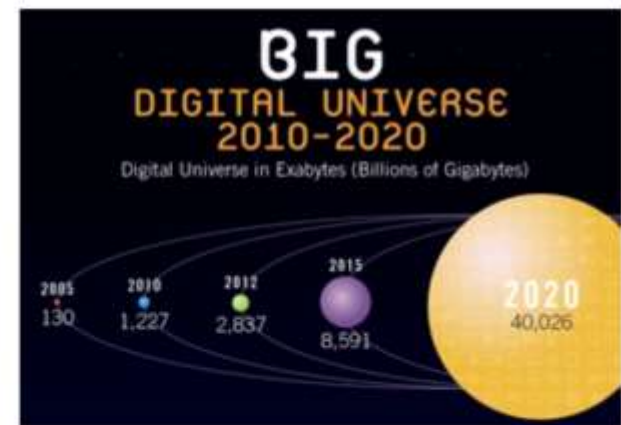 ▶ Supermarket checkout scanning

▶ **EPC (Electronic Produce Code)**

  ▶ Unique identity for every physical object anywhere in the world, for all time.

  ▶ Like UPC; but electronic

urn:epc:id:sgln:647132.435322.1

IoT – Driving lots of data into the cloud

- IDC 2012 study provides insight into the real numbers

  - "IDC now forecasts that we'll be generating 40 ZB (that's zettabytes, or trillions of gigabytes) by 2020"

  - "by 2020, 1.7 MB of new information will be created for each and every human being on the planet -- every second of every day"

  - "We are fast approaching a world where everything around us is potentially intelligent (compute, storage, etc.) meaning that the 'internet of things' is not only real and tangible, but will likely dwarf the amount of information we produce and consume as individuals"

The "internet of things"

Things versus People (Billion): 2020

People 7.6

Things* 200

*Includes computers, phones, vehicles, machines, toys, and smart devices that could be equipped with digital communications

BIG DIGITAL UNIVERSE 2010-2020

Digital Universe in Exabytes (Billions of Gigabytes)

2005 130
2010 1,227
2012 2,837
2015 8,591
2020 40,026

Ms Desiree Miloshevic - @Des

28 November 2013

IoT – Who controls the data?

- Inability of current institutions to deal with anything digital (i.e. data)

- Internet + IoT = Changes the nature of power

- Vertical integration and the lack of data oversight
  - Proprietary applications; proprietary data

- Ownership of data ill defined

Ms Desiree Miloshevic - @Des

IoT – Money being spent!

Beijing plans to invest 5 billion yuan ($800 million) in the IoT industry by 2015. The Ministry of Information and Technology estimates China's IoT market will hit 500 billion yuan ($80.3 billion) by 2015, then double to 1 trillion yuan ($166 billion) by 2020.

The level of hype around the financial promise of the Internet of Things is truly gargantuan. A May 2013 report from the McKinsey Institute suggests that connecting billions of ordinary devices to the Internet will add between $2.7 trillion and $6.2 trillion a year to the global economy by 2025.

Cisco, which has a big stake in the hardware infrastructure for a thriving Internet of Things, estimates that what it calls "the Internet of Everything" will boost global output by $14.4 trillion over 9 years, or a comparatively sane $1.6 trillion a year. General Electric, by contrast, goes even bigger than McKinsey, and estimates that the "Industrial Internet" will boost global GDP by $15.3 trillion in 2030.

Emergence of mega-market

IoT – Establishing new regulation

▶ **The EU is looking at IoT**

▶ CORDIS – An action plan for the European Union to introduce the governance based on the Internet of Things

▶ CASAGRAS – Coordination and support action for global RFID-related activities and standardization

▶ **The US Government FTC (Federal Trade Commission)**

▶ November 2013 Workshop "to explore consumer privacy and security issues posed by the growing connectivity of devices"

▶ **Chinese Government**

▶ Chengdu Internet of Things Technology Institute

http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf
http://www.ftc.gov/bcp/workshops/internet-of-things/
http://www.citti.com.cn/EN/

IoT – Privacy & Security

▶ WIRED January 2013 - "unprecedented security challenges in data privacy, safety and governance and trust"

▶ EU's "IoT Week 2013" June 2013 Helsinki Finland

    ▶ Privacy & Security Workshop

▶ US Government FTC set to investigate rules for the IoT

The rise of such connected devices essentially takes the established privacy framework the FTC adopted for web data and throws the problem into three dimensions. The FTC had established several categories of "sensitive data" in its 2012 Privacy Report, including Social Security numbers, precise geolocation data, financial records, health information and information about children. This data required higher levels of user consent and protections.

IoT – What's next? Who's doing what?

▶ **What next?**
  ▶ More visibility in consumer products
  ▶ Overhaul in security and privacy (of data, protocols and devices) hence new regulations
  ▶ More regulation of corporate data responsibility and transparency

▶ **Who's doing what?**
  ▶ Commercial
    ▶ http://iofthings.org/ - Internet of Things Consortium
    ▶ http://share.cisco.com/internet-of-things.html - Cisco Systems
    ▶ http://www.intel.com/ - Intel "IoT Solutions Group"

  ▶ European Union
    ▶ http://www.internet-of-things.eu/ - Internet of Things Europe
    ▶ http://www.iot-a.eu/public - Internet of Things Architecture
    ▶ http://www.iot-i.eu/public - The Internet of Things Initiative
    ▶ http://www.internet-of-things-research.eu/ - European Research Cluster

  ▶ US Government – NIST (National Institute of Standards and Technology)
    ▶ http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910478 - Internet of "What?"

IoT – Summary

▶ Hype

▶ Massive data creation

▶ Early dawn of regulatory oversight

Ms Desiree Miloshevic - @Des   28 November 2013

IoT – Questions and Answers

Ms Desiree Miloshevic - @Des

28 November 2013