Haire, Andrew J.

Conference Paper

What makes IoT different for the regulatory authority

2015 Regional Conference of the International Telecommunications Society (ITS): "The Intelligent World: Realizing Hopes, Overcoming Challenges", Los Angeles, USA, 25th-28th October, 2015

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Haire, Andrew J. (2015) : What makes IoT different for the regulatory authority, 2015 Regional Conference of the International Telecommunications Society (ITS): "The Intelligent World: Realizing Hopes, Overcoming Challenges", Los Angeles, USA, 25th-28th October, 2015, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/146343

Author: Andrew J. Haire

Introduction. As has been laid out carefully in prior writings, IoT, or its subset M2M or its superset IoE, is underpinned by the evolution of cheap communication, cheaper storage and computing, and more sophisticated analytics. Much has been written about 'solutions', 'architecture', 'interoperability', but not that much within the public policy conversation. Are marketplace rules necessary; what might shape them; what should they accomplish? But make no mistake, that even in the face of migration towards a more liberalized communications markets worldwide, that sector remains regulated, and we must be wary that rule makers may arrive, and may slow innovation's progress.

This paper intends to surface the public policy issues related to moving to an 'Intelligent World'. The authorities or governmental bodies with a say in 'what can', 'what can't', 'what should be' is grows each day. We have telecom regulators, competition authorities, and privacy commissions – each with a continuing sense that they must do something meaningful to justify their existence. [I take liberty to say this, as one who served as a regulator for over a decade in an Asian economy.] Twenty years ago only 14 countries in the world could claim that they regulated their communications market; today that number is over 200. Rules abound. Each creates regulations or sets policy; often by people who at time have difficulty understanding the technical nuances surrounding a technology driven marketplace.

But there is a new factor that IoT market's stakeholders must consider. No longer is one regulator the only authority 'in town', many are. The new world is now filled with interested, empowered and committed 'overseers'; policy setting has now become multi-stakeholder, usually without coordination or harmonization, and not bound by geography, economic sector, political ideology, or even technology.

The hope herein is to develop this conversation with a closer look at the regulatory and public policy issues surrounding the emerging Internet of Things (IoT). There has been much written on the differences between M2M (Machine to Machine) and IoT or even IoE (Internet of Everything). But for the sake of this discussion, the discussion will 'stick' to a single acronym, IoT, each of the others will be treated as within that universe, and policy topics considered below will address each and all together. For simplicity, reference will be to the IoT – and will make distinctions only when M2M or IoE demand such a policy distinction. For those seeking a more precise distinction, references exits[1], but this paper will keep to a broader view.

Further, this paper takes on a narrow purpose, but will be drawn from the lens of an Authority's mandate. Parenthetically, "Authority" is used loosely: it means anyone or any organization in a position to impose rules or laws impacting marketplace behavior – generally parts of governments such as legislatures, competition authorities or sector regulators hold that mandate. The main objective of what will be covered it to discuss policy issues that could become part of their thinking – a departure from typical articles whose focus tends toward interoperability or devices or applications or solutions.

[1] Polsonetti, C, *Know the Difference Between IoT and M2M*, 2nd ¶, Automation World, 15 Jul 2014, visited September 2015

Why is any of this this important? The communications sector remains regulated, and the societal reach of IoT demands deeper safeguards. The Authority will have an effect on the IoT's future.

The characteristics. Broadly how would IoT be characterized; what are its features? When the EU regulatory authority, DG Connect, painted this policy picture a few years back, their whitepaper[2] believed that the IoT characteristics were: ubiquity, miniaturization (even to the point of being invisible); ambiguity (it's not rational); identification (individuals and things are getting tagged, and this information is not easily forgotten); connectivity (given overall ease and efficiency to pass information); imbedded intelligence (and rapidly growing); seamless information flow (sometimes absent the context it was collected); distributed control (there is no managing center, just edges). Considering all of these together, this communications policy paradigm is radically different from anything an 'Authority' has previously seen.

What sets this apart? What places IoT policy apart from earlier ICT policy initiatives, what makes it different? And if so, why might this show up on any Authorities' doorstep: five characteristics, granted not comprehensive, are offered:

1 **Nature of the communication** In IoT architecture we have objects (sensors; devices; analytics; intelligence; etc.) These objects grow opaque – both in what they collect and how the information collected is used. Further, the architecture permits people controlling objects; objects controlling people; objects controlling other objects. Direct 'people' control is waning; objects fill this gap, then assume greater control by bringing forward habits called *the incompetence trap*[3]. A second trap may surface: people who increasingly fail to use their skills may think they are more qualitied than they actually are and fail to see their own inadequacy[4]. All of this raises a serious question of responsibility and accountability, and eventually leads to a possible overreliance on technology.

   A tragic example surfaced during Air France flight 447 in 2009[5], (pilots relied on 'fly by wire' so much that as this particular crisis unfolded, they were ill trained and thus incapable to cope; the plane crashed into the sea, bringing with it its passengers and crew). Only later did we see a reconsideration of management behavior toward automation[6]. The notion of 'de-skilling' is well documented[7], but raises a deep concern that highly skilled worker gives way to automation operated by the semi-skilled – skill fades over time, cost savings are gained but at the expense of quality.

2 **Risks for profiling** Data, especially given the ease of post-collection correlation, leads to profiling, and profiling results in discrimination, some good, but some bad. This may drive discriminatory commercial behaviors, which has a history of driving societal exclusion. Governments now do have a need to worry.

3 **Intrusion on civil society** The very pervasiveness of IoT, both present and foreseen, leads to societal divides – between those who understand and those who are possibly intimidated by the technology. It might also lead to false trust of that technology. Objects encompass an

---

[2] Van den Hoven, Jeroen, 2012, EU DG Connect; Ethics subgroup IoT – Version 4.0; p.4
[3] Crabb, Peter B; June 2010; International Journal of Technoethics, p19
[4] Lee, C, *Revisiting why incompetents think they're awesome*, arstechnica.com, visited Sept 2015
[5] Langewiesche, W., *The Human Factor*, Vanity Fair October 2014
[6] BestRid.com Blog; *What the Airline Industry Learned about Automation…*, 7Oct14
[7] Lerner, S,Univ of Waterloo, Waterloo, Ontario, Canada; *The Future of Work in North America*, Futures, March 1994
Agnew, A, et al, *Deskilling and reskilling within the labour process: The case of computer integrated manufacturing*, Int J Prodction Economics 52 (1997) p 317-324

ever growing part of daily lives – and thus a malfunction or error has an ever growing impact on society. Simply, we have seen two eras that ushered in social exclusion with the advent of the communications (mostly with the telephone and the mobile phone) and later with the advent of the internet. With the IoT we are witnessing the third divide – those who can utilize information from this platform and those who can't.

4 **Diffused control** IoT architecture by its very nature is not controlled from the center but from the edge. But under such diffusion, who becomes accountable, and thus liable, for that errant sensor collecting data, that weak credential check allowing unauthorized access, that data point taken out of context, passed on or sold, and then not adequately protecting future actions? A second issue arises: diffused networks inevitably lead to cross border data flows. Such flows, especially where personal information is involved raise serious privacy concerns among Authorities.

5 **Legal norms are no longer norms** Adequate notice, usually the pillar of consent, is leading to 'consent fatigue'[8]; people agree to sharing data and have no idea what they are agreeing to. Permissions are lengthy, and possibly deliberately confusing. Additionally the user in the 'world of IoT' will not have complete or relevant knowledge that information being collected was part of this consent. If the 'ordinary user' doesn't have time to understand, then who will protect the societally unprotected – those with special needs, such as children, those with disabilities and the elderly. Additionally gaining consent can be manipulated in such a way that often individuals grant permission when with better understanding they might not have[9].
A distressing test in London in 2014 proved this point[10]. Users were offered free WiFi at various points around the city, but only as long as they agreed to terms, one which included assigning their first born child for the duration of eternity. Six agreed.

Taken together the Authority has ample justification to become involved; but how?

What do they want? In the past an Authority worried about competition, fair play and growth. In a recent speech the head of BEREC – the European regulator's group – focused[11] on historical regulatory issues: 'evolution of internet-driven services that will stimulate the market and […] attention for the foreseeable future'. Allowing this list to expand when we consider what IoT is, will be radically different.

Going forward that expanded list will include societal justice, growing digital divides, trust, and the use of information[12]. And, given that the Authorities arguably hold sway on market outcomes, it should become a shared worry for IoT's developers and architects. A simple example: while it might be rewarding for your automobile to deliver benefits from its on-board technology, it would be less exciting if your car was prohibited across a national border because it doesn't comply with the rules where you are headed, such as individual's privacy or radio spectrum use. It is not enough to just understand rules of play, it is equally important to work with the 'rule-makers' to insure responsible rulemaking continues.

---

[8] Schermer, B, *Your consent is overrated,* Leiden Law Blog – University of Leiden, 11Apr13
[9] Adjerid, Idris, *Uninformed Consent: The Benefits and Limits of Transparency and Choice in Privacy Decision Making* (2013). Dissertations. Paper 403
[10] Fox-Brewster, T, The Guardian, *Londoners give up eldest children in public Wi-Fi security horror show,* 29 Sept 2014.
[11] BEREC chair speech http://www.contel.hr/2015/fatima-barros/ July 2015
[12] Van den Hoven, Jeroen, EU DG Connect; Ethics subgroup IoT – Version 4.0; P 19

How these elements are viewed?

Of the many policy responsibilities under the view of an Authority, but considering space and time available in this paper, we'll focus on three: protective rights – such as privacy, security, data protection, and include trust; safety – which includes societal risks, national security and public safety; economic opportunity – which includes growth, innovation and anticompetitive conduct.

But there is a fourth worth a strong mention: the traditional and historical role that this regulatory authority has always played. During the EU's work[13] to develop its Digital Agenda it raised six policy challenges related to IoT architecture: identification, privacy and data protection and security, architectures, ethics, standards and governance. Each challenge was addressed by a group of experts; charged with a mission to research then report. Leading up to that, a public consultation was conducted on IoT policy between April and July 2012. In the end the public's comments and expert's findings found their way into evaluations and in some cases, recommendations how to address this new robust opportunity. Their key points have been summarized by this paper, but this author recommends the value of a further review of this material[14].

Protective rights

While often the words 'privacy' and 'data protection' and 'information security' are used interchangeably leading to a blurred understanding, there is a clear difference between them. Very simply, privacy involves sharing only what you want to; data protection is sharing only with who you want to; security is keeping the unwanted away.

We tend to limit *privacy* policy considerations to guarding personally identifiable information (PII). Furthermore, until recently, we mistakenly thought if we protectively suppress the PII elements from data capture, then we protected the individual's identity. Highly sophisticated algorithms in the world of data analytics simply correlate[15] seemingly unrelated data to accurately determine identity[16]. Additionally, while some see opportunity from 'smart living' or 'smart cities' such as managing electricity grids, others see that as intrusive. What if the household meter were sensitive enough, and related analytics smart enough to determine – based on the occupant's moment to moment consumption –what the occupant was presently doing, maybe what food was consumed, what television program was viewed, which rooms were occupied. Incidentally, the upper house of the Dutch parliament shared these same concerns to turn away legislation to exploit IoT in an energy consumption application.

Security on the other hand is to keep unwanted intruders out – of your data and with your devices. If my home's door locks are controlled by automation, my security is only as guarded as the most inept hacker's success. Commercial pressures to produce sensors at the lowest possible cost should not give way to compromising the integrity of the broader system. A 'flash crash' resulting in a quick

---

[13] European Commission, *Europe's policy options for a dynamic and trustworthy development of the Internet of things* 31 May 2013, http://bookshop.europa.eu/en/europe-s-policy-options-for-a-dynamic-and-trustworthy-development-of-the-internet-of-things-pbKK0113297/ reviewed Dec 2014

[14] European Commission, *Conclusions of the Internet of Things public consultation, 2013,* http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation visited Dec 2013

[15] Adam Sadilek, Henry Kautz and Jeffrey Bingham, "Finding Your Friends and Following Them to Where You Are", 5th ACM Conference on Web Search and Data Mining, 2012

[16] MIT Technology Review http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/

'reboot' of firmware – offers false comfort of little to no harm because the object returns to service – BUT should not become the backdoor that the scoundrels with dishonest intentions enter.

Trust and *data protection*: Two elements are tightly interwoven. Delink these at one's peril. Data collected whether intentionally, incidentally, accidentally or inadvertently puts itself under someone's stewardship. Should that data become compromised – as seen in far too many recent headlines – and in any fashion and for any reason – the public's trust in accepting these intrusive IoT systems will be deeply damaged. Trust lost, will be difficult to restore. Jurisdictions worldwide are enacting legislation to make breaches 'painful' for those responsible. Some now realize that such legislation tends to be ill-directed: it focuses on collection, not intended use.

Over the past few years, the World Economic Forum, an international institution committed to improve the state of world through public-private cooperation, has reported[17] some goals about data use. In their work they urge moving:

- **From Transparency to Understanding:** People need to understand how data is being collected, whether with their consent or without – through observations and tracking mechanisms given the low cost of gathering and analyzing data.
- **From Passive Consent to Engaged Individuals:** Too often the organizations collecting and using data see their role as a yes-no / on-off degree of consent. New ways are needed to exercise more choice and control over this data that affects their lives.
- **From Black to White to Shades of Gray:** the context by which data is collected and used matters significantly. How is the data used; much like money, it means little until it is used.

In order to achieve a responsible level of trust during the flow of data, at least five oft-used words frame such flow: protection; accountability; empowerment; transparency and respect. There is an expected responsibility assumed for collecting personal information. Before the dawn of networked data, individual data was generally used once and for a specific purpose. But today, given the role of analytics, and the residual value of data that can be correlated in the future, reuse of data is common, allowing more value to others. Reused data, away from its original context, creates personal privacy risks. Social media and cloud platforms are reported to collect and retain every user keystroke, whether they presently need it or not. Storage and processing is cheap (Moore's Law at work), moving data simplified (programs like Hadoop are mainstream), the value of such information can forever harvested for future gain (look no further than Google, Amazon or Facebook).

When Glenn Greenwald, famous for his reporting of Edward Snowden's revelation in 2013, wrote[18] about a program known as XKeyscore he exposed the extend and depth of collecting everything a user does during internet use. The 'user' in this role could be anyone – worldwide. While this reporting primarily deals with data collection, there is no doubt about the power to perform interpretative and correlative analysis on this data.

In the recent past, especially with the advent of data mining technology, the line between public and private data use has become more opaque, and thus people no longer know if, when or how their personal information is used, or worse, shared. Trust is considered the key challenge for the Future Internet.[19] Trust builds when that 'object' – a term used earlier - performs in a certain and

[17] WEF; Unlocking the Value of Personal Data: From Collection to Usage; http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf
[18] Greenwald, G, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'* The Guardian, 31 July 2013
[19] De Paoli, S, *Toward Trust as Result*. Triple C, tripleC 9(2): 702-714, 2011; ISSN 1726-670X

predictable way and is usually not threatening any expectations of that 'person'. It is important to understand the need for collaboration between disciplines – between the ICT community designing and implementing the IoT platforms and the sociologists who have a sense of how society behaves. Very simply put: we have discussed earlier the person to object (etc., etc.) dynamic. "…failure to enhance trust may result to suspicion and eventual rejection of new technology"[20]. The cost of rejection comes at a high price; to regain that trust might be far more expensive than preventative remedies ever were.

Safety

Stepping past the concept of security just mentioned, and taking into account a far wider view, national security and public safety regarding network design, we learn that access is crucial. Given that forecasts see billions of devices being deployed, some into national infrastructure such as energy generation and distribution, transport infrastructure, agriculture, financial services, we are entering a society that is so reliant on these devices, that their very failure, especially on a massive basis will disrupt society far more than anyone can imagine today. Those with malicious intentions will be capable of disrupting economic wellbeing for an entire region or nation or nations.

Given the growing dependence on IoT devices, and in order to best prepare for the possibility of disruption, the US government has framed a review based on four efforts[21]:

- Security (Trustworthiness, resiliency, user behaviors, public/private partnership)
- Operations (Interoperability of systems, reliability of operations, spectrum prioritization, process coordination)
- Design (Best practices and standards, security-by-design, trust relationships, integration with national security/emergency preparedness programs)
- Policy (Resiliency, privacy, public safety, international considerations)

The intention is to best understand the risks so as to develop approaches for improved security and safety of citizens and protecting those parts of dependent society. Further past practices of developing technology in relative silos starts bluring with IoT. Devices and their roles are intertwined. Traffic signals throughout an entire grid are tied to street and parking sensors; weather forecasts are tied to communication signals.

A significant and growing concern is that devices (or sensors) will age and eventually fail needing replacement. Unlike past technology platforms, the scope of replacement is not measured in thousands of units, but hundreds of millions; such devices are not easily reached or even seen, but disbursed and scattered, and in some cases forgotten. This represents a policy issue because devices of no further interest, should be disposed of with full confidence that they present no further subsequent harm.

Opportunity, economic and societal.

Much has been written about various applications that make our lives easier and more efficient. Let's avoid repeating them; but a small portrait might be useful by bringing in a recent Bloomberg Businessweek article[22] on the 'smartest building' built near Amsterdam, in the Netherlands. This is

[20] Clark, J. Waterford Institute of Technology, *Future Internet: A Matter of Trust*, Nov 2008 eMobility Newsletter, previewed 2012
[21] NSTAC *Report to the President on the Internet of Things*, P4 and P9 2014
[22] Randall, T. *The Smartest Building in the World*, Bloomberg-BusinessWeek, 23 Sept 2015

enlightening because it reinforces the life enhancing, cost avoiding techniques that can be designed into a building, making the worker 'happier', the environment 'greener', and the owners 'thrifty'. This smartness is accomplished through very sophisticated monitoring of light, power consumption, temperature, humidity, motion and other workplace responsibilities – virtual office space, online access, parking, and meetings. The cleverness comes from sensor deployment. Connecting technology (IoT, without directly mentioning it in this reporting) with the individual, and vice versa, is shown to have significant benefits for those just mentioned. Oddly, there was no allusion to how the 2,500 workers in the building might cope, much less get their work done, if the, say, backup electrical power failed or if an unwanted intruder mischievously pierces protective data firewalls to disrupt these well planned flows. Someone once called this phenomenon "Murphy's Law".

IoT growth is inevitable. Given the widespread use of smartphones, with their ever-increasing power, combined with lowering communications costs, networking flexibilities, the ubiquity of sensor's capabilities, and rapid growth in this sector is mostly assured. Innovation will depend as much on our willingness of this intrusiveness to regiment our lives, as on the ingenuity of the designers.

With this economic opportunity brings economic risk: information gathered and harnessed will represent a new form or economic power; some call it the 'new oil'[23], while some have countered that argument[24]. Whether it is or not, the economic reality is here, and the government Authority needs to find that balance between societal and economic gains against citizen welfare. Further, we previously wrote about the rise of the "Data Baron"[25], much in the same way the robber baron arrived over a century ago. Governments are ill-equipped today, as they were then, to come to terms with this economic force. They quickly see the advantages, just like the 'smartest building' was idolized, but remain at some level of denial about the existence of adversities.

Legacy roles of regulators. Regulators in the ICT sector exist and have a role to play. To simplify this somewhat, let's limit the discussion to four purposes. They have a role: (1) as overseer of a scarce public resource; (2) as the proxy competitor in the absence of a real market competitor; (3) to harmonize participation in a market that demands interoperability; (4) to seek orderly competition among competitors that supply themselves vertically, but compete horizontally. There is a difference between (2) and (4), one relates to consumers and the other among competitors. The communications regulator's traditional responsibilities are usually borne by sets by statutes or laws but shaped by decades of prior decisions. As new opportunities arrive, such as the IoT, the Authorities must be decided quickly if existing 'rules' fit. If not, change is needed.

We will consider each of these four roles individually.

---

[23] World Economic Forum session, 9 June 2011, http://www.weforum.org/sessions/summary/personal-data-new-oil-21st-century, visited Sept 2015

[24] Thorp, J. *Big Data is Not the New Oil*, HBR 30 Nov 2012

[25] Haire, A & Mayer-Schönberger, V, *Big Data – Opportunity or Threat, June 2014* www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/Discussion%20papers%20and%20presentations%20-%20GSR14/Session3_GSR14-DiscussionPaper-BigData.pdf

(1) Manage the scarce resource.

When the regulatory authority takes the longer view on the future of IoT devices two critical issues always arrive: how to communicate with and among these devices, and how can each device be uniquely identified. Both present the designer with unwanted boundaries.

The first of these issues factors how the device communicates; via a 'wire' or via 'wireless' – one relies on a physical attached medium and the other uses radio spectrum. Let's address the more problematic of the two. If wireless, where the public's spectrum can be used, there are at least three possible approaches: use the spectrum assigned to an existing licensee, maybe a mobile operator; use unlicensed spectrum, which needs no relationship, but international engineering norms must be followed; use proprietary, fit for purpose spectrum. Paradoxically, for trans-border applications, such as automobile onboard computers, the unlicenced spectrum holds more potential than a relationship using the mobile operator's spectrum rights.

The sheer range of devices and sensors, along with the application diversity in the IoT architecture would indicate that spectrum needs are equally diverse. Some devices send small bits of data, while others transmit hoards; others are time sensitive – or in the somewhat annoying term, "mission critical" – while others can wait. Others may require sending small bits most of the time, but large streams far less frequently when updating the imbedded source program. To categorize or treat them in common leads to inefficiencies. Network design might demand prioritization, which in turn leads to discrimination; some justified some not. Regulators and Authorities worldwide seem to be joining the network neutrality[26] bandwagon in some way

Unlicenced spectrum band, sometimes called the ISM[27] band, is often referred to as 'licence exempt', and is used popularly for cordless phone, children's toys, Bluetooth devices, and WiFi communications, etc. Permission is not needed from a regulator almost globally, just compliance to worldwide transmission specifications. In turn the Authority offers no assurance that the band will be free from harmful interference – the engineering equivalent of *caveat emptor*. This very well is the most suitable band for IoT wireless devices. Euphemistically the band is called the 'public park' or the 'common' – anyone can use it as long as they observe some simple rules. So if we use the ISM device as a parallel, we know that the regulator is mostly concerned about non-interference or with the orderly conduct in this public band. This is accomplished by certifying the device, not the provider. The same should apply for M2M or IoT devices.

Another issue arises for a regulator if a platform choses a technology; say it uses GSM in the mobile spectrum bands from a licenced mobile operator. Should the regulator every want to re-farm or recover that band for a different use, there might be millions of devices, most likely unmanned that have to be found. It is one thing to ask subscribers to return their obsolete phones – maybe through incentives or promotions, it is a completely different matter to locate, recover and replace tens or hundreds of millions of scattered sensors or devices.

In several regulatory proceedings, the UK's in particular[28], several commenters recommended repurposing existing bands assigned to older technology devices to be re-farmed and dedicated to new technology, such as IoT. Of course the downside of adopting this plan and not harmonizing this

[26] https://en.wikipedia.org/wiki/Net_neutrality_law#By_geographic_regions visited August 2015
[27] https://en.wikipedia.org/wiki/ISM_band
[28] OFCOM *Spectrum Management Strategy*, 30 April 2014, http://stakeholders.ofcom.org.uk/consultations/spectrum-management-strategy/statement/

use globally is that the spectrum use becomes 'fit for purpose' – it has a narrow use in one jurisdiction. Understanding the rational that the US government used almost 70 years ago to convince the world to adopt the ISM, or licence exempt, policy was that devices – at the time it was microwave ovens – *might* be used on ships and thus would cross national boundaries. International use demanded international cooperation, and this is often seen as an excellent example of gaining such cooperation.

The second of these issues, device identification, also needs attention – how do you address a device, especially if it is within a public network such as the internet or part of it is within a closed network. Some will argue the traditional IP addresses (even once IPv6 is deployed) represents a sufficient start with sufficient governance mechanisms in place. Others will argue that traditional 'telephone numbers', sometimes referred to in the industry as E.164 numbers should work when needed. Other suggestions include using E.212 IMSI – mostly used as country identifiers in the global mobile network; and a proprietary address schemes.

Systems architects will contend that such hybrid design conventions will lead to future constraints. The core concerns remain: IoT devices not tied to geography should not use an identification scheme that is. Portability or mobility or nomadic capability no longer is part of market opportunity. The mobile sector overcame some of these limitations with the concept of a SIM card and even the IMEI (an identifier in each handphone). With that a new set of regulatory challenges arrived; one being mobile roaming retail charges. Oddly this is a consideration for IoT regulatory concerns – and will be covered below.

(2) The proxy competitor

Economic regulators have always served as the market's proxy competitor when the real one is absent. With the introduction of mobility, mostly cause by wireless technology, and later stimulated by data globalization caused by the internet platform a new stakeholder arrived at the regulator's doorstep: it had to regulate someone / something it had no reach over. The market also seized on this opportunity: it now had a revenue stream from someone that wasn't its customer – and had no economic obligation to be efficient. Astronomical prices for roaming usage arrived, and no one could do much about it other than a consumer chooses not to consume. Consumer welfare was irrelevant & it demonstrates where Authorities are powerless to play any constructive role. By extension if the IoT device is subjected to these same high roaming costs will it cripple opportunity for the wrong reason? The IoT developer then looks to the ISM spectrum alternative to insure the business model remains solvent, but weighs that against the potential of interference or unwanted intrusion in this unprotected band.

Roaming. Will a nomadic or mobility IoT device relying on wireless connectivity and intended to work in one geographic market easily adapt to its neighboring market? Not only is cost a concern, but spectrum assignments are. Band usage does not necessarily harmonize across a national border. Will the automobile or the tractor or the ship / airplane be less effective once it crosses a national boundary? Will that equipment be more expensive to operate? Would that IoT or M2M provider be expected to seek permission for their devices in every country anticipated for use? That is not only unrealistic, but inefficient.

(3) Harmonization: the promoter of standards

Devices require a protocol or language to communicate; there is a requirement for consistency for two devices to understand each other. Historically either proprietary or an open language existed. Proprietary protocols were developed, mostly because of the absence or availability of an open

standard. These proprietary platforms were the property of the developer and usually licenceed to those who used them – it also represented a huge commercial advantage for the developer because it could restrictively exercise control over innovation to suit its business model.

Once open source and technical standards arrived there were new opportunities available to manufacturers, especially in the IoT markets. But this paper is focused on policy, so what role might they play, if any. They can, but only to the extent that the market's stakeholders are willing to participate and cooperate. We must recognize that IoT, just like the internet itself, has a deep international aspect and that there are cultural, and technical and geographic differences that need to be factored. The regulatory Authority or the regional or global policy institution can play a significant role in bringing together disparate parties to reach a workable standard.

The MCIT in India has released a position paper[29] that clearly calls for a common shared architecture for these services within its jurisdiction. The government there has formed five working groups in economic verticals as broad reaching as – power, automotive, surveillance, health and security. In recognizing the scope and impact of IoT the government further indicated it expects to coordinate these findings with an effort to coordinate policy, and regulations.

(4) Competition

Might IoT prompt further liberalization of the communications market – i.e., who governs the control of the market devices; what is regulatory compliance? (And whose rules?). Or on the other hand is this beyond the reach of existing Authority or present legislation, so they chose to forebear – the metaphorical 'intentional walk'.

One responsibility of the Competition Authority is to evaluate consolidations of existing market participants. Historically the focus has been toward market power, usually following the merger – and normally conditions are applied to control the abuse of this new market power. Keep in mind that the industry in varying degrees around the world has moved from a infrastructure based model to a services based model. The result is the competition authority is faced with a dilemma: traditional measures to determine of market power in the ICT sector are obsolete. Data or information has growing value, and it is not being assessed properly by these Authorities, mostly because they lack the proper tools to make such assessments. Combining or consolidating businesses is exponential, not linear. This is Metcalfe's Law[30], although there is debate about its efficacy. This was simpler when providers sold services at a particular value; now providers trade in services that have a future mostly indeterminate value; an example when Google purchased Nest[31].

In the end, as we've just seen there are substantial gains to individuals, to economies, to societies, but they arrive with a cost. The job of the policy maker is to determine where the line must be drawn between these two or more competing factors. A final key point: by implying there are benefits and risks makes one falsely believe that this is two dimensional – something that a ledger sheet can quantitatively represent a score and thus an answer. This couldn't be farther from reality; the correct balancing point is most likely a moving target that the policy will need to identify, but also be prepared to continually adjust as society's norms demand.

---

[29] MCIT, Dept of Telecommunications, Govt of India, *National Telecom M2M Roadmap*, Oct 2014
[30] https://en.wikipedia.org/wiki/Metcalfe%27s_law
[31] Wohlsen, M, Wired, *What Google Really gets out of buying Nest for $3.2 Billion*, 14 Jan 2014

Conclusion. The EU expert group, noted above, arrived at several inferences[32]: need for transparency, both in the vendor supply relationship (how these systems function; independent certification with relevant metrics such as privacy and security), and in the public's understanding about what these objects are doing. This, in a way, leads to insuring access to information is governed by clear and understandable rules. Further there was a considered set of reports[33] released in mid-2014 from the Executive Office of the US President that recommended, among many other considerations, the policy focus for this broad issue should shift from collection to intended use.

When you consider what has been discussed and what exists in these policy statements in the US and EU and elsewhere, recommendations could be summarized as follows:

- **Resources.** We need to have full commitment and endorsement from all stakeholders of resource needs both at a local, regional and global level. By resources this includes: spectrum, standards, numbering.
- **Access.** Responsible access to information collected gives rise to responsibilities: inaccuracies to be expunged, and don't lose sight of data barons, who gain degrees of power opaquely.
- **Privacy concerns.** The largest IoT policy area with direct public / citizen impact. Intentions for data use should be part of the responsibility; changes of that use require re-permission; permission or consent should be clear, understandable and simple.
- **Transparency.** Both the device design (meaning capabilities) and the information collected belong in the public debate. A mandatory commitment that the 'algorithms' used to connect data are easily obtainable to insure an improved degree of fairness and accuracy over conclusions drawn from that data.
- **Aging.** When the useful life of a set of devices is completed, all stakeholders must be confident that they no longer present any liability either technically or societally.

Finally it is crucial that the public and industry conversations take place alongside the technological development. It is insufficient, arguably – naïve, to believe the IoT community can self-regulate or that the Authority can develop its rules alone. Both must work together to insure a successful future for this fastest contributing part of the communications sector.

[32] Van den Hoven, Jeroen, EU DG Connect; Ethics subgroup IoT – Version 4.0; P 20-21

[33] Executive Office of the President; May 1, 2014;
http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (visited May 2014) and
http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (visited May 2014)

Keywords: IoT policy, regulation of IoT, government authority, trust, identity

Andrew Haire with more than 30 years of experience spanning four continents has been associated with some of the industry's most successful telecom initiatives. He advises both governments and communication providers and is an expert in industry policy, market growth, strategy, technical opportunity, and economic structure. His portfolio included architecting major policy frameworks in the telecoms, technology, and postal sectors, as well as serving as regulator and responsible for ICT policy for 10 years at Singapore's iDA, soon after its inception in the year 2000.
He serves on the Board of the International Institute of Communications in London, and is Chairman of its US Chapter. Mr Haire holds a degree in engineering in the United States, attended the advanced management program from Harvard University. He has delivered papers / speeches on policy and regulatory frameworks in Asia, Europe and North America.