Dear Madam, Sir,

please find hereafter my contribution to this important discussion that I hope will give some additional food for thought for the further discussion.

Yours faithfully,
Dr Cees J.M. LANTING

- On leave from the CSEM research centre in Switzerland
- Senior Consultant at DATSA Belgium sprl Consulting services

- Outgoing Co-Chair EPoSS Working Group Manufacturing & Robotics
- Outgoing Co-Chair EPoSS Working Group Smart Communications – IoT
- EPoSS rapporteur for IoT and Building automation

- Member of the Business Advisory Council of the School Economics and Business (SEB) of State University of NY (SUNY) Oneonta

EPoSS = The European Technology Platform on Smart Systems Integration
Covering, among others, the IoT aspects of Smart Systems and Cyber Physical Systems

## Table of Contents

# Some recommendations and conclusions

**Rate of development and economic lifetime of equipment**
The developing IoT market is wrongly associated with smart phones and the related Google services markets.
Instead, it should be compared with the telecom market: developing slower due to deployment and roll-out delays, and with significant longer economic lifetime of the equipment, in the networks, at private company premises and even at consumer premises.

**The 'Google business model'**

The 'Google business model' may not work in IoT: whereas in 'the Internet of People' users give away data, even sensitive data, in return for access to some (useful) services, in an IoT environment access to data will be restricted:

**Market size**
It has to be concluded that, in spite of possibly large numbers of connected devices (estimated at 250 Billion by 2020), the market volume for both equipment and services will be much smaller than expected, and the market will develop slower, so that the market volume per year will be significantly lower than some expectations

**IoT and possible roles for the Government**

- It would make sense for local, state and federal governments to foster development of equipment and infrastructure for those applications where:
  - The usage would constitute a significant benefit for society,
  - While market functioning may not be sufficient
- The regulatory model can be based on three components:
  - Telecom regulation for the communications infrastructure
  - Surveillance cameras with view on public or others' property
  - And, the new component, non-imaging devices collecting data (also) from public or others' property
- Needed is a set of rules concerning the ownership of data.

**Some critical remarks up-front**

- If everything is seen as IoT, then at least some structuring of ‘everything’ would be required.
- Everybody knows what IoT, Industry4.0 and Big Data is. Except for the people that understand at least something about it.
- It would be helpful if people that talk about the ‘Internet of Things’ would at least understand how ‘the Internet’ works, for example, how they are connected to ‘the Internet’ (at different moments in time and at different locations).
- ‘The Internet’ does not exists: there does exist a concatenation of interconnected inter- and intra-nets.
- ‘The Internet of People’ does not exist: it is software clients running on machines (smart phones, tablets, computers, etc.) that represent the people in ‘the Internet’: ‘the Internet’ is, and has always been, fundamentally, ‘machine to machine’.
- To understand the integration of IoT in a companies’ business processes, at least some understanding of Industry/ie4.0, ESB (Enterprise Service Buss) and ERP (Enterprise Resource Planning) systems would be a requisite.
- IoT is more, much more than Wi-Fi, Bluetooth, Lora, . . . ; it will have to use a large variety of telecom infrastructure, from general purpose 2nd, 3rd, 4th and 5th generation mobile services, over specialised IoT telecom services, to satellite communications.
- One could probably make an APP to check with the camera of a mobile phone whether boiling potatoes are cooked. It seems unlikely that many persons would use such an APP, because people don’t like to take the risk of eating uncooked or overcooked potatoes. However, ‘health’ sensors that measure about as good as this Boiled Potato App are in common use. Is well prepared food more important than health, maybe?
- Who invented the IoT concept? The name appears to come from General Electric. But it would be fair to give at least some of the credit to NTT DoCoMo:  in the early days of 3G discussions, NTT DoCoMo predicted that more than 50 % of the SIM cards / subscribers to its mobile services would be 'machines' like intelligent fridges.

## What is IoT

- Possible IoT definitions
  - A definition, differentiating between IoT and IoS
    «The Internet of Things is the combination of
    devices centred around sensors, actuators, presence and positioning, distributed computer power, wired and wireless communication on the hardware side, and
    data collection/warehousing, applications and data analytics on the software side.
    It constitutes a major enabler for the use of data mining, and, predictive analytics and other big data techniques»
    (Modified, derived from a Morgan Stanley Research definition).
  - A simpler alternative definition:
    «The Internet of Things is about making devices communicate that before would not be connected / connectable; it may use 'the internet' as a useful infrastructure"

- IoT is about bringing in other and different categories of 'machines' into 'the Internet'. Then the first thing to do is to define where these categories are different, and try to classify them accordingly, e.g. based on:
  - Functionality
  - Behaviour
  - Communication needs
  - Etc.

- IoT will likely use 'the Internet' and an IP (Internet protocol) stack, but where possible, and in an appropriate, adapted way.

- IoT and IoS
  It is convenient to keep the 'old' distinction between IoT and IoS, as it concerns two different market aspects:
  - IoT-Infrastructure or IoT in restricted sense,
    and
  - IoT-Services or IoS

  However, in the following we will use 'IoT' for the combination of IoT infrastructure and IoT services.

- Wireless communications give an extra degree of freedom, but is not required, and sometimes even unwanted (interference, security, etc.)

- The first generation IoT was considered to be based on Radio Frequency Identification (RFID). RFIDs seem to have been almost forgotten, and with that, the importance of identification and localisation, in addition to sensing, collecting data and actuation.

- In sensing and actuating, 'Things' are not only IoT nodes. Similarly, using doctors as contact point for health, one would expect doctors to report about patients' health, not only about their own health. So, the 'Things' are around the IoT node 'Things', so 'Other Things': one could say, the 'Internet of the Other Things'!

**IoT technical challenges**

- A clear distinction is to be made between measuring and making smart estimates:
    - Smart estimates may not be a reliable or accurately alternative for measurement (e.g. energy measurement versus 'steps' in wearables, estimating the number of cars and passengers by looking at the number of mobile devices within the range of base stations covering a section of a motorway).
    - However, when measurement is difficult or not possible, smart estimates may be an acceptable alternative (e.g. flow of water in a river).
- The complexity of sensing and actuation / control are often underestimated: measuring and sensing, and actuation and control are sciences by themselves.
- Not all sensors are small and simple; the challenge is therefore also to find alternative, indirect means of measuring that result in measurement systems that are smaller and more suited for integration.
- Actuators may not be small and simple, and an indirect actuation may be required, e.g. low power electric steering higher power electric or electro-hydraulic actuation.
- Virtualisation of sensors and actuators may be a valuable tool simplifying introduction of new sensors and actuators, but oversimplification will lead to unsuitable and even dangerous usage situations and unsatisfactory performance.
- IoT platforms need therefore to be sufficiently aware of and represent actuators, sensor system characteristics and limitations, and applicable measurement and control algorithms; an important challenge for sensor nodes is therefore to have sufficient access to the development of matching function in gateways, 'platforms' and generic applications

**IoT issues and barriers**

The main IoT and IoS barriers are:

- Data access and ownership management, including privacy
    - Who owns the data, in particular data collected about others' things?
    - How is transfer of ownership and transfer of access right managed?
- Security
    - protection against unauthorised access (hacking)
    - protection against false data introduction (hacking)
    - protection against blocking access etc.
- The cost of developing and deploying infrastructure, including specialised sensing and actuation nodes
- The time necessary for the deployment of IoT infrastructure

**Data access and ownership management**

- Required is access and data ownership management
    - Access control and Privacy
    - Security
- The owner or operator of the sensor is implicitly the owner of the data generated
    - Example: the owner or operator of a car owns the data generated, the dealership should have the owner's permission to access the data for a specific purpose
    - Example: elevator in multi-tenant building (ownership and access agreements)

**An IoT and IoS market assessment**

- The IoT and IoS market cannot be more than a percentage of the cost savings that it helps to bring about, therefore only a few percent of the value of the markets to which IoT is applied as a tool

- Rate of development and economic lifetime of equipment
    - The developing IoT market is wrongly associated with smart phones and the related Google services markets.
    - Instead, it should be compared with the telecom market: developing slower due to deployment and roll-out delays, and with significant longer economic lifetime of the equipment, in the networks, at private company premises and even at consumer premises.

- IoT communications infrastructure and equipment market assessment
    - Communications infrastructure market:
        - extension of capacity of existing and developing general purpose communications infrastructure
        - roll-out of dedicated IoT communications infrastructure (e.g. LORA, etc.)
    - IoT equipment market assessment
        - Consumer market: high volume medium consumer value, low IoT content value
        - General purpose equipment: medium volume, low to medium IoT value
        - Specialised IoT measurement and actuation equipment: low volume medium to high value
    - IoT services market
        - Consumer market:
            - Risks to be tools for publishing / publicity, but by itself not profitable (Google model)
        - Tools and related services market:
            - Medium size market for tools and related services, addressing mainly bigger organisations as customers
        - Services market:
            - Services for small companies, either customised and expensive, or affordable 'standard', reusable services

- It has to be concluded that, in spite of possibly large numbers of connected devices (estimated at 250 Billion by 2020),

  - the market volume for both equipment and services will be much smaller than expected by a number of market studies
  - the market will develop slower, so that the market volume per year will be significantly lower than some expectations

- The 'Google business model' may not work in IoT: whereas in 'the Internet of People' users give away data, even sensitive data, in return for access to some (useful) services, in an IoT environment access to data will be restricted:
  - An important additional sensing and communications infrastructure is a prerequisite
  - Access to collected data will likely be restricted by owners, e.g. companies, for reason of security, privacy, or for protecting the collected data because of its commercial value.

  With that, also the application of Big Data principles may be constrained as in addition to fully owned data, only some data will be available publicly, while access to other data risks to be at a cost and/or conditional.

IoT and possible roles for the Government

- Fostering and advancement
    - It would make sense for local, state and federal governments to foster development of equipment and infrastructure for those applications where:
        - The usage would constitute a significant benefit for society,
        - While market functioning may not be sufficient
- Regulatory
    - The regulatory model can be based on three components:
        - Telecom regulation for the communications infrastructure
        - Surveillance cameras with view on public or others' property
        - And, the new component, non-imaging devices collecting data (also) from public or others' property
    - Needed is a set of rules concerning the ownership of data.
        - Whereas for many cases the owner of the equipment generating measurement data would implicitly be the owner of the data,
        - Exemptions may be in the medical and labour professional domains, where generally the preference should go to ownership for the human being on which the data is generated
    - Needed is a classification of privacy compromise and intrusion risks
        - Identifiable person
        - Traceability to person
        - Privacy intrusion seriousness level
    - Needed is also analysis of the additional risks:
        - False information to the public
        - Hacking, blocking, destroying information