Anyone's Game: Economic and Policy Implications of the Internet of Things as a Market for Services

Jaclyn SELBY
University of Southern California

Abstract: Research suggests the future of the Internet will be defined by ubiquitous computing: a networked environment in which smart objects, called 'Things,' are imbued with identification data and micro-processing power to form an Internet of Things (IoT). Data production across the Internet continues to proliferate at exponential rates. Thus, this paper aims to provide an introductory framework for the IoT as a market for value extraction from captured data, supported by cloud computing and semantic web services. The paper outlines the technological basis for the IoT in brief, as well as assessing the current state of scholarship in this area. The IoT is then divided into four market segments by the type of end-user addressed by service providers (individuals, firms, city-government, national-government) in order to highlight and illustrate the major policy implications of this emerging services market.

Key words: Internet of Things, ubiquitous computing, big data, cloud computing, policy.

■ Introduction: the data explosion

In 2008, a quarter of the world's population had gained access to the Internet. It took more than three decades for the first billion people to get online - but just eight years for the second billion. One of the most significant outcomes of this rapid growth of the networked world is that it produces a lot of data. The European Commission estimates that the public Web contains 55 trillion hyperlinks, 600 billion RFID tags, and produces more than eight terabytes of information traffic per second (NAVAJO *et al*., 2009). Furthermore, the rate of traffic continues to increase exponentially each year with growth largely driven by high resolution inputs over broadband connections from multimedia devices such as remote cameras, complex sensors and smart phones. At this scale, automated digital computation is necessary to parse and respond to the information the Internet produces. Consequently, the likely future of the Internet is one defined by ubiquitous computing: a pervasive networked environment in which smart objects,

henceforth called 'Things,' are imbued with identification data and micro-processing power to form an 'Internet of Things.'

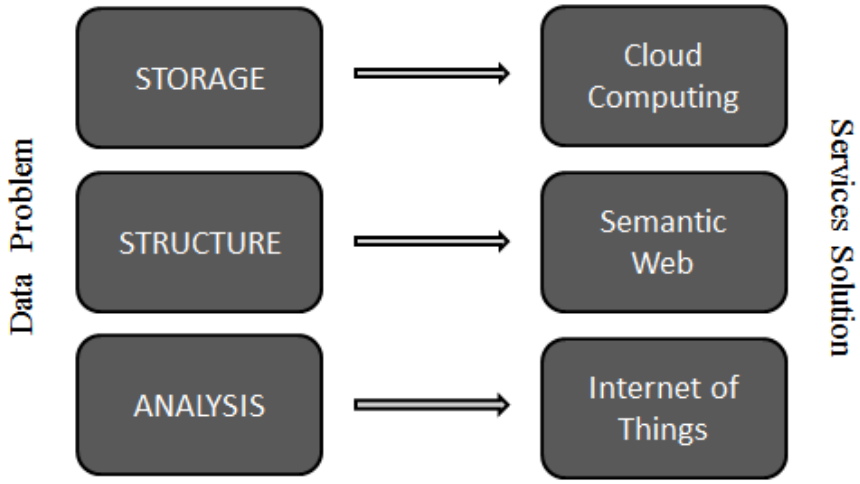
Simply put, the Internet of Things (IoT) is comprised of webs formed by physical objects, such as sensors or everyday objects like appliances and vehicles, which are capable of structured communication to and from remote databases and between themselves. The IoT's emergence is essentially a convergence between the digital World Wide Web – and its attendant information flows – and the physical world. Furthermore, the IoT must be distinguished as capable of interfacing with but clearly distinct from the Internet of Media (online content) and the Internet of Services (online commerce and software applications).

This paper aims to offer an introductory framework for defining and assessing the Internet of Things as a services market. It proceeds by first clarifying how the IoT as a market has developed in response to the demands of tackling the current data explosion in the networked economy. It then provides a brief overview of the technical underpinnings of the IoT. Next, a review of the literature on the business case for the IoT is undertaken and determines that there is no clear macro-level framework to assess this phenomenon from an economic or regulatory standpoint. The author then proposes – for illustrative and pedagogical purposes – a practical division of the IoT into four distinct market segments based on scale of service in order to highlight emerging service clusters and implications for policy. The paper concludes with a broad overview of significant policy issues for the nascent IoT market and offers recommendations and avenues for further research.

■ Three building blocks for data management markets

If the Internet can be likened to an enormous data production machine, its output largely resembles so much disorganized flotsam and jetsam. Only a small percentage of the data online is 'structured,' meaning that it is standardized to be machine-readable. Thus, it is useful to break down the overall problem of automating value extraction from captured data into three component features: storage, structure, and analysis. These are addressed by three overlapping but distinct markets for data management that have emerged in recent years: Cloud Computing, the Semantic Web, and – most recently – the Internet of Things.

Figure 1 – The data management market(s)



Storage

The concept of Storage encompasses both the question of where data should 'live' and the delivery of computing power to process it. This group of issues is addressed by the market for Cloud Computing, which may be loosely defined as the provision of on-demand services to provide networked access to storage and processing resources via a remote – usually Internet-based-platform (KUSHIDA, MURRAY & ZYSMAN, 2012). On a practical level, this means that firms, rather than directly owning the means to store or process their data, may rent these capabilities from 'cloud' services providers.

Structure

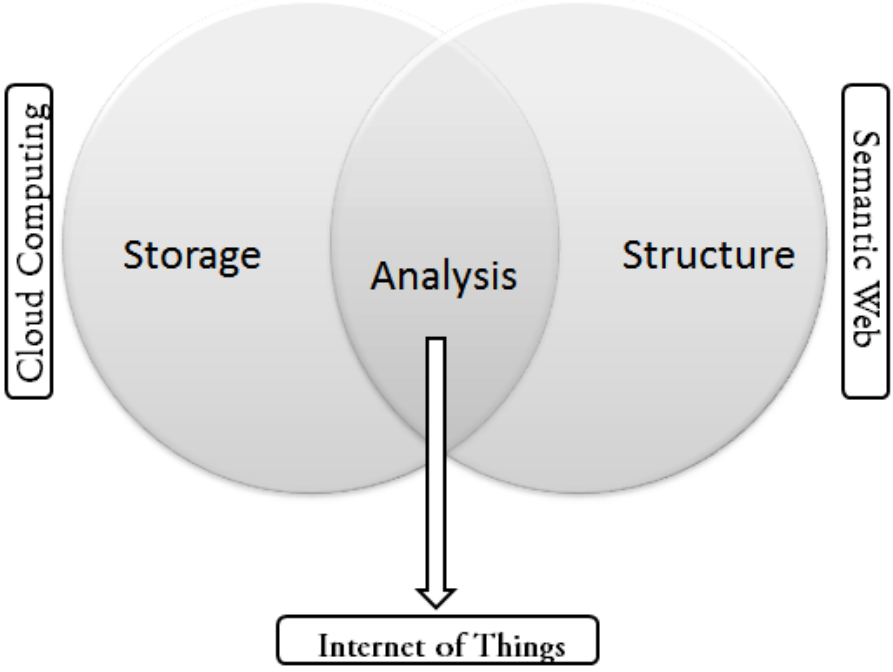
The concept of Structure addresses the issue of identifying and classifying different types of data in a manner that is standardized, contextual, and machine-readable. A set of technologies for encoding data, collectively termed the Semantic Web, attaches context and structure to the online data stream via the application of complex but efficient content-indexing and labeling schemes (BERNERS-LEE, LASSILA & HENDLER,

2001). Fundamentally, the Semantic Web can be seen as a group of services that appends and standardizes metadata (ie. the information that describes data) such that machines or virtual agents can categorize and respond appropriately to the data they encounter.

Analysis

The problem of Analysis may be summed up as a question of how to extract meaningful value from data that has been captured. Storage and Structure are necessary but insufficient preconditions for the solution of this puzzle; it is machine logic that is crucial to data comprehension on a scale beyond human computation. Thus, by making it possible for machines to access, identify, and transmit remote data, Cloud Computing and the Semantic Web set the foundations for the third set of services – the IoT – built around the idea that some Things are capable of processing logic that allows them to respond dynamically to incoming data. A 'smart' shipment, for example might determine its own route through the supply chain based on data it receives about live traffic conditions.

Figure 2 - Service foundations for the IoT



To simplify a discussion of Things that encompass a vast range of capabilities and specifications, this paper puts forward that the majority of definitions across the literature contain the following features (CASAGRAS, 2009; International Telecommunications Union - ITU, 2005; VERMESAN & HARRISON, 2009):

- All 'Things' are physical objects containing Network Embedded Devices (NEDs), a general term for devices capable of either holding passive information that can be identified by other devices in a network or capable of active transmission of information to the network.
- NEDs provide a standardized means for object-specific identification.
- Some Things can gather information about the physical environment via the use of sensors.
- The networked environment may provide virtual counterparts, such as a webpages, which can act as interfaces for Things.
- Things capable of communication may communicate with people, other Things, or virtual objects such as databases.
- Things operate autonomously without human intervention; it is implied they are robust, cheap and long-lasting.

CHAVES & NOCHTA (2010) further suggest that both basic and higher level functions of the Things, or Smart Objects, can be grouped into five categories: information storage, information collection, information communication and processing, and performance of actions. These categories can be considered the basis for all the applications comprising the market we call the IoT.

■ Technological foundations for the IoT

The IoT contains a vast range of technical standards and ways to accomplish the connection of physical objects to remote networks that is informed by a multidisciplinary legacy that includes computer science, psychology, management strategy research, and electrical and mechanical engineering. This paper – being non-technical in nature – provides a brief description of the most typical technologies for this purpose.

A simple and cheap system of item identification is provided by Radio Frequency Identification (RFID) technology, which has been in use since

1939 (Transportation, 2006) but in this context provides an unobtrusive method of using short-wave radio to identify physical objects. Sometimes considered an advanced barcode, the RFID system is comprised of the following elements: tags and readers, antennae, communications hardware and software infrastructure. The RFID tag is a microprocessor chip that may be active (capable of broadcasting) or passive (only capable of being identified). The system is always 'turned on,' meaning that whether active or passive it always responds to a signal. The tag contains a unique identity that is discoverable by an RFID reader, a device that can read from and write data to tags operating on the same radio frequency and technical specifications (International Telecommunications Union - ITU, 2005). The RFID antenna creates a transfer point for the data to be read or transmitted via the communications infrastructure.

The primary technology used for Smart Objects capable of collecting information from the environment is the Wireless Sensor Network (WSN), an inexpensive and miniaturized system capable of collecting, sending, and processing data. The most basic components include a sensor unit, a micro-processor chip with a battery, and wireless communication modules (SHEN & LIU, 2010). The WSN functions autonomously but may also be remotely controlled. Other optional function units are dependent on the type(s) of information being gathered by the sensor. The current range of possibilities is tremendous and includes temperature, chemical composition, humidity, pressure, location, vibration, object orientation, sound, image, air flow, light, pressure, or energy usage (van LIESHOUT *et al*., 2007; VALHOULI, 2010; ZOUGANELI & SVINNSET, 2009). The possible applications that might emerge as a consequence of connecting the sensor to the networked environment are almost infinite in their scope.

In addition to the most common hardware, there are also frequently used coding systems for object identification. In the IoT the most prominent – although certainly not singular - method of generating unique identifiers is the Electronic Product Code (EPC) (FLEISCH, 2010). The EPC is a string of numbers generally used to label objects in the retail supply chain; it is divided into numbers which identify product type, manufacturer, and virtually unlimited unique item identifiers such as transportation route, origin and shelf-time. The EPC may also be used to map object data to an online internet protocol (IP) address in order to create a virtual counterpart to the smart object – ie. a web page hosting its data.

■ The business case for the IoT: state of the literature

Today, the majority of research addressing the IoT details specific applications with a few comprehensive reports attempting, industry by industry, to illustrate the full scope of future services offerings (International Telecommunications Union - ITU, 2005; van LIESHOUT *et al*., 2007; VERMESAN & HARRISON, 2009). It is also notable that beyond the hard sciences, much of what is written in this area is contained in conference proceedings, private sector and think tank reports, and government agency publications, rather than in peer-reviewed journals, suggesting a field still in an emergent phase of scholarship. The economic aspects of the IoT have been particularly overlooked, as demonstrated by a literature review of 85 academic journal papers published between 1995 and 2005 (NGAI, MOON, RIGGINS & YI, 2008) on the subject of radio frequency identification (RFID). Ngai et al.group these papers into just four categories: RFID technology, Applications, Policy Issues, and Other. Over a third of the papers were on technical issues, an additional third of the papers detailed specific applications, 12.9 percent were about policy issues, and the rest were general introductions. Of the policy papers, all of them covered one of the following three issues: privacy (45.4 %), security (36.4%), and standards (18.2%) (2008).

Although it is possible to ascertain that 15 distinct industries were addressed, and that some articles appeared in management journals, no papers in their sample had a primarily economic or business focus. In part this may be due to a lack of empirical data for thorough economic analyses of a nascent industry. However, the extensive literature on existing services which employ Things, as well as myriad descriptions of potential applications, provides a detailed roadmap of the future of goods, services, and even service providers in the IoT. Furthermore, research on technical specifications, standards, and large-scale applications additionally allows for inferences about capital and technical requirements for service providers. One may conclude that the field is open for compelling arguments about broad economic implications of the IoT as well as assessments of its likely industrial organization.

One particular problem in the extant IoT literature is that in focusing narrowly on single applications or services types, there is a tendency to myopia. Typically, the bounding criterion used for discussions about services, technical standards, or even regulation is the specific industrial sector (ie. energy, health, transportation). Many IoT service providers,

however, operate across a wide number of sectors in order to benefit from the economies of scope arising from widely applicable technical applications. For pedagogical purposes, a broader segmentation strategy is called for to better provide an illustration of emerging clusters of services and broad policy issues in this arena. Consequently, the following discussion loosely organizes the IoT into four distinct market segments characterized by the type of end-user addressed by service-providers: individual-level, firm-level, city-government-level and national-government-level.

■ An overview of the IoT market by scale of service provision

Although the IoT market is still relatively small, the provision of Storage and Structure services for data management through the Cloud Computing and Semantic Web markets has rapidly expanded, setting the stage for the exponential growth of Analysis services. Market figures for the IoT are difficult to calculate, particularly where Things – such as networked phones – are subsets of other markets. Estimates place current market capitalization at $5.5 billion USD (WEBER & WEBER, 2010) and approximations of future size range from $20 billion USD to $100 billion USD (VALHOULI, 2010).

Services provision at the individual-level

The market for individual-level services in the Internet of Things, as measured by the estimated number of connectable consumer devices by 2020, is hypothesized to be somewhere between 6 and 44 billion with 16 billion as a 'reasonable' estimate (MORRISH, 2010). Based on the literature on applications directed at individual consumers (KORTUEM & KAWSAR, 2010; WELBOURNE *et al*., 2009; ZOUGANELI & SVINNSET, 2009), the following major services categories emerge:

- *Personal electronic devices and appliances:* the variety of Things connected to the Internet to deliver information, such as email, or use built in sensors to take appropriate action in response to environmental data, such as feeding your fish.
- *Personal network solutions:* e.g. 'smart homes' in which energy systems and appliances can interface with each other and with remote objects or mobile networks localized to a vehicle.

- *Records interfacing via smart 'everyday' objects:* this includes Things which interface with larger databases, such as vehicles which can update insurance records.

These services represent a tremendous number of industries, ranging from healthcare and energy to food and animal husbandry. IoT services for individuals are characterized by niche applications and services and a high degree of product differentiation is already evident, particularly where product substitutability is high. Here, capital requirements are kept relatively low by the possibilities of small scale production and minimal technical requirements due to the smaller necessary broadcast distances for smart objects in personal networks.

Services provision at the firm-level

The market for business-to-business services is the most developed in the IoT. The use of RFID to track objects through the supply-chain is well known and has been widely adopted by large retailers like Walmart and Amazon to greatly reduce distribution costs. Firms like IBM, for example, estimate the IoT market for business services will grow so much that they have invested $12 billion USD over four years ("A different game," 2010). The author's review of services offered to firms (HALLER, KARNOUSKOS & SCHROTH, 2009; YAN & HUANG, 2009; ZOUGANELI & SVINNSET, 2009) suggests the following clusters:

- *Consumer intelligence:* using Things to capture information about consumer that can be 'mined' to inform decisions about product and service improvement and planning.
- *Business intelligence:* using Things with sensors to capture information about the firm's activities and environment (energy usage, resource management) which may improve efficiency and performance.
- *Retail supply chain management:* tracking objects through the supply chain, allowing for 'just-in-time' production of products.
- *Industrial automation:* 'smart factories' which run themselves.
- *Product security services:* using Things to prevent theft and counterfeiting.
- *Regulatory compliance:* using Things with sensors to ensure standards for environmental and product safety are met.

The requirements for services provision to firms differ greatly as compared to those for individual end-users. Providers must have access to significant means of production in order to provide the vast number of Things required for large retail supply operations while maintaining low marginal costs per unit. The bar for technology is also higher; computer systems must be able to track products accurately across the global supply chain. Additionally, some networked devices must reliably perform complex operations with little to no human intervention.

Services provision at the city-government-level

City governments have long been amongst the biggest gatherers of data, keeping records on demographic statistics, economic figures, weather data, and legal regulations, amongst other things. It is of no surprise that they stand to benefit greatly from automated data management. Interest in 'Smart Cities' has recently grown rapidly; more than 50 cities worldwide use IoT services for some aspect of city administration and spending on Smart City initiatives is projected to grow from $8 billion USD in 2010 to almost $40 billion in 2016 (ABI Research, 2011). The author's review of literature detailing IoT services at this scale (International Telecommunications Union-ITU, 2005; van LIESHOUT *et al*., 2007; VERMESAN & HARRISON, 2009) suggests the following categories of service:

- *Infrastructure services:* e.g. networked traffic systems and energy grids.
- *Resource management:* using Things with sensors to manage water, energy, and other natural resources.
- *Public Safety:* e.g. using Things with sensors to track contaminated food or vaccine stocks.
- *Environmental monitoring:* using Things with sensors to measure pollution, rainfall etc.
- *Animal tracking:* using Things to track zoo animals or livestock.
- *Local record systems:* using Things to track public library books or government documents, etc.
- *Local fines and ticketing:* automating traffic tickets and fines via Things with sensors.
- *Infrastructure security:* smart buildings capable of monitoring themselves for needed repairs or security breaches.

- *Emergency response coordination:* networked systems can anticipate and coordinate emergency action.

The characteristics of service provision at the city-government level differ yet again from requirements of provision to individuals and businesses. The centralization of city administration results in high capital investments and technical know-how in order to create custom solutions for large numbers of data types, data standards, and existing records that must be uniformly semantically structured and stored in the cloud.

Services provision at the national-government level

The size of the market for IoT services to national governments is enormous, given that this segment also comprises military spending and is projected to grow to at least $42 billion USD by 2017 (ABI Research, 2011). As one example, the U.S. Department of Defense doubled its spending on IoT services from $115 million in 2006 to $230 million in 2010 as it attempted to manage an ecosystem of 376,200 objects and 51,000 vendors across 2,000 legacy logistics systems (Transportation, 2006). As governments increase regulations designed to combat such widespread problems as counterfeit drug production, energy efficiency, food-borne disease, and illegal trafficking, a corresponding increase will happen in the demand for IoT services. The author's review of the literature suggests the following services clusters at this scale (ATZORI, IERA & MORABITO, 2010; International Telecommunications Union - ITU, 2005; van LIESHOUT *et al*., 2007; VERMESAN & HARRISON, 2009):

- *Military:* includes the military supply chain, resource management, and security requirements.
- *Disease and disaster networking:* the use of Things with sensors to monitor, predict, and coordinate responses to biological events.
- *Movement of goods and peoples:* e.g. baggage tracking at airports, border control, prison services, agricultural tracking.
- *ID cards:* using Things to identify all government issued IDs, such as e-passports, national ID cards, driver's licenses, or public transport passes.
- *Public safety:* using Things with sensors to track contaminated food, pharmaceuticals, or vaccine stocks
- *National environmental monitoring:* e.g. using Things with sensors to monitor national forests for poaching or oil reserves for contamination.

- *National infrastructure management and security:* smart buildings or highways or bridges capable of monitoring themselves for needed repairs or security breaches.

One primary characteristic of service provision to national governments is the enormity of up-front capital costs and resource requirements. For complex purposes such as military installations, network-enabled tags may cost $90 or even $5000 USD, as compared to their average cost of 10 cents (Transportation, 2006).

■ Policy implications of the IoT market

The above assessment of the variety of services comprising the IoT industry demonstrates that there is a diversity of public and private stakeholders invested in shaping the future of the Internet of Things. As with the early days of the Internet, steps must be taken to make the IoT market competitive, secure, and interoperable. Researchers highlight privacy, security, and standards as the primary policy issues that must be addressed (NGAI *et al.*, 2008) but the governance and prioritization of these issues differ depending on the end-user being addressed. At the level of individual consumers, privacy is highlighted while security issues take precedence for national governments. Although the problem of standards has the widest applicability, it is most salient in business-to-business services, where the complex coordination requirements of the global supply chain highlight the need for interoperability. The following discussion introduces the primary points of argument in the IoT policy arena and the additional discussion draws focus to a fourth area of policy in need of attention: the IoT as a public utility.

Standards

Many of the early niche applications of the IoT in the late 1990s were services for the use of national governments or marketed to individuals. In the former case, proprietary formats didn't pose a problem because the users were operating in closed military systems where logistics systems did not need to be interoperable unless the military planned to share them with another organization, which was unlikely (MATTERN & FLOERKEMEIER, 2010). In the latter case, applications for individual consumers were often

designed to do just one thing (open a garage door or unlock a car) and remotes were not expected to be universal. Today, as more consumers use multi-purpose Things that collect and transmit their personal data to provide services, they are increasingly invested in the use of non-proprietary and common data standards in order to be able to transport their data to another service provider if they should choose to do so. However, the greatest push for standards is at the firm level scale where the wide-scale adoption of IoT services in the global supply chain means that retailers must be able to coordinate with distributors and producers worldwide. Thus, the promotion and technological development of the Electronic Product Code as a global coding identification standard is primarily spearheaded by the EPCGlobal consortium of private sector firms (HALLER *et al*., 2009). The consequences of poor standardization may have less impact on service provision to city and national governments, where one vendor may develop a natural monopoly. In markets where end-users include individuals and firms, however, proprietary coding and hardware formats may create considerable barriers to entry for new firms or even incumbent firms, who are unable to compete for customers that are faced with the high switching costs of moving from one standard to another. Market building opportunities – critical to a growing industry – in the form of joint product ventures or technology transfers may also be lost.

Because the Things in the IoT are physical rather than virtual objects and consequently subject to real-world design constraints, there will always be a range of technological standards that play an important role in the Internet of Things. Differences in technical architecture are acceptable as long as a common interface can be developed in order to allow for data transfer and communication between devices without information loss. This approach has been successfully used in automated factories or automated homes where a plethora of different devices must be able to communicate with each other (HALLER *et al*., 2009). Interoperability in fact has at least three advantages over universal standards: 1) the most appropriate technological implementation can be used for a given application. 2) Using a common interface instead of a common form factor is more adaptable to future developments in a nascent field where new protocols and innovations continuously emerge. 3) Some variety in standards is better for security. On the other hand, the technical requirements for producing a common interface increase with every standard it has to accommodate and there are currently more than 500 industry standards for data exchange (Transportation, 2006), only a fraction of which can be accommodated by interoperability. RFID systems as currently implemented are a particular problem as they support a

number of different radio frequencies which are incompatible and various different encoding schemes for objects (VERMESAN & HARRISON, 2009), meaning some Things cannot be identified or may be misidentified. Furthermore, RFID operates by using unlicensed radio spectrum to identify Things, meaning radio frequencies which are not already assigned to another service such as mobile telephony. Because there is no international governing body to assign RFID frequencies, each country may set its own rules (NGAI *et al*., 2008) and there is no consistency as to which bands are unlicensed from country to country. Consequently, in order to be interoperable across international boundaries, Things must be capable of operating on multiple radio frequencies.

Privacy and security

Privacy and security share core themes as concerns within the IoT sphere, which are the prevention of unauthorized data access, transmission, loss, manipulation, or blockage. When services are provided to individual consumers, these issues are largely framed as privacy concerns connected to personal data protection and regulations concerning behavioral tracking and monitoring, although personal data security is also of concern. Because transactions for individual-level goods and services providers in the IoT largely involves commercial relationships between individuals and private sector firms, there is an emphasis on the prevention of data privacy violations that may occur as part of the service provider's attempt to strategically maximize firm performance in a highly competitive market. Research on privacy highlights consumer fears that retailers will use smart objects to develop detailed psychological profiles, even when the data collected is purely transactional (KUMAR, 2003). Furthermore, there is significant resistance against the idea that products can become Things without consumer knowledge or consent. A German study of consumers concerned about RFID privacy risks identified five primary concerns: unauthorized access, object tracking, retrieving social networks, technology paternalism, and making people responsible for objects (van LIESHOUT *et al*., 2007). Examples of the fourth and fifth categories included a shelf that sounds an alarm when products are returned to the wrong place and the use of sensors on trashcans to fine someone for littering.

In the European Union, which has been extremely proactive in its approach to the challenges and opportunities of the Future of the Internet, there exist a number of legal privacy directives with significance for service

providers in the IoT market. These include the Data Protection Directive (DPD), which addresses acceptable uses for personal data and requirements for privacy, the Electronic Commerce Directive (ECD), which requires explicit consumer consent for contractual terms and conditions between the consumer and the commercial service provider, and the Privacy and Electronic Communications Directive, which regulates the capture and usage of location-based data (SLETTEMEAAS, 2009).

When the end-user of IoT services is organizational – ie. a firm, city administration, or national government, the concerns about unauthorized data access, transmission, loss, manipulation, or blockage are framed as security breaches, or even terrorism. The consequences of such violations may have large-scale penalties ranging from loss of profit to lives lost. Here, the focus of concern does not emerge out of market interactions themselves but from unauthorized outsiders. However, market structure does play a role. Where markets are concentrated and a government user has limited vendor choices to provide an IoT solution to an infrastructure problem, such as traffic control or water resource management, breach of the system may be extremely devastating. The issue is further addressed below in consideration of the IoT as a public utility but becomes particularly significant when one considers that the IoT is especially vulnerable to security threats.

Total information security requires that a system be able to provide authorization, confidentiality, integrity, non-repudiation, and availability (ELOFF, ELOFF, DLAMINI & ZIELINSKI, 2009). This is not currently possible within the IoT. Things typically run autonomously, and consequently they are often unattended and may be open to physical manipulation or attack. Wireless and radio communications are not difficult to infiltrate, which means that it is relatively simple to illicitly track Things, damage sensors, capture data in transmission, or introduce false information into the data stream (ATZORI *et al*., 2010; CHRISTIN, REINHARDT, MOGRE, & STEINMETZ, 2009; NGAI *et al*., 2008). Because many Things, particularly passive ID tags, do not have large energy or computing resources it is difficult to integrate complex security authentication schemes into them, particularly where frequent response to an authentication server is required (ATZORI *et al*., 2010).

Currently, the dominant options for firms and government users with IoT security concerns are to implement physical protection schemes, to disable network-embedded devices (NEDs), to temporarily suspend NEDs, to create a set of aliases, or to adopt higher-cost advanced tags with limited cryptographic capabilities (ELOFF *et al*., 2009). Governments may also

choose to solve this problem via regulations imposing minimum security standards for Things, albeit at the cost of potentially significantly raising technological and capital barriers to market entry.

The IoT as a public utility

At the two scales of service provision involving governments, particularly at the level of the city administration, many of the most obvious IoT applications for infrastructure and resource management across various industrial sectors can be classified as public utilities. Examples include transportation management, efficient energy grids, or water resource monitoring. High capital and technical requirements pose significant barriers to entry in both these markets, which could lead to natural monopolies particularly as dominant firms achieve economies of scale or invest more heavily in expensive and long-term technical innovation. In this scenario, it is possible that in the absence of regulation to encourage competition, a paucity of providers may drive up prices for services provision.

Although this question is largely ignored in the IoT literature, a second, more critical issue is the possibility of lock-in. A private provider of public utilities facing high costs in these two markets may be incentivized to develop and adopt proprietary standards for, say, a traffic management system, deliberately raising switching costs to dissuade competition. Consequently, in the event of an equipment failure or critical parts shortage it is important to consider that there may be little hope of assistance from another vendor.

■ Concluding remarks

On the surface, the growth of data capture represents tremendous progress and opportunity, with applications that may improve every aspect of daily life from crime prevention to healthcare. The availability of cheap mass storage, combined with semantic identification schemes and the wide implementation of ubiquitous networked computing systems, may indeed solve the problem of the coming data tsunami. However, information is only as useful as our ability to extract value from it and the systems currently in place to capture, manage, and analyze data are grossly inadequate to the task. The coming convergence of Cloud Computing, The Semantic Web, and The Internet of Things represents an inflection point – a change so large

in magnitude that it could change the fundamentals of the information economy and data management markets on a worldwide scale. One might imagine a smart pillcase application, for example, which sends a mobile alert when a person picks up a medication at the drugstore that conflicts with the medications in his cabinet at home. The database containing his previous prescription and purchasing history with the pharmacy must be able to directly cross-reference a national database of known drug interactions and provide an instantaneous conclusion when the barcode on the new medication is scanned.

By offering an introduction that frames the Internet of Things as a critical and growing services market in the era of big data, this paper hopes to lure more academics, policymakers, and citizens to the discussion table. Outside of consumer privacy issues, the discussion agenda for standards (which impact both security and privacy) and competition policy within the IoT market is today still largely driven by two large private sector consortiums, EPCGlobal, a group of 90 firms promoting the use of the Electronic Product Code as a universal identification standard, and a corporate alliance called "IP for Smart Objects" (IPSO) that was founded in 2008 by Atmel, Cisco, Intel and SAP to promote the integration of internet protocols (IP) with smart objects.

Although there are significant limitations to the examination of nascent industries and analyses must necessarily make use of secondary, partial and forecasted data, it is becoming increasingly possible to establish economic and policy perspectives and goals with regards to guiding the future of this market. Given the number of industries involved and the sheer variety of applications, scale of services is used here as a simple tool by which to bound and classify the components of the IoT into four broad arenas which can be clearly tied to macro-level policy issues. Although many other strategies for division can be – and have been – employed in this regard, this is one approach that may offer an accessible lens for the future analysis of industrial organization or competitive dynamics in this area. Technology evolves exponentially but our ability to regulate it only moves incrementally. Here the challenge arises to encourage progress by adopting the long-view by acting early to establish standards for interoperability, active policy debates, and the promotion of competition.

References

ABI Research (2011): "Smart Cities: Municipal Networking, Communications, Traffic/Transportation, and Energy", Long Island, NY: ABI Research. http://abiresearch.com/research/1007213-Smart_Cities

ATZORI, L., IERA, A. & MORABITO, G. (2010): "The Internet of Things: A survey", *Computer Networks*, 54, 2787-2805.

BARNEY, J. B. (1986): "Types of Competition and the Theory of Strategy: Toward an Integrative Framework", *The Academy of Management Review*, 11(4), 791-800.

BERNERS-LEE, T., LASSILA, O. & HENDLER, J. (2001, May): "The Semantic Web", *Scientific American*, 284(5), 35-38.

CASAGRAS (2009): *RFID and the Inclusive Model for the Internet of Things*, Coordination And Support Action for Global RFID-Related Activities and Standardization (p. 88), UK: CASAGRAS.

CHAVES, L. W. & NOCHTA, Z. (2010): "Breakthrough Towards the Internet of Things", *Unique Radio Innovation for the 21st Century*, 25-38.

CHRISTIN, D., REINHARDT, A., MOGRE, P. S. & STEINMETZ, R. (2009): "Wireless Sensor Networks and the Internet of Things: Selected Challenges", *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze*, Hamburg, Germany.

ELOFF, J. H. P., ELOFF, M. M., DLAMINI, M. T., & ZIELINSKI, M. P. (2009). Internet of people, things and services-the convergence of security, trust and privacy. 3rd CompanionAble Workshop–IoPTS, Novotel (p. 8). Brussels.

FLEISCH, E. (2010): *What is the Internet of Things?: An Economic Perspective*, Auto-ID Labs White Paper WP-BIZAPP-053, ETH Zurich/University of St. Gallen.

HALLER, S., KARNOUSKOS, S. & SCHROTH, C. (2009): "The Internet of Things in an enterprise context", *Future Internet-FIS 2008*, 14-28.

International Telecommunications Union - ITU (2005): *The Internet of Things: Executive Summary*, ITU Internet Reports (p. 28), Geneva, Switzerland.

KORTUEM, G. & KAWSAR, F. (2010): "User Innovation for the Internet of Things", *Proceedings of the Workshop What can the Internet of Things do for the Citizen (CIoT) at The 8th International Conference on Pervasive Computing (Pervasive 2010)*, Helsinki, Finland.

KUMAR, R. (2003): "Interaction of RFID technology and public policy", *Wipro White Paper*, presented at the RFID Privacy Workshop, Boston, MA: Massachusetts Institute of Technology.

KUSHIDA, K., MURRAY, J. & ZYSMAN, J. (2012): "The Gathering Storm: Analyzing the Cloud Computing Ecosystem and Implications for Public Policy", *Communications & Strategies*, 85(1), 63-85.

van LIESHOUT, M., GROSSI, L., SPINELLI, G., HELMUS, S., KOOL, L., PENNINGS, L., STAP, R., *et al*. (2007): "RFID Technologies: Emerging Issues, Challenges and Policy Options", I. Maghiros, P. Rotter & M. v. Lieshout, Luxembourg, European Commission, Directorate-General Joint Research Centre, Institute for Prospective Technological Studies.

MATTERN, F. & FLOERKEMEIER, C. (2010): "From the Internet of Computers to the Internet of Things", *Informatik-Spektrum*, 33(2).

McWILLIAMS, A. & SMART, D. L. (1993): "Efficiency v. structure-conduct-performance: Implications for strategy research and practice", *Journal of Management*, 19(1), 63-78. doi:10.1016/0149-2063(93)90045-O

MORRISH, J. (2010, Oct. 29): "'Internet of Things' will grow to 16 billion connectable consumer devices by 2020", *Analysys Mason*. (Retrieved December 13, 2010). http://www.analysysmason.com/Research/Content/Reports/RRY04_Internet_of_Things_Oct2010/

NAVAJO, M. M., BALLESTEROS, I. L., SASSEN, A. M., D'ELIA, S., GOYET, M. M., SANTAELLA, J. & TSELENTIS, G. *et al*. (2009): *Draft Report of the Task Force on Interdisciplinary Research Activities Applicable to the Future Internet*, Information Society Directorate-General DG INFSO (pp. 3-5). Brussels, Belgium: European Commission.

NGAI, E. W. T., MOON, K. K., RIGGINS, F. J. & YI, C. Y. (2008): "RFID research: An academic literature review (1995-2005) and future research directions", *International Journal of Production Economics*, 112(2), 510-520.

SHEN, G., & LIU, B. (2010). Research on Application of Internet of Things in Electronic Commerce. Electronic Commerce and Security (ISECS), 2010 Third International Symposium on (pp. 13–16).

SLETTEMEAAS, D. (2009): "RFID – the 'Next Step' in Consumer-Product Relations or Orwellian Nightmare? Challenges for Research and Policy", *Journal of Consumer Policy*, 32(3), 219-244.

The Economist (2010, February 25): "A different game". http://www.economist.com/node/15557421

Transportation (2006): *Research Opportunities in Radio Frequency Identification Transportation Applications*.

VALHOULI, C. (2010): *The Internet of things: Networked objects and Smart Devices,* The Hammersmith Group Research Report, Hammersmith Group.

VERMESAN, O. & HARRISON, M. (2009): "Internet of Things Strategic Research Roadmap", European Commission-Information Society and Media DG.

WEBER, R. H. & WEBER, R. (2010): *Internet of Things: Legal Perspectives*, Springer.

WELBOURNE, E., BATTLE, L., COLE, G., GOULD, K., RECTOR, K., RAYMER, S. & BALAZINSKA, M. *et al*. (2009): "Building the internet of things using RFID: the RFID ecosystem experience", *Internet Computing, IEEE*, 13(3), 48-55.

YAN, B. & HUANG, G. (2009): "Application of RFID and Internet of Things in Monitoring and Anti-counterfeiting for Products", *Business and Information Management*, 2008. ISBIM'08. (Vol. 1, pp. 392-395).

ZOUGANELI, E. & SVINNSET, I. E. (2009): "Connected objects and the Internet of things – A paradigm shift", *PS'09,* International Conference on *Photonics in Switching* (pp. 1-4).