



## What is the Real Business Case for the 'Internet of Things'?

■ **Just under ten years ago** Massachusetts Institute of Technology (MIT), working on a project with EAN.UCC coined the phrase the "Internet of Things". The project developed and 'EPCGlobal' emerged, promoting Radio Frequency Identification (RFID) technology based solutions that were 'set to revolutionise the supply chain'. It was predicted that RFID tagged items and the 'Internet of Things' would be ubiquitous by 2005. Yet here we are approaching 2009, and still waiting for something to happen. Why are we still waiting, and what is the real business case behind the 'Internet of Things'? ■

Bob Williams, FCMA  
CSI, Group Senior Consultant  
Email: bw\_csi@fastmail.fm  
www.2-csi.com

### 1 INTRODUCTION

Just under ten years ago Massachusetts Institute of Technology (MIT), working on a project with EAN.UCC- the article numbering organisations, coined the phrase the "Internet of Things". The project developed and 'EPCGlobal' emerged, promoting Radio Frequency Identification (RFID) technology based solutions that were 'set to revolutionise the supply chain'. The adoption of this technology and approach would "drive 10% of cost out of the supply chain" and radically affect our capabilities to interact with everyday objects in our home. We would be able to find out what was left in the fridge while we were in the supermarket, products would warn us when they went out of date, products would protect themselves against shoplifting, and we could avoid check-out queues at the supermarket. With such powerful business cases it was predicted that RFID tagged items and the 'Internet of Things' would be ubiquitous by 2005. Yet here we are approaching 2009, and still waiting for something to happen. Why are we still waiting, and what is the real business case behind the 'Internet of Things'?

The socio-economic aspects - health and safety, the environment, lawful interception, privacy, security, access to and inclusivity of the technology, the role of government, etc., will all affect the take up of the 'Internet of Things', but there is one overriding issue that will have more impact on the future of the 'Internet of Things' and RFID than any other- the business case. **Without a business case, there is no business!**

Debate about the 'Internet of Things' is generally centred around when the technology will become ubiquitous and pervasive, rather than *if* the technology will become pervasive and what the *extent* of its penetration will be and what technologies are at its core. This article applies some business case logic to the discussion, and as a consequence

challenges some of the fundamental assumptions behind the 'Internet of Things' and concludes that the architecture of the 'Internet of Things' will be different and more limited than some of the assumptions being made, and the architecture will reflect a more structured, yet more viable, pyramid of communications abilities and options, than a single tier world of devices chatting with each other using RFID devices.

## 2 THE 'INTERNET OF THINGS' CONCEPT

The 1999 papers from MIT, available for many years on their website, considered what MIT called the 'Internet of Things' as *"The vision of the Auto-ID Center is to create a universal environment in which computers understand the world without help from human beings"*. McFarlane explains in these papers his concept of MIT-Auto-ID Based Control.

*"An intelligent product is a physical and information based representation of an item for retail which:*

- 1) Possesses a unique identification;*
- 2) Is capable of communicating effectively with its environment;*
- 3) Can retain or store data about itself;*
- 4) Deploys a language which can articulate its features, production, usage, disposal requirements, etc.; and*
- 5) Is capable of participating in or making decisions relevant to its own destiny on a continuous basis."*

It is important to note that the MIT studies were very supply chain focused, the statement *"every item will be tagged"* should not be taken too literally to mean *"everything"* will be tagged. McFarlane was very clear - *"information based representation of an item for retail"*. The mole in the garden, the robin in the tree, and the trees in the Amazon rainforest were never in the assumption *"every item"*. Yet their (sensible) exclusions mean that the original concept of the 'Internet of Things' has always had clear, but very artificial, boundaries. It only applied to things that pass through the supply chain.

Yet as EPC Global and the RFID industry have pursued this opportunity, this limitation is somehow missed, yet the limitation fundamentally affects the scope and impact of the 'Internet of Things'. It has a significant impact on the practicability of the concept described as *"a universal environment in which computers understand the world without help from human beings"* because it presupposes that every item was at one time a retail item, and we know that this is not, and never will be, the case. It is time to re-evaluate and reshape some of these concepts based on what is likely to be realised.

In order for all or any of the possibilities of the 'Internet of Things' to come about, there must be investment, in many cases very serious investment. And investment will only be made if there is an adequate business case. And this is what has been lacking to date.

## 3 THE BUSINESS CASE ASSUMPTIONS

It is important to take into account that the 'Internet of Things' is a concept invented by academics, and not a response to any expressed market need.

That said, the 'Internet of Things' is a truly perceptive disruptive concept that can have major impact on society and business. However it is critically important that, if it is to succeed, it must be built on solid business cases, not on the hype of *"because we can"* or the share price movement of its participating actors.

The whole 'Internet of Things' concept has, to date been posited on the capabilities and limitation of the technology identified as the enabling technology to enable the 'Internet of Things' to be possible - RFID.

In the past the single dimension Bar Code has made a significant contribution to the supply chain and other business models such as asset management, but is a general identifier and not item specific. 2-D bar codes provide a richer source of data but, once printed, are not up-datable. Radio Frequency Identification (RFID) transponders, NFC mobile phones, location systems using UWB communication, Bluetooth or ZigBee-based wireless sensors, and other ubiquitous computing technologies that permanently collect and process data on their environment, appear to offer real business case advantages.

However, whereas the whole 'Internet of Things' project has developed itself around the use of RFID, it is not the devices per-se, but the continuous and dense stream of real-time data that grants an information system with relevant and real time item specific data that creates an 'Internet of Things' that reflect events in the physical world, and provides the business case(s) for the system and its components and the business will only materialise where the business case works for the *user* market place.

In its initial 'Internet of Things' project in 1999, MIT forecasted the ubiquitous use of RFID tags for the 'Internet of Things' by 2005. It forecasted a completed tag price of \$US 0.05 by 2006. OK, so academics are always optimistic in respect of time-scales, but some of the basic economics of the forecasts just never did make any sense.

MIT may with some justification counter that the tag today is more complex than that which they postulated in their project, but any subsequent additional complexities in the tag design are specifically to user needs, for without this there is no business case benefit for the investment. But the counter is that price will determine the take up point and business justification, and will therefore limit the penetration.

In the event no purchaser was able to demand the volumes of tags that would obtain the prices forecasted by MIT, so the business case for the user doesn't work at prices at which tags could be obtained.

The 'Internet of Things' described by MIT, based on ubiquitous use of tags in supermarkets, is predicated on all retail items being tagged, and all home and business items being RFID tagged and able to communicate, at least when interrogated.

As Williams pointed out back in 2003 in "The Future of Automatic Product Identification", with many grocery retail products on sale at under \$0.50, an RFID tag, whether it costs US\$0.28 or US\$0.05, is a significant cost burden and with profit margins usually below 10%, there is no demonstrable business case that can justify the cost of the use of RFID tags at this pricing level and in these circumstances. Not now, not ever.

And if you compare the tag price fall predicted by MIT (in order to achieve market penetration) against the volume growth predicted by them, the total business value hardly grew for many years, so tag vendors would earn only a little more for investing heavily, taking the risks, and selling billions of tags rather than a selling few million at current prices, without any substantial increase in actual profit. This business model also did not stack up, never would stack up, for the RFID tag manufacturers, so again, the move of tag price to an inconsequential level is not going to happen, certainly not in the lifespan of current business model project justifications.

The industry predicts that polymer RFID tags may change all this in a decade. But you don't write a business case for today based on possibilities in ten years time. And the consequences of these economic facts on the shape and potential of the 'Internet of Things' is significant. It means that an RFID tag on every item is a pipedream that will never come to reality. (There, I have said it, the emperor has no clothes!)

So do we throw away the concept of the 'Internet of Things' as a flawed concept? I hope not. For although there have been some weaknesses in the concepts and architectures proposed, the many potential benefits remain significant.

#### 4 THE 'INTERNET OF THINGS' IS NOT JUST ABOUT RFID

This is so fundamental that it shapes the viable architectures for the 'Internet of Things' for the foreseeable future. The idea that the 'Internet of Things' can happen because RFID tagging will become ubiquitous for every item, just does not stand the business case test.

At this stage we have to challenge some of the basic assumptions made for the 'Internet of Things'. McFarlane's tenets of the 'Internet of Things' need to be challenged - and on at least two counts they fail the business case test.

Firstly, the declared objective "*to create a universal environment in which computers understand the world without help from human beings*" does not state a business case reason why this is desirable. And we have to ask the question, what is the business case justification for this? Just because it is technically possible doesn't make it any more sensible or desirable.

The only reason that can be linked to a viable business case is, as stated above, not the devices per-se, but the continuous and dense stream of real-time data that grants an information system relevant and real time item specific data that creates an 'Internet of Things (IoT)'. So we have to be clear that the business case for the 'Internet of Things' is not in the business case for RFID devices, but is the business case justification for having access to that information, and that RFID systems are just one way of providing that information in circumstances where that technology is the most appropriate and cost effective.

The second count where the early conceptualisation fails the business case test is in McFarlane's five characteristics of an intelligent product. These are about unique identification, communicating with its environment, storing data, using standard language and "*is capable of participating in or making decisions relevant to its own destiny on a continuous basis*".

This last point is the reason for providing intelligence in the device - the other points can be met from a passive data store, so long as it is accessible.

If you accept that, in many cases, communicating effectively with its environment may simply mean making the identification and data available to be interrogated, this can be achieved from a passive data store. And indeed the RFID technology espoused in all of the early 'Internet of Things' thinking is a passive RFID tag that will only yield its data on interrogation, so its only difference from a bar code is in the conditions that the data is accessed and that data on an IC memory can be updated, and not that it is 'capable of making decisions relevant to its own destiny'. So here not only is the business case unclear, but the logic of the original concept is flawed. If we think this through,

it is clear that some items will need to communicate while others need only to be interrogatable, and that some data is permanent, and other data variable.

The issue of a unique identity, which is fundamental to some of the 'Internet of Things' thinking, also needs to be challenged on business case grounds. For many years barcodes have successfully provided a generic identity, but not an individual identity. There are good reasons to extend this to group identity, for example to identify the sell by date for a batch of goods. But this is not always required and if not required and if it involves cost has no business case justification. In some cases there is a real reason for a unique identity when there is a unique aspect to an item such as its weight, its history etc. But where is the business case to extend this to every item? Unambiguous identification may be adequate in many cases.

The consequence is that many aspects of the 'Internet of Things' can be achieved with less expensive technology, indeed often with technology, such as bar code, that is already widely deployed.

**The result is that the business case justifiable 'Internet of Things' will be a 'pyramid', a structured hierarchy of identity, data stores and capabilities, based on need, as justified by, and limited by, the business case.**

The first consequence is that the information on many items will continue to be held in a bar code. Currently bar code identification only identifies type (e.g. 450 gramme tin of baked beans by producer X). If a bar code is to be individual, it will have to be sprayed onto the products individually and not, as at present, art-worked into the product packaging. These areas and the associated business case (or lack thereof) need to be quantified and developed if such items are to be included in the 'Internet of Things' and must justify the investment.

There *are* good business case justifications for the use of RFID technology at an item level. Marks and Spencer, for example, use the technology to reduce fraud of returned goods under warranty, where the higher price of the products justifies the business case. Razor blades with combined anti-theft EAS/RFID tags provide another example of where a business case can be justified. The business case for sell by date information, where this is crucial information, as in fresh foods, provide a new market opportunity in the 'Internet of Things' world, both for the retailer in stocking his shelves and potentially for the end user in the home or office, additionally creating markets for new product features, enabling pressure on the user to restock, and providing refrigerator manufacturers with sales marketing and advertising advantage. In this world, marketing may also have a viable business case to absorb/cost justify the use of RFID tags, for example a vendor of wine or packs of beer may be prepared to absorb the cost of a tag for the opportunity to better close a sale. However these cases have to be made. Where they can be made they will extend the reach of the 'Internet of Things'.

## 5 WHAT THEN WILL THE 'INTERNET OF THINGS' COMPRISE?

If you follow and accept the logic of the argument so far, then the extension to the logic is that only things that *need* to communicate will be equipped to communicate. Towards the top of the 'pyramid' described above, this will be with fully interactive peer to peer machine communications (for example my PDA to your computer), with RFID tags filling the voids where investment in peer to peer equipment cannot be cost justified, because RFID tags provide the least cost means to satisfy this need, and passive data stores (such as bar code) will provide data and identification below this level, and much of the world will still remain 'unidentified' and 'unidentifiable'.

Another feature that we can define about the 'Internet of Things' as it is likely to be realised, and a consequence directly at variance with McFarlanes concept that an item is '*capable of participating in or making decisions relevant to its own destiny on a continuous basis*' is that **Communications will only happen on the direct or indirect instruction of a sentient item (at the top of the pyramid) or on the instruction of an intelligent item (layer 2)**, and even at layer 2, the control of the intelligent item is normally controlled or predetermined by a sentient item (in the 'Internet of Things', all things, including humans, are 'items'), because only these upper levels can make decisions about justifying the business case.

The 'Internet of Things', then, relies on a case to case basis, where the cost is considered (by a sentient being) an acceptable price to satisfy a requirement or desire, and the 'Internet of Things' is shaped (and limited) by these business cases.

This business case based concept of the 'Internet of Things' will not only rely on RFID tags or smart labels or smart cards. Where it is only necessary to collect static information (such as item identification, weight, sell by date, source etc.), bar codes, probably 2D bar codes, can be used to obtain the data, and the technology of mobile and nomadic devices are moving to enable functionality to read bar codes.

Rather than equip every *item* to communicate actively when interrogated, we will improve the ability of the *readers* to scan passive information such as bar codes, because the business case is stronger. Many of us are already used to self scanning supermarket checkouts, and many mobile phones can now read bar codes. So while the concept of a refrigerator that can automatically interrogate the electronic RFID labels in the fridge (that also provided data for the supermarket stock management and checkout) is very attractive, there are other, less expensive, ways to achieve the same end.

Much of the 'Internet of Things' could be achieved in this respect by manually barcode scanning, for example, the goods into the refrigerator, perhaps by a scanner set into the screen on the refrigerator. That way the 'sell by' date could be recorded in the same way and alerts given via the screen. If the information at the supermarket checkout also collected sell by dates, using even today's WiFi technology, that information could be transferred to my PDA and telephoned to my refrigerator or home computer, and also apply to purchased items that are throughout the home, but not necessarily in the refrigerator or freezer.

Consider the effect on the shape of these conclusions on the architecture and capabilities of the 'Internet of Things'. It will not be a peer to peer based world with all items connected, but a world of items where some are RFID tagged, some items are bar code tagged, some items have the ability to interrogate, and some items will remain unconnected.

The 'Internet of Things' is more about what we do with information that is available than it is dependent on RFID Tags. RFID tags will play their part, that is sure, but they are only a part of the 'Internet of Things'. And in describing the architecture of the 'Internet of Things', we also need to be a little more sophisticated than simply 'item' identification of every item. We have several classes of item, which form the previously described hierarchical pyramid, and the technology used to obtain information from or send information to that class of item will differ. The classes may be for example:

Class A : Items with generic permanent static data (e.g. tin of tomatoes)

Class B : Items with group static data (e.g. lettuce with sell by date)

- Class C : Items with unique permanent static data (e.g. cut of meat with specific unique weight, source and sell by date)
- Class D : Item with variable generic static data (e.g. generically identified pack of frozen goods with a temperature sensor)
- Class E : Item with variable group static data (e.g. pallet of cartons of items)
- Class F : Item with generic transient static data (e.g. load on a truck trailer)
- Class G : Item with variable unique static data (toll tag; uniquely identified item with temperature sensor)
- Class H : Item with group variable data (e.g. vehicle)
- Class I : Item with unique variable data (e.g. refrigerator, music centre, central heating, house alarm, vehicle etc.)
- Class J : Intelligent item (e.g. computer, PDA)
- Class K : Sentient item (e.g. human)

These classes are arbitrary and proposed for the purposes of this article rather than a formal classification. Figure 1 shows some pictorial views of this 'Internet of Things' pyramid.

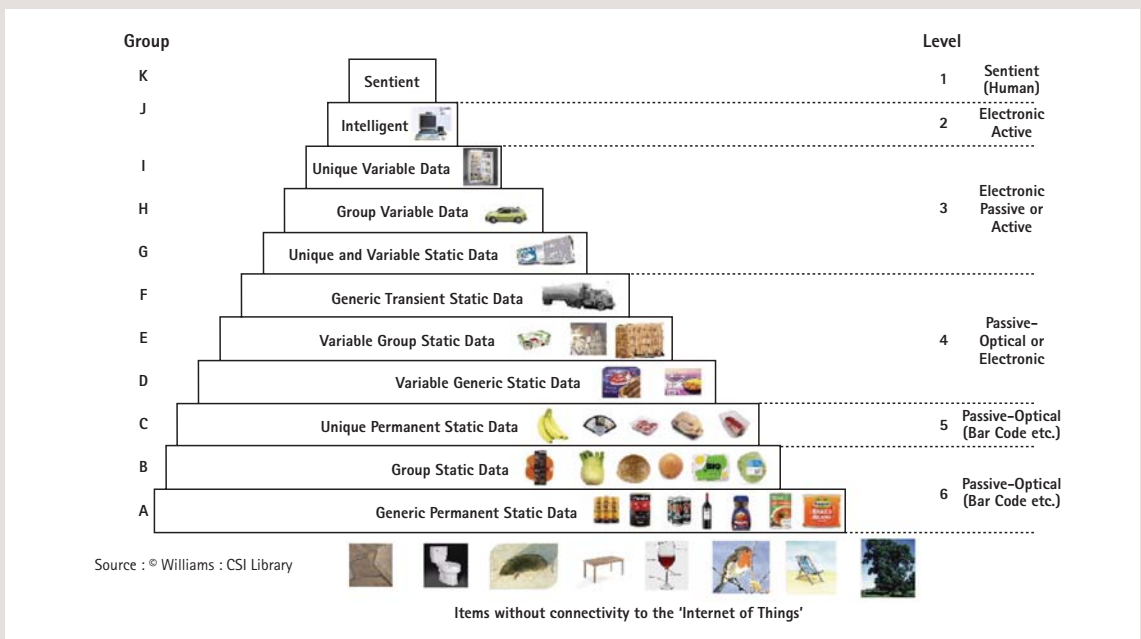


Figure 1: A profile view of the IoT Pyramid

In the figure we see a view of the world (as a pyramid) where there is no attempt to identify every item. Most of the items in the world - the tree in the field, the deckchair on the beach, the robin in the tree, etc., simply have no need to communicate via the 'Internet of Things' - so they won't. **In reality, the consequence is that, for the foreseeable future, most of the items in the world will not be connected.** We could, in the 'Internet of Things' world, call this the '*unidentified/unidentifiable*' class of items.

As we move up the pyramid, the next layers in the 'Internet of Things' pyramid are those that have the capability to be identified, but are passive, they can be identified if interrogated, but have no power to initiate a communication session. Groups B, C, D will normally be identified by a bar code, in the case of b) simply as a generic identification

of an item such as a tin of tomatoes, in the case of c) an item such as a lettuce where there are many instances with the same identification and a group of them with the same sell by date. In the case of Group D, the items are individual, not generic, because, for example, each has a different weight. In the world of the 'Internet of Things', we could call this the '*Passively identifiable*' class of items. That additional information may not be unique as there may be multiple instances of items of the same weight. Where RFID tags are used they will be passive tags.

There is a fundamental difference between data which is variable but passive (as in the example of a kilogramme of sausages used in Class D) and data from a sensor, which may also be passive and only respond when interrogated, but in some cases may also initiate a communication session if some parameter (e.g. temperature) strays outside of defined limits – We could call this class (Class E in the figures) something like '*Communications instigation capable items*'. (Of course this would only occur where there is a justifiable business case).

Groups D and G represent situations where bundled information is available about items, in Group D generically identifiable items, in Group G uniquely identifiable items. These may be, for example, 'toll tags' that identify the ingress and egress points of a vehicle journey. Both of these groups are unlikely to instigate a communication session and are more likely to respond to an interrogation, but neither possibility can be ruled out. We could call this group '*Items carrying data about other items*'.

By the time we get to Group H we are talking about items that will have not only some unique identification but unique addressing capability, can instigate a communications session or respond to an interrogation, and may handle large amounts of transient variable data. An intelligent car would be a good example. We could call this group '*Items effecting services for other items*'.

At the top of the pyramid we have truly intelligent devices such as computers or sentient items (such as people) who have the power to instigate communications sessions and interrogate items. The principle difference between 'intelligent items' and 'sentient items' is that the operating decisions made by 'intelligent items' are normally established by, under the control of, or their behaviour has been set up by, sentient items (such as humans). So at the top of the 'Internet of Things' pyramid we can always expect a sentient being in control, and **not** items that are "capable of participating in or making decisions relevant to their own destiny". This is a fundamental development away from the original MIT concepts. And the reason for this is that only with this hierarchy can business case decisions be justified and their investment obtained.

We could, of course make different classification groups and classes, but that is not the point. The point is that the 'Internet of Things' is not, and never will be, a network of peer self actualising items (using RFID), but will comprise a hierarchy of classes of items of different characteristics and capabilities; the nature of which is determined by the business case for their existence, and the technology utilised will be justifiable by the business case (and will only sometimes use RFID).

The business case for the use of RFID in the 'Internet of Things' is therefore structured in multiple classes, justified by the economics of their business cases, and they will not be designed to have features or behaviour other than that justified by their business case (although there may be additional downstream benefits, and benefits discovered at a later date but not part of the original business case), and their capabilities will be only those justifiable by their individual business cases. There will be no killer business case justification, per se, for the 'Internet of Things', and many items in the world will remain outside of the 'Internet of Things'.

## 6 CONCLUSION

To realise the potential of the concept of the 'Internet of Things', attention needs to be focussed on new, Internet type, manipulation of the available data, and in this respect the data carrier technology, though important because of its limitations, becomes a secondary consideration. Rules need to be developed for interactions between these classes of items, and web services need to be developed to enable these data collections/exchanges/transactions. It is this area of standards for data management, transfer and manipulation (rather than any particular air interface) where most attention should now be focussed if the 'Internet of Things' is to happen.

To summarise, while RFID has an important role in the 'Internet of Things', it is only one data carrier technology that will be used to achieve the 'Internet of Things', and while the commercial market place will develop the products (software systems) that make the internet things work, more attention needs to be focussed on the generic building block 'web services' that enable the 'Internet of Things' to function interoperably. Standardised web services are required and the Standards Development Organisations (CEN, ISO, ETSI) would have an important role to play here.

## 7 ABOUT THE AUTHOR

Bob Williams has been an independent consultant in Automatic Identification and Intelligent Transport Systems for more than 25 years. He was the Editor for some of the ISO Standards for RFID and continues to monitor developments in standardisation for RFID and the 'Internet of Things'. He is the author of 'Understanding Bar Coding' (PIRA), 'Automatic Identification' (PIRA) and 'The Future of Automatic Product Identification' (PIRA).