OPPORTUNITIES AND CHALLENGES OF THE INTERNET OF THINGS RELATED TO CONSUMER

Cristian Bogdan Onete[1], Doru Alexandru Pleșea[2] and Irina Albăstroiu[3]
[1)2) 3)]*Bucharest University of Economic Studies, Romania*
E-mail: cristian.onete@com.ase.ro; E-mail: pleseadoru@gmail.com;
E-mail: irina.albastroiu@com.ase.ro

Abstract
Nowadays, we have connected devices that meet our daily needs, "smart objects" that monitor our homes, cars, work environment and physical activity. These devices have gained crucial importance in our life. Hereby, we are entering into a new era, one in which the Internet of Thing (IoT) will replace the traditional Internet that we know today. Although IoT is expected to have a massive impact on individuals, it is still in its early days and many challenges lie ahead.
As consumers and users of connected smart devices, we focus to such an extent on the incredible functionality of IoT that we often forget to think about the possible implications for our private life and security. Many questions arise about the vulnerability of these devices, which are often installed outside of a traditional IT structure, without integrated security attributes. Thus, expected benefits must take into account the challenges especially related to privacy and security that IoT may pose. Data loss, malware, unauthorized access to personal data, intrusive use or illegal surveillance are risks that need to be addressed. Beyond compliance with legal and technical norms, there are important implications that IoT has on society, in general, and on consumer, in particular.
This paper is motivated by the above considerations, providing insight into challenges and opportunities of IoT related to consumer. Through reviewing the literature, the article firstly clarifies the significance of this concept and then discusses the applications of IoT related to individual consumer, highlighting those processes and activities that can be dramatically changed by IoT and the wide range of challenges faced by these networks.

Keywords: Internet of Things (IoT); connected smart devices; consumer; security; privacy.

JEL Classification: O33.

Introduction

Kevin Ashton, technology pioneer, cofounder and executive director of the Auto-ID Center at MIT (Massachusetts Institute of Technology), has coined and used the syntagma "*the Internet of Things" (IoT)* in a presentation he made in 1999 in order to describe the network connecting objects in the physical world to the Internet. Referring later to this concept,

Ashton (2009) affirmed that IoT has the potential to change the world, just as the Internet did or beyond.
Over time, the term has evolved into one that describes the IoT as a network of entities that are connected through any form of sensor, enabling these entities, to be located, identified, and even operated upon. IoT is the concept of basically connecting any device with an on and off switch to the Internet and/or to each other (Morgan, 2014). The IoT is a giant network of connected "things" (including people and any natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network).
Considering the existing studies in the relevant literature regarding the IoT, we note the following aspects: the majority of existing studies have investigated application of the IoT from firm or government perspectives (Schlick, Ferber and Hupp, 2013; Weber, 2010; Zhao et al., 2013), a multitude of papers focuses on technical aspects, presenting the IoT design, architecture and implementation (Bing, 2014; Gubbi et al., 2013; Weyrich and Ebert, 2016) and only few studies investigated IoT's impact on consumer (Gao and Bai, 2014; Kim and Shin, 2015; Shin and Park, 2017). Given the complexity and heterogeneity of IoT, it is required to examine the matter from consumer point of view that encompasses social and user-related factors. Such as all new developments, there is potential for both increased opportunities and risks for individual users. Under these circumstances, this paper aims to present such an approach by detailing some of the benefits of IoT related to consumer and endangerment that are part of the IoT phenomenon.

1. Current state of knowledge concerning Internet of Things

Internet of Things (sometimes called "*the Cloud of Things*") generally refers to "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (ITU, 2012, p.2).
The term "*Internet of Everything*" is sometimes used referring to an almost limitless number of connections that could be possible between people, systems, devices and industry. Also, European Commission (2010) addressed the Internet of Things as a *"great Internet"* that will contain all items daily used, from home appliances, furniture, clothes, mobile phones, coffee makers, washing machines, headphones, lamps, wearable devices, food, medicines, vehicles, roads, buildings etc.; all these can be spotted, identified, addressed and controlled via the Internet.
The Internet of Things is already a daily presence in our lives: in our homes where smart counters coordinate and save electricity consumption; the Internet connection in our cars; the OnStar system (US) or eCall (EU) system that triggers an automatic response in case of accidents, follows the car if it's stolen or provides technical assistance as required; on our bodies as an insert in the smart shirts etc. "Smart" or "intelligent" is a term increasingly adopted to describe things or processes that have the ability to compute, connect and communicate to differentiate from the machines and equipment working in isolation.
Nowadays, broadband Internet is become more widely available and more devices are being created with Wi-Fi capabilities and sensors, creating the premises for the IoT. Also, the tremendous drop of prices for database storage devices required for the collection, storage and processing of trillions of bits has an important role in creating the premises for IoT.
Likewise, there is a confluence of several *devices and applications* that have transformed an area of "science fiction" into reality, such as: barcodes, RFID (Radio Frequency

Identification) devices (tags), NFC (Near Field Communication), SaaS (Software-as-a-Service), active sensors, IPv6 Internet protocol which enables the Internet address to be available in any object that has software stored: toothbrush, coffee machine, refrigerator, dishwasher etc.

Another common related term, *M2M (Machine-to-Machine)* is a technology which enables devices of the same type to communicate. To allow these communications, devices had to be connected to each other and to larger systems using standard protocols like Wi-Fi, Bluetooth and Zigbee. M2M communications allows sensors in one place to communicate with control systems for an automated response. Industrial processes have widened M2M further to include connections with human interfaces, sometimes referred to as the *"Industrial Internet of Things" (IIoT).* The IoT has an impact on end consumers, while the IIoT has an impact on industries like manufacturing, aviation, agriculture, oil & gas, transportation, energy etc. While the industrial IoT got an earlier start, the consumer IoT is not far behind.

For every person living on earth**,** there will be at least 2, maybe even 6 connected "things" by 2020. Ericsson's mobility report (2016) forecasts around 29 Billion connected devices by 2021. 18 billion of these will be related to IoT (in this forecast a connected device is a physical object that has an IP stack, enabling two-way communication over a network interface). Between 2016 and 2022, IoT devices are expected to increase at a CAGR (compound annual growth rate) of 21 percent. In the figure no. 1, illustrating all connected devices, IoT is divided into short-range segment (consists of devices connected by unlicensed radio with a typical range of up to around 100 meters - such as Wi-Fi, Bluetooth and ZigBee - and devices connected over fixed line local area connections) and wide-area segments (consists of devices using cellular connections (3GPP-based - 3rd Generation Partnership Project - a collaboration between groups of telecommunications associations) as well as unlicensed low-power technologies (such as Sigfox, LoRa and Ingenu)).

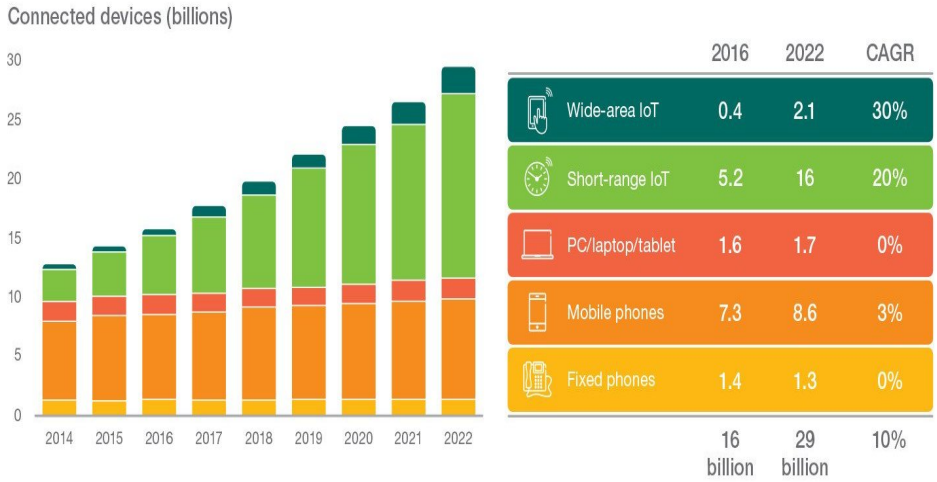

Figure no. 1: Forecast regarding connected devices
Source: Ericsson, 2016, p.33

Determinants of the proliferation of IoT are appearance and development of the following technologies or applications (Crânganu, Luchian and Breaban, 2015):
- *Artificial Intelligence (AI)* - the goal of artificial intelligence is to operate with large amounts of unstructured data - such as those produced by IoT devices - and to make actionable decisions related to these data. In short, AI is the technology that gives meaning to data and engender meaningful instruction, such as commands for IoT devices to perform specific actions.
- *Machine Learning* - is the umbrella term for algorithms that, automatically or with a human support, identify patterns and determine what type of behavior of IoT devices tends to create the desired results. Based on learning algorithms, computers can act without being explicitly programmed. In the last decade, machine learning technology has given to us, among other, cars without drivers, speech recognition, effective search over the Internet and an extensive understanding of the human genome.
- *Data Mining* - is the analytical process of exploration of the large databases - Big Data - for searching and finding consistent patterns and/or systematic relationships between different variables, followed by application of detected patterns to new datasets.
The Internet of Things appears as a mix of household applications and intelligent industrial components. From an *application/industry* point of view, Lueth (2014) has developed a market segmentation that is suitable for understanding the IoT ecosystem (figure no. 2).

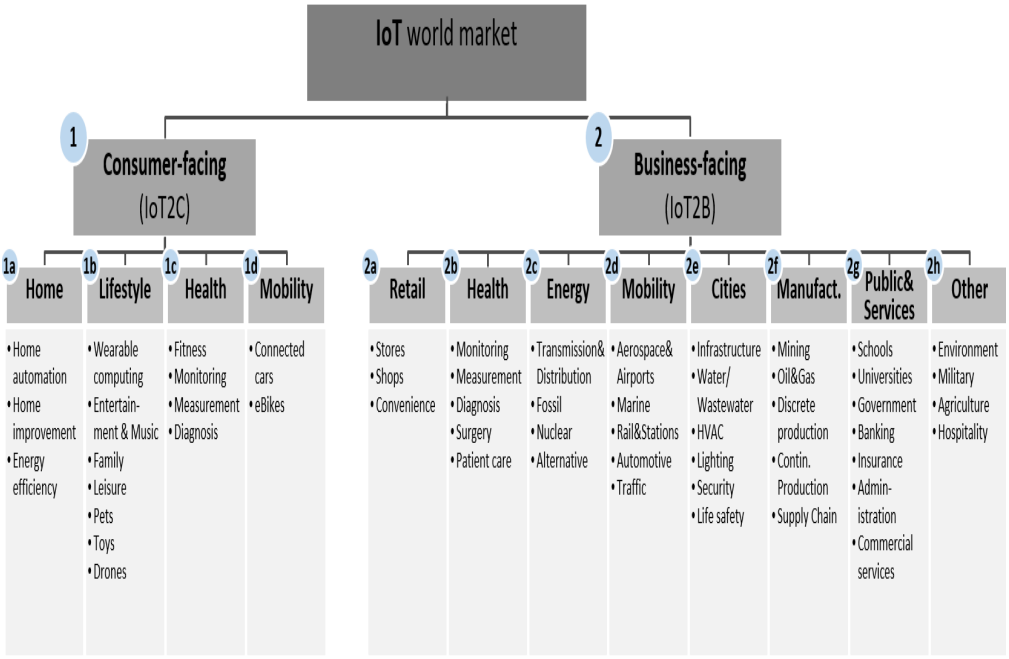

Figure no. 2: IoT market segments
Source: Lueth, 2014

Also, the McKinsey Global Institute (2015) describes the broad range of potential applications in terms of "settings" where IoT is expected to create value for industry and users in environments such as homes, offices, factories, worksites (mining, oil and gas, and

construction), retail environments, cities,vehicles, and the outdoors (including autonomous vehicles (outside urban locations), and flight navigation, real-time routing, connected navigation, shipment tracking). It is also included a ″human" setting for systems/devices that attach to the human body and enable to monitor and maintain human health and wellness.

2. Main consumer applications of the Internet of Things and potential benefits

The IoT technologies apply or will apply soon in a myriad of areas. Currently, major consumer applications of the Internet of Things include (Consumers International, 2016; McKinsey Global Institute, 2015; Savu, Tomescu and Băjenaru, 2017):

- *Wireless wearables and portable devices* track and record physical activity like exercise, eating, sleeping or behaviour like reading, commuting etc. Whether it is Jawbone Up, Fitbit Flex or Apple SmartWatch, wearable devices constitute the majority of the Internet of Things applications for consumers. As indicated by recent studies (Accenture, 2014), is more likely for consumers to see value in health & fitness wearable technology.
- *Smart home/home automation* is a concept referring to the connectivity within the housing. A typical house is now a lot of devices that are ready for automation by IoT, such as thermostats, smoke detectors, lamps, windows, doors, locks and more. Some devices are related with the entertainment area (e.g., Smart TV), others are related with lighting, heating, access and security. *Home applications* will dominate the consumer IoT market in the next years. Among the best known organizations involved in the field are included Nest, Apple, Philips and Belkin.
- *Intelligent health system and connected medical devices* have enormous potential for the welfare of people in general. New types of instruments for real-time monitoring health and for improve medical decisions based on large data sets of the patient are some of the expected benefits. IoT will have the greatest impact on the way diseases are diagnosed and treated. Basically, through IoT healthcare can be more accessible. For example, the IoT devices allow the rapidly and early detection of abnormalities in the body, followed by a diagnosis and a proper treatment. Medical institutions could release drugs more efficiently by analyzing feedback from IoT devices. These devices can be of various sizes, implanted in the human body or monitoring the patient in his living environment. In other words, IoT devices can be used to monitor patient health and transmit all the information necessary for medical staff in order to provide a more accurate and personalized care.
- *Connected cars and self-driving cars* will change the world. Currently, the driver must manually configure devices and their functions, from radio to heating/air conditioning, navigation and others. IoT devices embedded in cars will release drivers of worries and configure many of these current applications. Whether is about self-driving cars or assisted drivers, connection with other machines, mapping services or traffic control will play an important role in the future. The next generation of entertainment systems on board of the vehicle and remote monitoring are also interesting concepts. A large number of manufacturers, which plays an important role such as Google, Microsoft and Apple have developed platforms dedicated to connected vehicles.

Also, s*mart city* solutions promise to meet the problems faced by city dwellers. These problems include traffic congestion, noise, pollution and urban insecurity. Data produced by smart cities will be processed and analyzed to determine how to improve quality of life in each city, from the management of financial resources to the fight against crime. The biggest advantage of using IoT technology are savings to the municipal budgets. Other

areas where smart cities will achieve cost reductions, are the consumption of water and energy, management of domestic and industrial waste, public safety (firefighters, police officers, rescue, traffic controllers) or intelligent buildings (e.g., Seattle is a world leader in its efforts to build buildings with low energy consumption).
The capabilities and applications of Internet of Things primarily involves the following types of benefits for individual consumers:
- *Convenience and efficiency* - the disparate nature of providers, regulators and systems makes many daily consumer experiences inconvenient, time consuming and inefficient, meanwhile automating tasks such as reading energy meters or checking use by dates of food and medicines or supplies being reordered based on needs can save time and money (Sîrbu. Săseanu, Ghiță, 2015).
- *Enhanced experience* - more interconnections between devices and aggregation of information could increase user convenience, but a step on from convenience is the idea that consumer experiences could be enhanced or made more enjoyable by Internet of Things technology. IoT can generate a dramatic increase in the quality of life.
- *Decision making support* - even some critical information, found on time and shared with right people can lead to more informed decisions, daily processes optimization, identify new opportunities, and predict behavior and enabling consumers to act themselves or outsource that task to services based on these patterns of behavior and use.

3. Challenges faced by the Internet of Things
IoT implementation on a global scale, affecting billions of people and devices has not only benefits. In this new era of connectedness, some issues seem essential:
- *Security and data privacy* - the problem lies in the fact that most of the equipment used every day is marketed without taken into account isuues like *confidentiality* or *data protection*. Users generally assume that businesses and legislators have taken these risks into account and solved them. Or, if customers do not understand the importance of data confidentiality and do not ask for it, manufacturers do not deal with it, knowing that purchasing decisions are not based on this criterion and compatibility, price or design issues are more important. Moreover, the problem has been aggravated by the fact that many of us have accepted, voluntarily or with a bent, concessions in respecting our privacy and our security to get what we consider more precious, namely, access to the cutting-edge technology. Often, Internet connections are vulnerable, regardless of their type (WiFi, Bluetooth, cellular, satellite or microwave) or how they are connected to the "cloud" or other servers and services set to search, process or receive data from an IoT application. These vulnerabilities may allow a hacker to intercept, tamper with, or block communications, and in some cases to take control of a physical device. For instance, children's video surveillance systems can reassure parents by allowing to watch their children at any distance from smartphone. But if the system is not protected, they can expose their little ones to danger. Also, recent experiences have shown that it is possible to hijack a vehicle on its way through its entertainment system and to disable the accelerator. In the same way, an unauthorized person will be able to reset the thermostat to a high temperature so that the boiler works nonstop or to turn off the thermostat so that all the radiators are frozen and broken while we are on holiday. Issues become even more serious if we talk about health and vulnerability of medical devices, since it is possible to remotely manipulate the infusion pumps of some drugs (e.g., morphine, antibiotics or those used in chemotherapy), defibrillators, scanners or X-ray machines.

- *Tolerance to errors* - The world of things is more dynamic and mobile than the world of computers, with contexts that change rapidly and in unexpected ways. However, users want to rely on things that work properly. Structuring the Internet of Things in a robust and reliable mode requires multiple level redundancy and the ability to automatically adapt to changing conditions.
- *Scalability* - the Internet of Things has a potential for global application beyond the conventional Internet. Things, however, mainly cooperate in a local environment. So, basic functionalities such as communication and service discovery should work as efficiently in both environments (Savu, Tomescu and Băjenaru, 2017).
- *Interoperability* - smart objects can be subject to very different conditions, such as the available energy and the bandwidth required for communications. However, in order to facilitate communication and cooperation, common practices and standards are necessary (Savu, Tomescu and Băjenaru, 2017).
- *Managing large data volume* - all major technology companies are concerned about and allocate significant amounts of money for managing the data that each Internet user generates. We can refer here on analyzing consumer habits, leisure timelines, health monitoring, financial investments, virtually any detail in user life can be taken as data that can be interpreted. Managing the volume of these data is still a challenge. In order to take advantage of the disparate data, it must be possible for service providers to extract some generalized conclusions as a result of analyzing and interpreting data. However, generating useful information from raw data from sensors that can trigger further action is not a slight action.

As indicated by recent studies (Accenture, 2014), price, security and privacy are concerns of the consumers, but companies can overcome them by demonstrating value of connected smart devices to consumers. Better educating consumers will be an important factor in growing this market.

Conclusions

The Internet of Things designates billions of connected smart devices changing current data volumes about our lifestyle, our work habits, and our relaxation practices. It is supposed that these devices will make our businesses more productive and our lives simpler, healthier and smarter, but there is often a reverse. Connectivity of IoT devices is simultaneously a prerequisite and an Achilles' heel. Communication networks that allow these types of devices to exchange information are not coded or protected. It's like leaving open the door of your house. The interior of our homes, our cars, our pets and even our refrigerators are accessible with one click.

For increased security in IoT, we need to start by creating secure technologies with effective real-time privacy controls. Implementing IoT applications requires the careful knowledge about the most critical issues concerning the privacy protection and secure transmission of data generated by the connected objects through IP networks.

References

Accenture, 2014. *The Internet of Things: The Future of Consumer Adoption*. [online] Accenture. Available at: <https://www.accenture.com/t20150624T211456__w__/us-

en/_acnmedia/Accenture/ConversionAssets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf> [Accessed 21 March 2017].

Ashton, K., 2009. That "Internet of Things" thing. *RFID Journal*, 22(7), pp.97-114.

Bing, X., 2014. Key IoT Technology and Application Research. *Applied Mechanics and Materials*, 543, pp.3411-3414.

Consumers International, 2016. *Connection and Protection in the Digital Age. The Internet of Things and Challenges for Consumer Protection*. London: Consumers International.

Crânganu, C., Luchian H. and Breaban M.E., 2015. *Artificial Intelligent Approaches in Petroleum Geosciences*. New York: Springer.

Ericsson, 2016. *Mobility Report - On the Pulse of the Networked Society*. [online] Ericsson. Available at: <https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf> [Accessed 21 March 2017].

European Commission, 2010. *Bringing European Values to the Internet of Things*. [online] Neelie Kroes at 2nd Annual Internet of Things Conference - Reference: EC SPEECH/10/279. Available at: <http://europa.eu/rapid/press-release_SPEECH-10-279_en.htm> [Accesed 19 March 2017].

International Telecommunication Union (ITU), 2012. *Overview of the Internet of Things - Recommendation ITU-T Y.2060*. [online] ITU. Available at: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060> [Accessed 19 March 2017].

Gao, L. and Bai, X., 2014. A Unified Perspective on the Factors Influencing Consumer Acceptance of Internet of Things Technology. *Asia Pacific Journal of Marketing and Logistics*, 26(2), pp.211-231.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems*, 29(7), pp.1645-1660.

Kim, K. and Shin, D., 2015. An Acceptance Model for Smart Watches. *Internet Research*, 25(4), pp.527-541.

Lueth, K.L., 2014. *IoT market segments – Biggest Opportunities in Industrial Manufacturing*. [online] IoT Analytics. Available at: <https://iot-analytics.com/iot-market-segments-analysis/> [Accessed 19 March 2017].

McKinsey Global Institute, 2015. *The Internet of Things: Mapping the Value Beyond the Hype*. [online] McKinsey Global Institute. Available at: <http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world> [Accessed 19 March 2017].

Morgan, J., 2014. *A Simple Explanation of 'The Internet of Things'*. [online] Forbes. Available at: <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7733f5821d09> [Accessed 19 March 2017].

Savu, D., Tomescu, M. and Băjenaru, L., 2017. Internetul lucrurilor – o nouă paradigmă a conectării în Internet. *Revista Română de Informatică şi Automatică,* 27(1), pp.5-14.

Schlick, J., Ferber, S. and Hupp, J., 2013. *IoT Applications – Value Creation for Industry*. Aalborg: River Publisher.

Shin, D.-H. and Park, Y.J., 2017. Understanding the Internet of Things Ecosystem: Multi-Level Analysis of Users, Society and Ecology. *Digital Policy, Regulation and Governance*, 19(1), pp.77-100.

Sîrbu, M.O., Săseanu, A.S. and Ghiță, S.I., 2015. Consumers' perception on the use of innovative technologies in creating store atmosphere. *Amfiteatru Economic*, 17(39), pp. 567-582.

Weber, R.H. 2010. Internet of Things: New Security and Privacy Challenges. *Computer Law & Security Review*, 26(1), pp.23-30.

Weyrich, M. and Ebert, C., 2016. Reference Architectures for the Internet of Things. *IEEE Software*, 33(1), pp.112–116.

Zhao, J., Zheng, X., Dong, R. and Shao, G., 2013. The Planning, Construction, and Management Toward Sustainable Cities in China Needs the Environmental Internet of Things. *International Journal of Sustainable Development & World Ecology*, 2(2), pp.1-4.