Advances in Social Science, Education and Humanities Research (ASSEHR), volume 252
3rd International Conference on Judicial, Administrative and Humanitarian Problems
of State Structures and Economic Subjects (JAHP 2018)

Internet of Things in Digital Marketing and Data Security Concerns

Nadezhda Arkhipova
Russian State University for Humanities
Moscow, Russia

Madina Gurieva
Department of Marketing and Advertising
Russian State University for Humanities
Moscow, Russia
E-mail: gurieva.m@rggu.ru

***Abstract*—The article analyzes certain aspects of the Internet of Things (IoT), the role it plays in industrial and consumer spheres, and the implications of IoT for marketers. Numerous applications of IoT are changing the everyday life of consumers and also provide huge amounts of data available for marketing analysis. However, the possibilities of IoT are accompanied by certain risks including an unauthorized access to and the use of personal information. New regulation concerning data protection is coming into force in Europe, which will concern not only European companies.**

Keywords—digital marketing; Internet of Things; Industrial Internet of Things; Consumer Internet of Things; data security

I. INTRODUCTION

IoT (or the Internet of Things) is one of the new developments of digital transformation, probably the most influential one, the consequences of which are not yet completely clear. Even the explanation of what the IoT is can differ. The Gartner IT glossary describes the IoT as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment", meanwhile Cisco defines it as "the convergence of IT networks, operational technology (OT), and smart objects", and also as the moment in time when the number of connected devices exceeded the number of people with Internet access [1]. According to Cisco, this happened between 2008 and 2009, and today the estimates show approximately 28 billion connected devices with a realistic forecast of 50 billion by 2020. Even from the quantitative point of view, the impact of this phenomenon can be huge and omnipresent.

II. INDUSTRIAL IOT

IoT today is present in so many spheres of life that the term itself is becoming too wide. So, it is often divided into Industrial and Consumer IoT segments. These two are quite different but we can also see some convergence. The Industrial IoT is the technology and applications as they are used in industries such as manufacturing, logistics, healthcare, agriculture, automotive and industrial markets and basically in almost every other industry. The difference from Consumer IoT mainly lies in the types of devices/applications and the technologies that power them. The industrial devices are extremely useful in tracking equipment and assets in general. They can also offer huge savings on maintenance and replacement costs in the spheres where technical condition of devices is crucial and regular check-ups are excessively expensive, complicated and sometimes not sufficient to ensure proper operation. For example, the wind turbines that are becoming an increasingly important source of energy in Europe, had been previously checked on a time-schedule basis which was expensive and not efficient enough. The Industrial IoT sensors that are installed now permit maintenance of the blades of such turbines on a predicting condition-monitoring basis. Sensors that measure the behavior of equipment (vibration, material strength, etc) can transmit the information to the Internet, where it is analyzed it and the decision to replace a part of mechanism can be taken weeks or months earlier than it becomes too dangerous to operate it. For the equipment designed to last decades such a system of continuous monitoring in real time can mean substantial efficiency in terms of economy and safety. Smart cities are another important example of Industrial IoT use whereby this technology ensures that the assets and resources are managed as efficiently as possible in terms of economic, social and environmental sustainability. The city of Barcelona, for example, is employing the IoT solutions to face several of the city issues such as traffic (using dynamically managed street lights, Wi-Fi on public transport, parking space sensors helping to reduce traffic in city center where up to 40 per cent of all traffic can be generated by cars looking for a parking space), lighting, pollution (using sensors which in real-time show levels of pollutions in urban areas), waste management. Moscow is also utilizing some of these possibilities, i.e. public transport Wi-Fi, parking application for smartphones, public transportation applications like Yandex.Transport that shows routes, stops and vehicles location in real time. Overall, one of the main possibilities provided by the Industrial IoT is the transition from checking the situation and reacting to the already existing problems to the real-time monitoring of the situation, predicting problems and being proactive.

III. CONSUMER IOT

The Consumer IoT or CIoT refers to the Internet of Things in the context of consumer applications, use cases

and devices. These are extremely important from the digital marketing point of view as they offer unprecedented possibilities in terms of brand loyalty and, what is more important, data collection and analysis. Consumer Internet of Things applications range from very simple and inexpensive ones such as personal fitness devices to high-end smart home automation applications. The most popular use cases from consumer's interest point of view are connected and smart TV, along with connected streaming devices, connected car applications, wearables (including health tracking possibilities), home control devices and systems in general (Smart home), Internet-enabled voice-command systems, IoT-enabled appliances, virtual reality headsets and games and all types of smart watches. Buying interest in smart glasses is also on the rise.

The possibility CIoT gives consumer is a way to overcome distances. Many of the consumers are just starting to comprehend the extent of changes. Previously we used to have remote control appliances with very limited operating range so one had to be physically present within certain distance from the device to operate it using the remote controls. Now there are remote appliances and wireless devices connected to the Internet and allowing new levels of comfort and security. Distance is not a constraint and the consumers are increasingly able to switch on or operate any linked device from any part of the world in real time as if they were physically present locally. Besides giving complete flexibility of operation it also provides added safety, avoiding accidents by switching off certain equipment remotely in case of accidents. It has also proven to be very useful in saving energy. The Smart Home systems, for example, include remote household appliances control (including fridges, cookers, washing machines), room temperature control (air conditioners), entertainment systems operation and home security. Intrusions and unauthorized entries can now be monitored, and many consumers are interested in buying connected home surveillance cameras for this purpose.

Personal healthcare is another major area where the benefits of CIoT are obvious. Numerous wearables, i.e. blood pressure and heart rate bands, blood sugar monitors, wireless insulin pumps, activity and wellness monitors and many other devices which are powered by IoT connect directly to the healthcare system or to the caregiver getting timely assistance when something is not right. These types of smart things are especially important when the patients are small children in need of parent's supervision. For example, wireless connected glucometers and insulin pumps are crucial for socialization and educational inclusion of the children with type 1 diabetes in Russia allowing them to go to regular kindergartens or schools with the parent being able to monitor the situation. Other areas of use in the healthcare industry include patient surveillance, care of the elderly and the disabled, fall detection or tracking elderly people with mental or memory disorders. All of these are becoming increasingly popular with the consumers and the trend will obviously continue. In Russia, for example, with the planned retirement age increase from 55-60 years to 63-65 years the problem of caring for the elderly will unavoidably become more vital. Previously it was not uncommon for people at 55-60 to retire and take care of their elderly parents. If they are to work for additional 5-8 years in the future, then the gadgets and appliances helping to monitor the state of health and whereabouts of the elderly person will be in demand. Of course, the IoT in healthcare is not limited only to the wearable devices. It also includes electronic recordkeeping or, for example, connected medical equipment like MRI.

The direct impact of IoT on marketing activities will express itself not only in what products (connected gadgets, devices, etc.) will be in demand but also in the change of consumer expectations, in new possibilities of inventory tracking, mobile purchasing and in analytics of consumer choices.

The consumers are expecting a new level of convenience. The need of convenience is not new however the meaning of client's convenience has shifted from a comfortable distance to the grocery store and nice atmosphere and assortment in-store to a world where the products the person needs appear at his/her door literally as soon as possible. The modern consumer is used to on-demand food, music, entertainment, everything. On the marketer's side these expectations require a whole new level of organization and supply chain management but in return he can get increased customer loyalty both to manufacturer's brand and retailer's brand. The Amazon.com was one of the first companies to introduce this new approach to customer service – the Amazon Dash button which is a small wireless device that can be installed anywhere in the house. It's free (the $4.99 paid for each button are credited back to client's account after the first order) and can be obtained for any popular brand of customer's choice. The customer only has to set up buttons using the Amazon App and select the specific products of the brand that he wants to order when he presses the button. After that, any time the button is pressed the device will use Wi-Fi to instantly order pre-selected items from Amazon and they will be delivered the next day. In addition, Amazon.com introduced virtual dash buttons and a Dash Wand that is voice operated and can order products, search the Internet or operate smart things at home receiving voice commands. The reviews for the Wand are not all the highest but the direction and the future of customer service are obvious.

IoT also opens new possibilities for data collection and analytics. The possibility to obtain and process huge amounts of consumer information and to create an offer that would be completely adapted for their specific needs is rather a new development in digital marketing, but it has already proved its efficiency. Contemporary instruments of marketing analytics, the big data can accumulate and process endless amount information concerning the client, his demographic and behavioral characteristics, his relationship with the brand, the way he makes his purchase decisions, his previous queries and searches, competing brands offers he had seen, etc. The information is collected online and offline and the client expects that the company knows and remembers his preferences and is prepared to offer the expected level of service when and where he needs it. What the majority of the customers do not realize is the amount of additional

information collected by the smart things surrounding him at home, in the streets and in the office. For example, the Edge – Amsterdam office building of Deloitte consulting firm, often called possibly the smartest office space ever constructed – knows a lot of things about each person working inside. It knows where they live, what car they drive, who they're meeting on any given day and how much sugar they put in coffee. From the minute a person wakes up, he's connected. The app checks his schedule, and the building recognizes his car when he arrives and directs to a parking spot and so on. The Edge is full of sensors – there are about 30,000 of them and this helps to accumulate huge quantities of data.

IV. Risks and Vulnerabilities of IoT and Security Problems

As almost any new technological development, IoT brings not only new possibilities and level of comfort but new risks and vulnerabilities. They could be roughly divided into three groups or types of risks. The first two of them are closely connected – these are the risks concerning the huge amount of connected IoT elements (smart things, sensors), their vulnerability to physical (sensors and other devices can be positioned in various places, where it is very hard to ensure their protection) and, more importantly, cyber-attacks, on the one hand, and the risk to person's health, property and safety resulting from such attacks [2]. Many experts point out that the popularity of IoT and the practically endless advantages result in new IoT products manufacturers' wish to fast-track them into use, get the benefits of cost-saving efficiencies that the IoT can deliver. But in an attempt to make everything internet enabled, security can sometimes be overlooked. Many consumers are prepared to protect their desktops and laptops from cyber-attacks by installing proper antivirus protection software. At the same time, people are often overlooking numerous smart gadgets and appliances that are connected and as such are also vulnerable. It does not only concern the Consumer IoT but also internet-connected critical national infrastructure from power stations to transport to finance to medical devices and healthcare, which are at increasing risk from cyber-attacks.

The global energy sector has already fallen victim to several successful cyber-attacks. In 2010, one of the first known large-scale incidents, Stuxnet, targeted an Iranian nuclear facility. Then in 2016, malware known as Industroyer was used to strike Ukraine's national grid. It was the first ever known malware specifically designed to attack electrical grids and the fourth malware publicly revealed to target industrial control systems. The risk in this sphere is elevated because utilities are often running old supervisory control and data acquisition (SCADA) systems, which had never been designed to be connected to the Internet in the first place. IoT programs layered on top in an attempt to increase efficiency the security challenge only aggravate the situation.

There are numerous examples of vulnerable systems and devices in healthcare. For example, last year in the US it was discovered that 465,000 pacemakers needed a firmware update to close security holes. There were also reports that hackers had entered US hospital networks via insecure medical devices, including MRI scanners and X-Ray machines, accessed patients' medical records, and changed drug doses remotely. Healthcare systems pose a particular challenge to security specialists, because replacing old technology is not always possible. The medical equipment machines are often extremely expensive and are used for many years before being replaced, so old systems are combined with local hospital networks. Such devices cannot be redesigned, patched, or upgraded quickly and easily. This is because medical devices need to be serviced by the manufacturer and the lack the data backup and restore functions that are usually performed when recovering from malware attacks. So, according to experts, keeping operating systems and applications continuously patched and upgraded is essential, especially in an environment where hardware upgrades may not be possible for budgetary reasons. The cyber security expenses in the IoT sphere worldwide are expected to reach $1.5 billion in 2018, a 28 per cent increase from 2017 and there is also a forecast of $3.1 billion IoT security expenses in 2021 [3].

The third type of IoT risks is connected with the data collected by the systems, unauthorized access to this data and/or unauthorized use thereof. Marketers have to view this risk seriously because data collection and analysis has served as a basis for digital marketing possibilities as mentioned above. The consumers are just starting to understand the amount of information about their personalities, lifestyles and behavior available to companies. And while people are used to getting personalized offers, they are also scared at the thought that all this information can be used by unknown companies and people and influence their lives in unforeseeable ways. The information collected for example by an IoT wearable such as wellness watch or bracelet could be analyzed, interpreted and used by potential employers or insurance companies. Weight, health issues, exercise regimen information might become available to them and some unpleasant conclusions followed by specific decisions made. The consumers are becoming increasingly careful about data protection. They demand more control over what information about them is collected, how it is stored and used.

The lawmakers are increasingly concerned by the problem of cyber privacy and new regulatory frameworks are created. In May 2018, the European General Data Protection Regulation, also known as GDPR, became enforceable. The Regulation concerns all companies that process personal data of EU citizens, no matter where these companies or 'data processors' are. So, it also applies for organizations outside of the EU, Russia for example.

The GDPR establishes the main principles of personal data processing. Personal data should be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing

for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')[4].

Obviously, any company involved in IoT projects whereby personal data is involved has to examine their practices as in IoT there are many components that can pose a security risk and are often not seen or understood well enough. Recent research, conducted by 25 data protection regulators worldwide among others showed that, "59 percent of devices failed to adequately explain to customers how their personal information was collected, used and disclosed, 68 percent failed to properly explain how information was stored and 72 percent didn't explain consumers how to delete their data off the device".

Another new legal framework concerning IoT is being created in Europe: the ePrivacy Regulation. This regulation concerns all electronic communications, clearly including the Internet of Things. The document is also expected to provide for specific safeguards in machine-to-machine communications in particular sectors.

V. CONCLUSION

Therefore the regulation of the IoT sphere is bound to change drastically in the near future. The changes will entail increase in data security expenses but also higher level of personal data protection the customers are seeking which should not be ignored by the marketers. Rather than looking at new regulation as an obstacle, marketers should seize the opportunity to ensure their marketing practices comply to the high standards. So while the marketers still need to provide their customers with an experience that is informed by thorough understanding of their behavior's and preferences, it is also important to assure the customers that their personal data is processed in a safe and responsible manner.

REFERENCES

[1] Gartner IT Glossary [Electronic Resource] - The URL: http://www.gartner.com/it-glossary/internet-of-things/

[2] The Internet of Things. Reduce Security Risks with Automated Policies. 2015 [Electronic Resource] - The URL: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf

[3] Chris Middleton, Gartner: IoT security spend hitting $1.5 billion – but strategy poor, in Internet of Business, March 18, 2018. [Electronic resource] – The URL: https://internetofbusiness.com/gartner-iot-security-spend-hitting-1-5-billion-but-strategy-poor/

[4] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Electronic resource] – https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3265-1-1.