XONA PARTNERS

and OLSWANG

Internet of Things

Roadmaps and Regulatory Considerations

Dr. Riad Hartani, Frank Rayal, Rolf Lumpe
(Xona Partners)
&
Purvi Parekh (Olswang)

October 2015

Preamble

The Internet of Things (IoT) is by definition a vast topic that encompasses multiple markets, technologies, and disciplines. IoT comes with the promise of a new wave of applications and services deployment, significant investments and returns. Together with such promise, comes a series of obstacles – commercial, technical, regulatory and legal - that combined could slow down the rate of adoption of many smart technologies. IoT applications are broad, fragmented and (currently at least) siloed in specific verticals where multiple competing technologies (and law) vie for prominence. The topics of security and privacy become complex. Questions around the adequacy of resources for M2M services are paramount. Consumer acceptance of M2M services is fundamental.

From this perspective, IoT is an evolutionary process that will exhibit varying adoption rates in each silo while the market and regulators work their way through the challenges.

In this paper, we set out an ecosystem reference model for IoT and provide a brief overview of some key challenges, with special emphasis on the legal and regulatory aspects, how they are being addressed and how upcoming changes may impact in the future.

The IoT Ecosystem

To conceptually define IoT, consider a five-layer functional model that includes devices, connectivity, applications, platforms, and services (Figure 1):

Devices: Sensors, identifiers and gateways are types of IoT devices used to collect and convey information. Devices are designed and deployed to meet the application use case requirements. They can range from simple identifiers that provide specific information on the object, to complex devices that have the ability to measure (sensors) and process data (gateways). The application, use case and deployment scenario places requirements on the device such as size, weight, power consumption, and life of operation or deployment. This in turn impacts the connectivity of the device to the network. A variety of IoT devices have emerged in various business verticals, starting in the utility / energy sectors and evolving to devices in the health, transportation, home and finance ecosystems amongst others.

Connectivity: Devices can be connected directly to the network, or indirectly through another similar device (mesh) or a gateway that is provisioned to support multiple devices. Connectivity can be through a number of physical media such as copper, fiber and optical cable, or through the air through a number of wireless technologies. One of the challenges in IoT is the proliferation of connectivity standards, which is a common symptom of the breadth and fragmentation of IoT application requirements. These standards span the entire logical protocol stack through layers 1 – 7. Examples of connectivity would include the traditional 2.5/3/4G networks, as well as various local area solutions (Zigbee, Wi-Fi, Bluetooth, others) and low power wide area solutions (e.g. Weightless) among others.

Applications: Applications define the use case of the device and include all the necessary functions required to make use of the device for the intended purpose including the hardware and software architectures. IoT application stores are emerging with applicability to specific industry verticals, with the health wearable devices being a recent example.

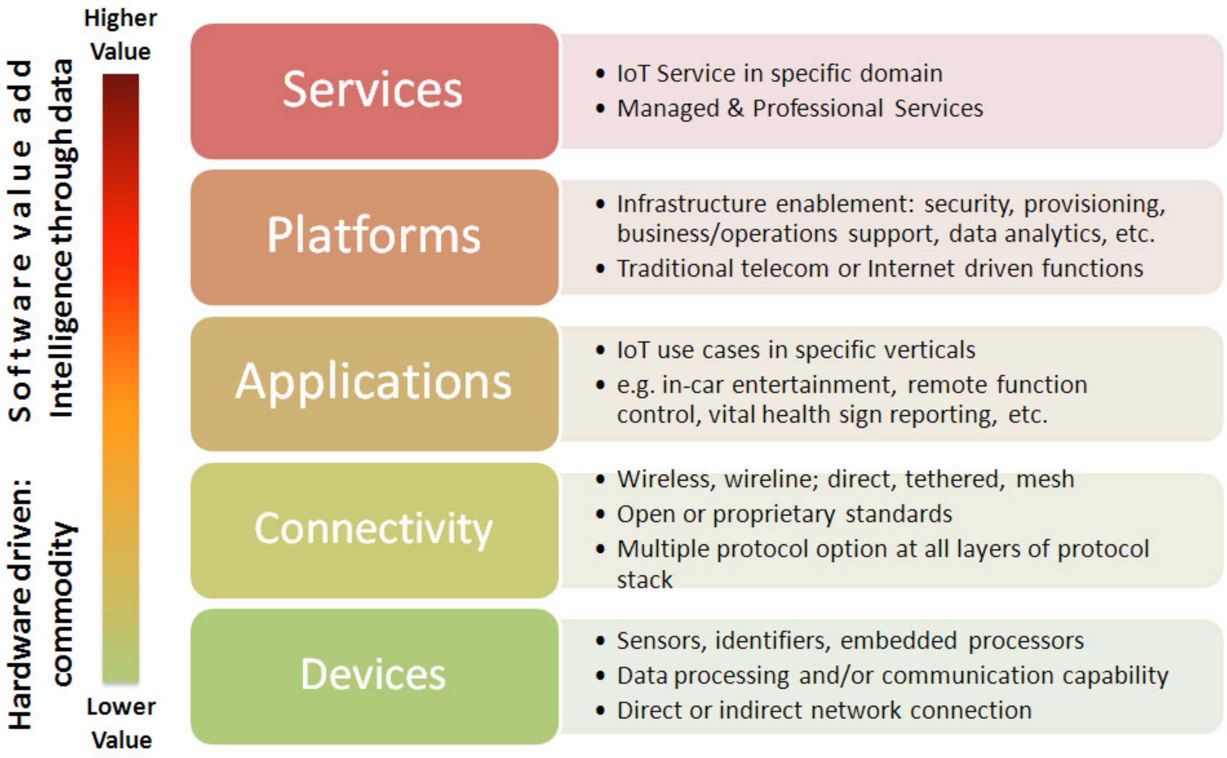

Higher Value
Lower Value
Software value add Intelligence through data
Hardware driven: commodity
Services
• IoT Service in specific domain
• Managed & Professional Services
Platforms
• Infrastructure enablement: security, provisioning, business/operations support, data analytics, etc.
• Traditional telecom or Internet driven functions
Applications
• IoT use cases in specific verticals
• e.g. in-car entertainment, remote function control, vital health sign reporting, etc.
Connectivity
• Wireless, wireline; direct, tethered, mesh
• Open or proprietary standards
• Multiple protocol option at all layers of protocol stack
Devices
• Sensors, identifiers, embedded processors
• Data processing and/or communication capability
• Direct or indirect network connection

Figure 1: IoT ecosystem reference model.

Platforms: Devices and connectivity require a platform to provide a service. Platforms are used to provision devices, manage and control them. They are used for billing and fraud detection. Platforms also provide the means to customize functions and data according to the requirements of end users. From this perspective, platforms allow the IoT infrastructure to perform as required.

Services: This references the IoT service to the end-customer. The service provider leverages all the downstream elements in this value chain: platforms, applications, connectivity and devices. The service provider can be the same or different from the platform and application provider. Examples include automotive automated diagnostic, medical geriatrics and remote power consumption optimization.

The IoT Connectivity Model – The data

In order to put it into context our conclusions and observations on IoT development, we model data flow, which can be characterized by three stages: data creation, transmission, and consumption.

Data creation: Data is generated by different types of devices, Data has specific characteristics such as rate, volume, latency, and frequency. For example, video surveillance has a high data rate whereas Supervisory Control And Data Acquisition (SCADA) systems have a low bit rate. Taking this example further, in many SCADA applications, the latency has to be very low to accommodate specific requirements of an application such as a fault in an electric transformer that requires the instantaneous switching of electric currents to avoid damage while there is higher tolerance to latency in video applications.

The creation of data can bring with it data privacy and security concerns at both a user level and a regulatory level. Although data flows may appear small, they still leave a digital trail. By the same token whilst a specific silo of information may appear harmless, putting silos together can provide a detailed insight into a person's life, opening them up to user profiling or tracking. An added complication is the different layers in the privacy evaluation; data is not just recorded in the database of an M2M service provider, but also in the database of the mobile network provider and/or in a home gateway or device. Add cloud services into the mix and the locations and jurisdictions where data resides also increases. All of these factors bring IoT and M2M services into the realms of data privacy legislation.

From a policy perspective the regulatory approach on IoT has not favored the creation or adoption of bespoke IoT legislation. The reality is that there is plenty of vertical legislation that applies to the IoT ecosystem under communications, privacy and sector specific laws, much in the same way as it applies to the majority of new technologies in the market. Instead a favored approach is that of "privacy by design" i.e. taking privacy and human values into account throughout the whole IoT engineering process. The concept, which actually originated a decade[1] ago, has been given the regulatory thumbs up across both sides of the Atlantic while Asia is closely observing the adaptation. Recently Federal Trade Commission Chairwoman Edith Ramirez endorsed the idea of companies conducting privacy (and security risk) assessments during the design process as well as the testing of security measures before products launch. Her endorsement went wider than just the engineering phase; she was also supportive of ongoing monitoring of products for vulnerabilities throughout their life cycle.

Data transmission: The transmission of data raises questions around bandwidth, latency, compression, encoding, multiplexing and and security, especially when considering the various platforms and networks over which data may traverse. Data encryption and device authentication are commonly adopted to combat security concerns. In addition, and although not mandated by regulators, commercial contracts in the IoT value chain increasingly incorporate detailed provisions around security defining responsibilities and liabilities as between all of the parties in the IoT value chain – not just the two parties at sitting at the negotiating table. These provisions range from stringent obligations on protecting against false requests for information to implementing ways to identify and combat unauthenticated commands. User behavior is also legislated for, with users being mandated to change passwords at regular intervals.

As with data creation privacy remains a concern, particularly where data is being transmitted across different countries or being routed to countries which do not have the same level of data privacy protection as exhibited in the country of origin. Data protection rules already tailor for such transfers and how these are to be handled in order to safeguard its protection.

Data consumption: Data is consumed in different ways, depending on the application. Simple systems that involve the user directly interacting with device is a mainstream medium. Think of the interaction with a wearable through an application on a mobile device or tablet. Alternatively and increasingly, sophisticated techniques based on data sciences are used to seek information beyond the original intended use. Whilst the collectors of that data promote the benefits that such data collection could result in (e.g. a homeowner may install a Google Nest thermostat, which she can control remotely; however, the data can also be shared with the utility company to control temperature within certain bounds during peak hours and to create more overall efficiencies),

[1] Joint report on "Privacy-enhancing technologies" by Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organization for Applied Scientific Research

from a privacy perspective there are immediate concerns. Users do not want to be tracked or profiled unless they have specifically consented.

Observations on IoT Market Space

By deploying the conceptual IoT framework above, we can model developments across the ecosystem layers starting with devices and connectivity and ending with platforms and services.

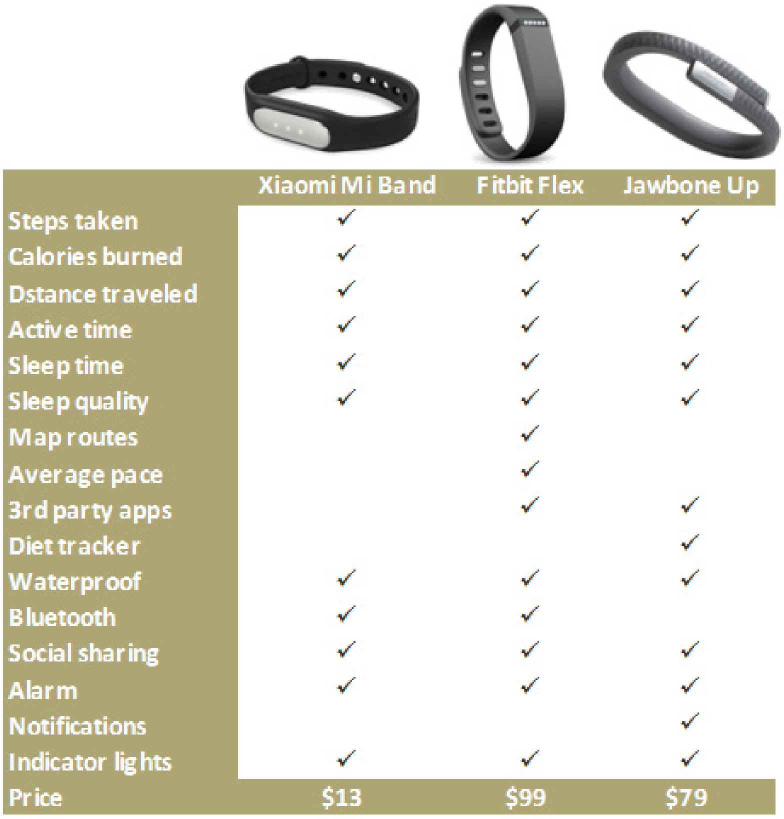
To start, we note that the IoT use case requires requires a devices and connectivity, underpinned by the interoperability of services, devices and platforms. Device characteristics such as size, weight, placement, mobility, power and communication characteristics as defined by the application drive what connectivity is required. Each vertical market (for example, automotive, utility, agriculture, home, health, general industry, etc.) uses different options thus resulting in a proliferation of connectivity standards. Whilst there are attempts at harmonization and standardization across verticals, we are not yet in a place where it is the norm.

1. Proliferation of connectivity standards: Depending on the characteristics of connectivity, various standards have been, or are, in the process of being defined. 3GPP standards such as GPRS, UMTS and LTE are licensed band access schemes that rely on high power for long range, consequently are relatively expensive in comparison with other connectivity techniques. On the other hand, technologies such as Bluetooth are meant for short-range communications in unlicensed spectrum and are low on power consumption. Various LPWA proprietary solutions have also recently emerged, mostly in unlicensed sub-1GHz spectrum but also in some licensed bands. Wi-Fi relies on higher power and provides longer range than Bluetooth albeit at a higher cost.

In recent years, advancements in silicon technologies such as 28 and 14 nm processes have significantly reduced power consumption to allow ever-smaller devices with less battery requirements to come to market. Coupled with the maturity of smartphones, this has led to the significant increase in wearables and personal connected devices.

From a regulatory standpoint international adoption through common standards has been on the agenda of many regulators and interested stakeholder bodies, keen not to stall the advancement of IoT. Only a few weeks ago, IEEE, the world's largest professional organization dedicated to advancing technology for humanity, announced that the Industrial Internet Consortium® (IIC) and the IEEE Standards Association (IEEE-SA) were collaborating toward development of a comprehensive architecture for an interoperable Internet of Things (IoT) around the world. In parallel various verticals are looking specifically at better harmonization. Take the automotive sector for example where new legislation was announced in the US around the creation of federal standards that secure cars and protect drivers' privacy.

2. Commoditization of devices: Essential to enable the business case for IoT applications is the trend of cost reductions in devices, as illustrated with the large number of players commercializing consumer wearables (Figure 2). The challenge to device manufacturers is how to differentiate from competitors. Our observation is that software applications and platforms, including operating systems, are the essential leverages used by device manufacturers to differentiate (e.g. Apple/iOS, Google/Android; Samsung attempt at differentiating through Tizen, and in a similar way Alibaba and XiaMi's own platforms design).



	Xiaomi Mi Band	Fitbit Flex	Jawbone Up
Steps taken	✓	✓	✓
Calories burned	✓	✓	✓
Dstance traveled	✓	✓	✓
Active time	✓	✓	✓
Sleep time	✓	✓	✓
Sleep quality	✓	✓	✓
Map routes		✓	
Average pace		✓	
3rd party apps		✓	✓
Diet tracker			✓
Waterproof	✓	✓	✓
Bluetooth	✓	✓	
Social sharing	✓	✓	✓
Alarm	✓	✓	✓
Notifications			✓
Indicator lights	✓	✓	✓
Price	$13	$99	$79

Figure 2: Device commoditization.

3. Commoditization of connectivity: As with devices we are seeing a downward slope of cost reduction for connectivity costs of IoT applications, driven by the need to enable the business case of most applications. There are many variants of connectivity including wireline andwireless technologies and increasingly a spectrum in between of license free/license exempt wireless opportunities. The lowest cost wireless connectivity leverages license-exempt spectrum over short distance (Figure 3). Wearables, for example, leverage Bluetooth to connect with smartphones. Alternatively, some consumer devices rely on longer-range license-exempt technologies such as Wi-Fi. Central hubs for connectivity and routing are deployed to tether over longer distances for remote control and monitoring. Where mobility is required, wireless technologies in licensed spectrum can be implemented albeit at a higher cost. It is exactly because of this that regulators are looking to support the IoT business case by considering comparable spectrum solutions that fall within the spaces between the licensed bands.

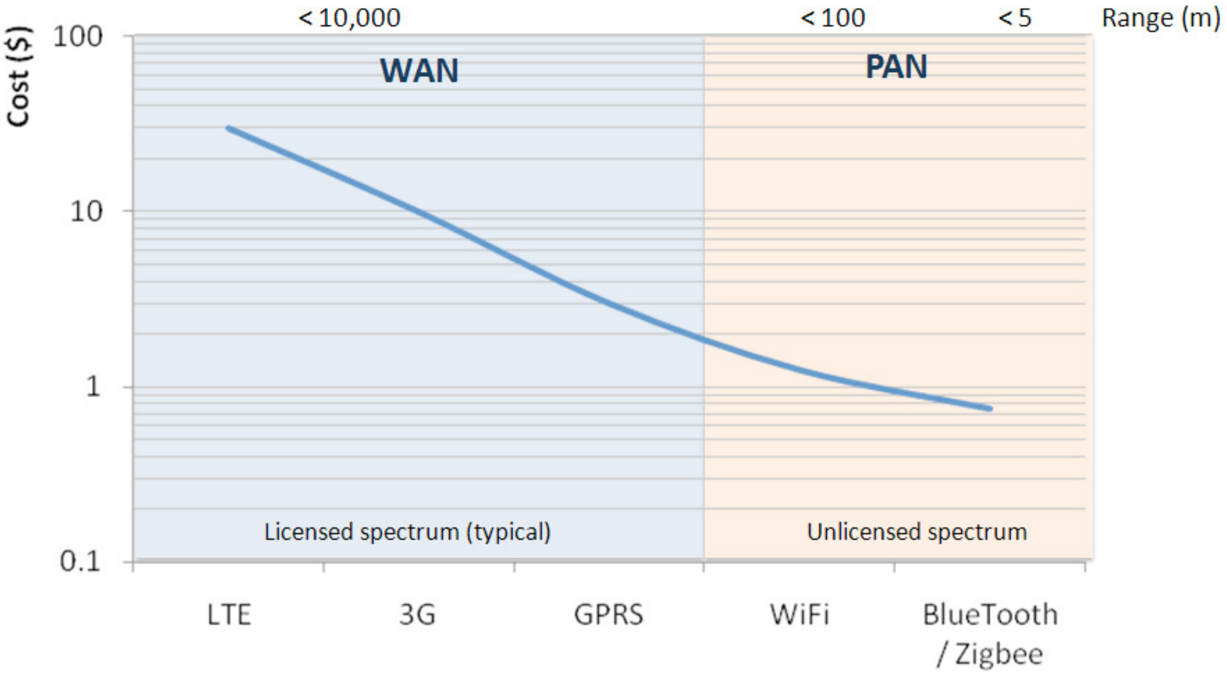


Figure 3: Cost dynamics for IoT wireless connectivity.

4. Emergence of long-range low power wireless technologies: We see an opportunity for very long range wireless technologies that are low power, low cost and work over long ranges (Figure 4). Such technologies are now on the market but it is still early days in the proof of their commercial viability (for example, Neul Weightless, SigFox Ultra Narrow Band, Semtech LoRa, and On-Ramp). These technologies often assume the build-out of a parallel IoT network to the mobile network.

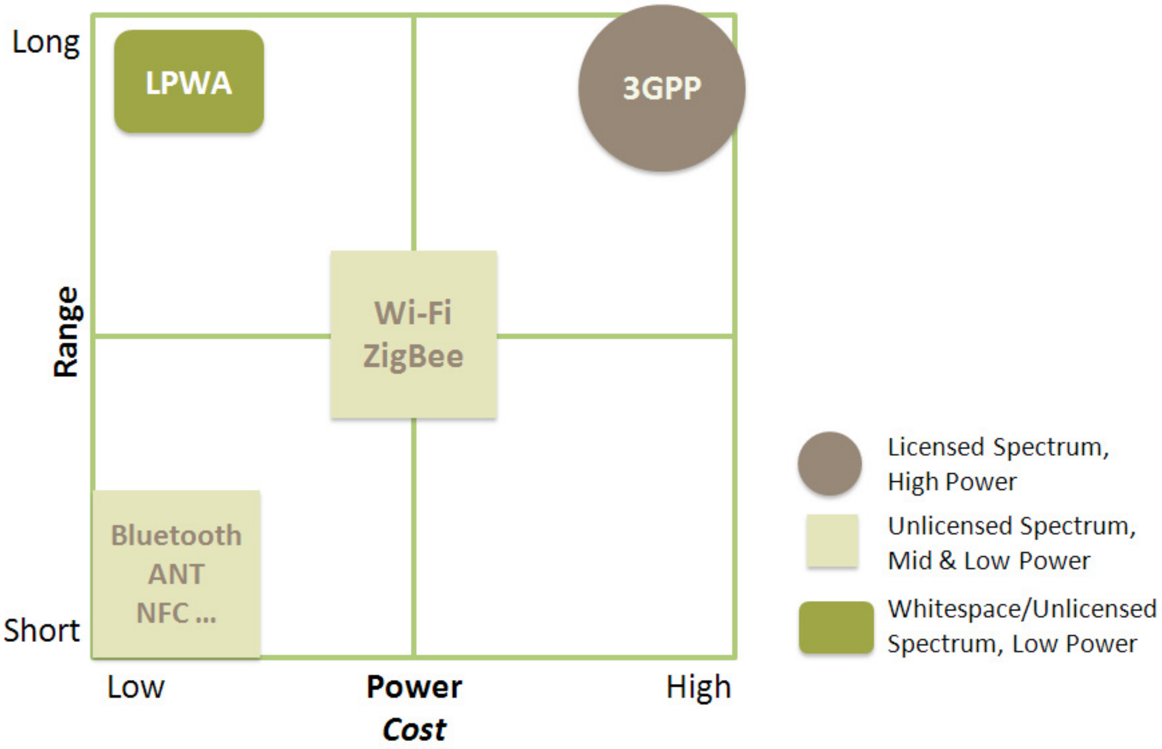

Long
Range
Short
LPWA
3GPP
Wi-Fi ZigBee
Bluetooth ANT NFC ...
Low
Power
Cost
High
Licensed Spectrum, High Power
Unlicensed Spectrum, Mid & Low Power
Whitespace/Unlicensed Spectrum, Low Power

Figure 4: IoT Wireless connectivity.

5. Competition and harmonization of connectivity standards: Connectivity standards have been progressing slowly but steadily. The challenge is not in the definition of these standards, but more in the number of variety of competing and complementary standards, as well as the conflicting interests of the industrial groups behind the various standards. Although harmonization is ongoing, it is very likely that IoT solutions will face challenges for rapid mass adoption. The development of interworking platforms with open APIs will help alleviate some of these challenges by allowing interoperability of different standards or different implementations of the same standards. This is not only the case for physical and link layer standards, but also includes aspects related to applications and services running on top of the IoT ecosystem.

6. Partnerships and alliances to win the IoT platform war: The development of IoT solutions is inherently about the development of ecosystems around offered solutions. Such ecosystems are not mandated by legislation but instead built via negotiated partnerships between various industry players. Given regulatory challenges on revenue, the leading players will seek to control the ecosystem by providing a platform that would host IoT applications, and over which IoT services will be built (Figure 5), as this is an important new revenue stream for them. As in any platform model, such as those in smartphones and the Internet, the key is to increase its adoption. Various models are being put in place to achieve this, via the development of open source IoT connectivity and interworking software, open APIs to plug into the platforms, and SDKs to develop services on top of the platform. We foresee the emergence of selective alliances over the next few years, across industry verticals, with a focus on advancing specific IoT platforms, but progressively evolving towards selecting winners, as it's traditionally the case for Internet-centric business models. Various contenders are already in the game to achieve this, including the Internet platform players (Google, Apple, Amazon, etc.), the lead industrial players with a specific vertical focus (e.g. GE for industrial Internet), as well as mobile operators, particularly those who support a strategy towards Internet-scale OTT deployment.

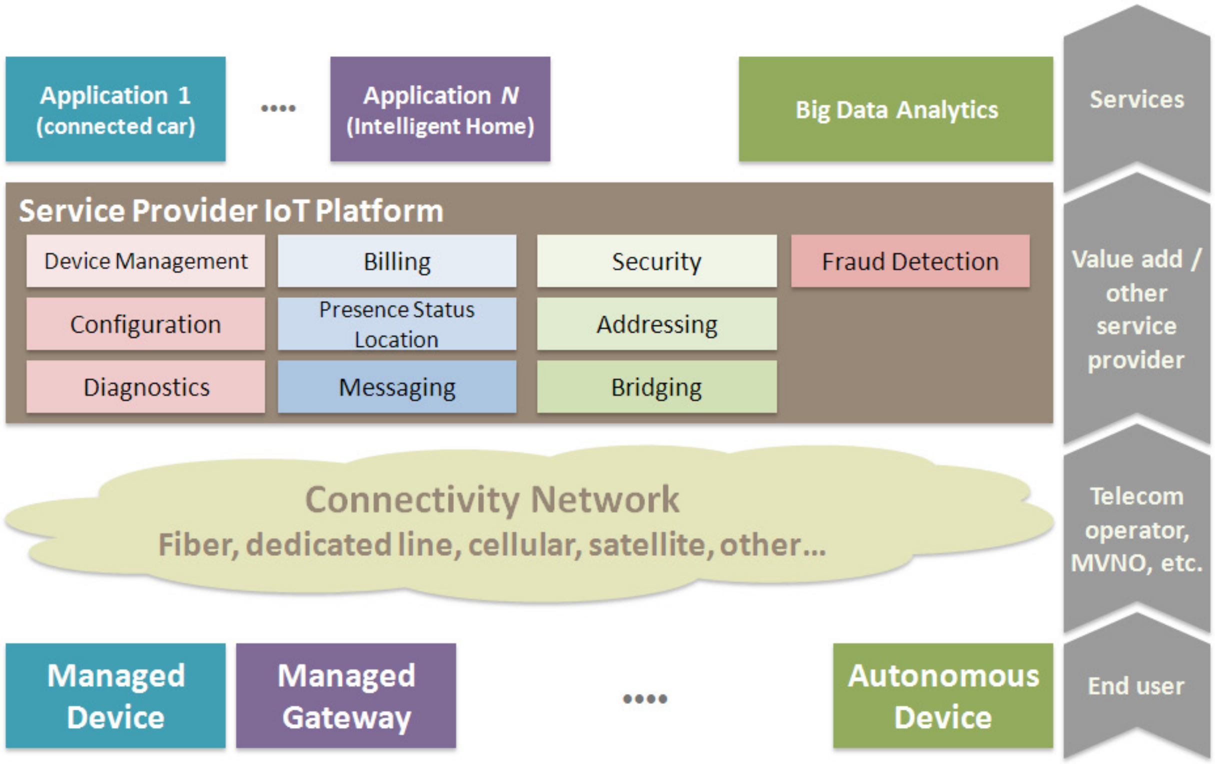


Figure 5: Value appropriation through platforms.

7. Emergence of new MNO and MVNO service models: A key dynamic of the IoT market is that the majority of 'value' in any IoT application lies not in the simple carriage of data, but in the provision of an overall service. For example, a wide-area wireless enabled home security system represents a significant revenue opportunity for a mobile or virtual mobile network operator, including revenues from device sales, installation, and monthly service fees. However, the data traffic revenue that such a solution generates is likely to be relatively small in comparison. Similarly a connected health solution will include the connectivity network as well as the platform to manage the solution, interfacing with the various stakeholders in the health solution value chain. The story is the same for many other IoT applications: the real opportunity for mobile operators lies in moving up the value stack and away from the simple provision of data carriage services. The result is an ecosystem that is complex, multi-party and heterogeneous in nature. The mobile network operator provides the connectivity and IoT management for value add. IoT solution providers (either OTT service providers or mobile service providers who offers IoT solutions) will have to integrate all the components of the ecosystem for the end-to-end IoT solution. Each has a crucial role to play in the value chain.

With such a complex chain comes a mesh of legal liabilities and challenges. Individual responsibilities are more difficult to segment and hence to legislate for. Privacy and privacy responsibilities require more careful scrutiny as do security requirements and obligations around where these sit in the value chain. Commercial leverage will play an even more important part.

8. Extracting value through data sciences: Temporarily putting to one side the fundamental privacy issues around extracting value in this way, as businesses evolve to leverage the huge amounts of data assembled, mining and learning through such data creates significant opportunities. By the same token so does optimizing communication between those producing it and those using it. The desired goal of IoT businesses is to create a solid foundation architecture that is able to provide these optimal functional capabilities together with a platform to overlay data science applications. This would include the various layers in the data value chain – optimized processing through an acceleration of migrations to the cloud, scalable data management leveraging big data models and the use of customized data sciences solutions for business intelligence creation. This "solution" is complemented by a fundamental re-architecture of IT models within the businesses integrating IoT models.

We are now witnessing the emergence of an enhanced (and new in some cases) set of machine learning and data mining algorithms, specifically focused on clustering and predictive modeling in high dimensional spaces which is based on imprecise, uncertain and incomplete information, efficient statistical data summarization and features extraction algorithms as well as large-scale real-time data stream management. These tools will be at the core of the processing engines being commercialized or running in open source environment, and will aim, when applied to specific industry problems, at optimizing the existing business logic and augment it with new functionalities over time.

9. Evolution to 5G: In terms of timing and mass market adoption of advanced IoT solutions, it is very likely that this will converge and overlap with the specification and rollout of the first 5G networks. It is then natural that 5G specifications will have to take into account IoT requirements, either directly or via the complementary technologies that will form the future mobile ecosystem (including evolutions of Wi-Fi, LPWA, Zigbee, etc.). As such, the LTE roadmap will continue to evolve to include new features that represent a precursor to those in 5G. For example, LTE-

MTC in Release 13 aims to reduce power consumption of LTE devices for IoT applications and achieve low cost points by eliminating some of the broadband features of LTE (Figure 6). On the core, back-end and underlying IT infrastructure, a gradual move towards virtualization, specific functionality enablement in private/hybrid/public cloud environment, and integration of big data analysis frameworks into network data management, will start appearing. All of these aspects will in essence contribute to bringing advanced IoT solutions and IoT centric business models to markets.

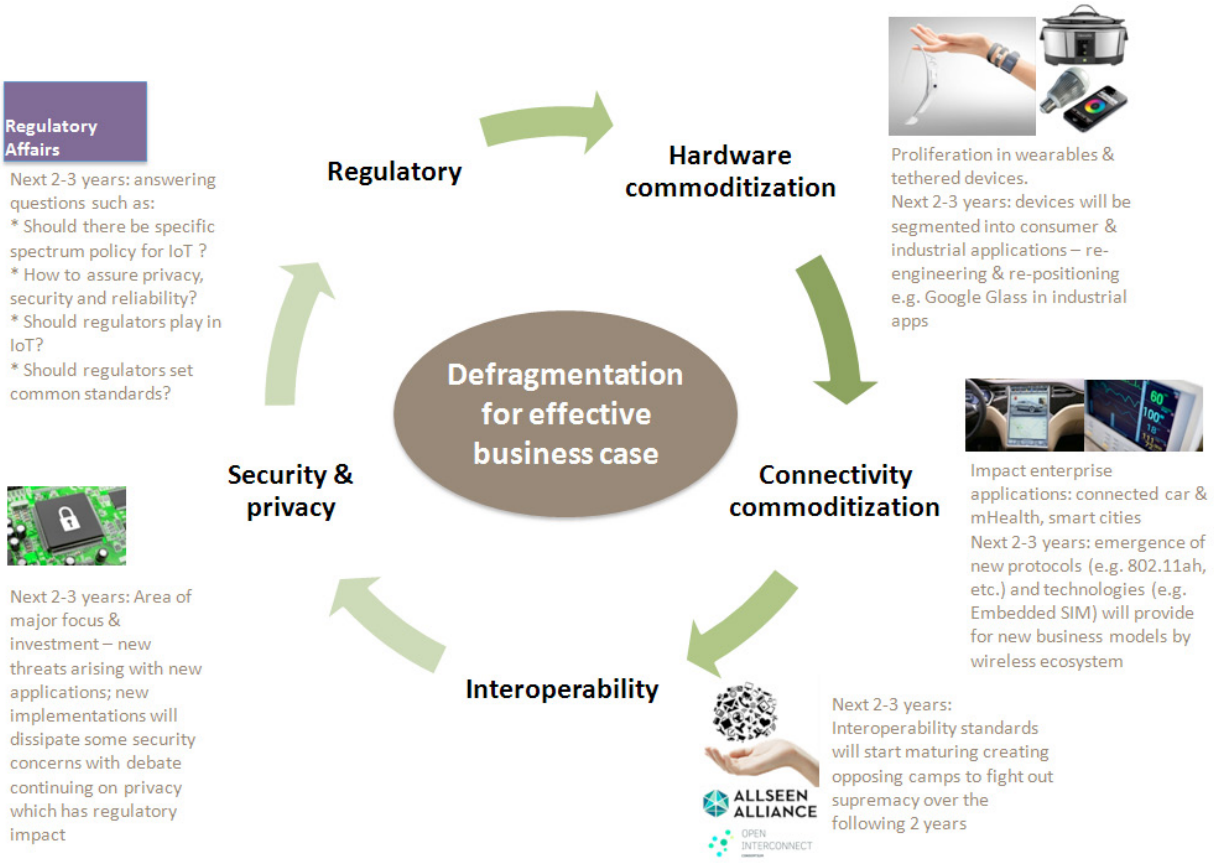

Regulatory Affairs
Next 2-3 years: answering questions such as:
* Should there be specific spectrum policy for IoT ?
* How to assure privacy, security and reliability?
* Should regulators play in IoT?
* Should regulators set common standards?
Regulatory
Hardware commoditization
Proliferation in wearables & tethered devices.
Next 2-3 years: devices will be segmented into consumer & industrial applications – re-engineering & re-positioning e.g. Google Glass in industrial apps
Defragmentation for effective business case
Security & privacy
Connectivity commoditization
Impact enterprise applications: connected car & mHealth, smart cities
Next 2-3 years: emergence of new protocols (e.g. 802.11ah, etc.) and technologies (e.g. Embedded SIM) will provide for new business models by wireless ecosystem
Next 2-3 years: Area of major focus & investment – new threats arising with new applications; new implementations will dissipate some security concerns with debate continuing on privacy which has regulatory impact
Interoperability
ALLSEEN ALLIANCE
OPEN INTERCONNECT
Next 2-3 years: Interoperability standards will start maturing creating opposing camps to fight out supremacy over the following 2 years

Figure 6: IoT ecosystem dynamics.

IoT – The Road Ahead

As far as mass adoption is concerned the IoT era has had various false starts. The recent convergence of various trends including innovation in low power and low cost device technologies, scalable network connectivity as well as mainstream cloud and big data processing models have opened a new window for the emergence of IoT based value added services that will in time become mainstream. Vertical specific creation of common standards, legislations and regulatory approach will further support greater international deployment.

With the significant transformation in the IoT ecosystem comes challenge and opportunity. IoT, in its blurring of the distinction between public and private, is driving increased focus change in the business and legal landscape, with significant implications for regulatory and policy makers over the next decade. Indeed, as most recently highlighted by BEREC's (the Body of European Regulators for Electronic Communications) report and public consultation on M2M services, this focus is about how to facilitate M2M and to make it thrive. Whether this means that we are looking at more rather than less regulation remains to be seen.

Acronyms

3G	Third generation
3GPP	Third generation partnership project
4G	Fourth generation
5G	Fifth generation
API	Application program interface
DSL	Digital subscriber line
GPRS	General packet radio service
GPS	Global positioning system
GSM	Global System for Mobile communications
iOS	iPhone operating system
IoT	Internet of Things
IP	Internet protocol
IT	Information technology
LPWA	Low power wide area
LTE	Long Term Evolution
MNO	Mobile network operator
MTC	Machine type-communication
MVNO	Mobile virtual network operator
P2P	Peer to peer
PLC	Power line communications
SCADA	Supervisory control and data acquisition
SDK	Software development kit
SIM	Subscriber identity module
UMTS	Universal Mobile Telecommunications System
V2P	Vehicle to Pedestrian communications
V2V	Vehicle to Vehicle communications
WRC	World Radio Conference
IP	Internet Protocol
IS	Industry Standard
ITU	International Telecommunication Union
JDBC	Java Database Connectivity
LTU	Long Term Evolution
M2M	Machine to machine
METIA	Mobile and wireless communications Enablers for Twenty-twenty (2020) Information Society
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
MTAS	Multimedia Telephony Messaging Server
MVNO	Mobile Virtual Network Operator

Xona Partners (Xona) is a boutique advisory services firm specialized in technology, media and telecommunications. Xona was founded in 2012 by a team of seasoned technologists and startup founders, managing directors in global ventures, and investment advisors. Drawing on its founders' cross-functional expertise, Xona offers a unique multi-disciplinary integrative technology and investment advisory service to private equity and venture funds, technology corporations, as well as regulators and public sector organizations. We help our clients in pre-investment due diligence, post investment life-cycle management, and strategic technology management to develop new sources of revenue. The firm operates out of four regional hubs which include San Francisco, Paris, Dubai, and Singapore.

Purvi Parekh is Head of the International Telecoms practice at Olswang LLP. Olswang LLP is a pioneering law firm with a distinctive approach to business law and an immersive culture. Thanks to our decisive, connected and highly-commercial people, we have built an unparalleled TMT practice, which makes us the firm of choice for true innovation. We have also established a commanding reputation for changing the face of business in a wide range of other industries, notably Real Estate. Headquartered in London, Olswang has an international presence spanning Belgium, France, Germany, Spain, the UK and Singapore.

Xona Partners

www.xonapartners.com

advisors@xonapartners.com