DE GRUYTER OPEN

DOI 10.2478/vjes-2018-0015

IoT and EU Law – E-Human Security

Alexandru TĂBUȘCĂ
Silvia-Maria TĂBUȘCĂ
Gabriel GARAIS
Romanian-American University, Romania
tabusca.alexandru@profesor.rau.ro

Abstract

The new realities brought on us by the growing usage of IoT devices should be paralleled by new sets of paradigms and regulations, in order to not only accomplish the raise in the living standards of people but also to increase their level of human security. The IoT devices, as well as, in whole, the virtually completely internet connected society we live in today, need strong and clear rules and regulations, need laws that can help maintain and improve the cyber-security level. While being able to electronically track one's children, by a multitude of IoT and other electronic devices, it is a great and useful feature we have to take into account that the same information, now shared over the internet, might also get into the wrong hands and lead to unpleasant or even dangerous situations.

Keywords: *IoT, internet of things, EU single digital market, cyber-security, EU law, human security*

JEL Classification: O33

Introduction

The IoT paradigm brings about new and innovative ways for the people to take advantage of the present-day technology but, in the same time, it brings new legal issues that have to be tackled in order for the society to respect the private information, to assure one's privacy and, in whole, to increase the level of human security by means of the e-human security sub-chapter.

The business models today adapt quite quickly and quite a number of companies, including well established and flagship names of all industries, involve the technology within their relations with the customers. More and more sensors and beacons are available for the IoT developers and implementers, more and more possibilities to keep track of different things related to a customer. This new reality transforms the classical "selling" businesses into some sort of "service offering" businesses. Instead of selling a certain product, more and more companies are broadening their horizon and sell the same product filled with different sensors which can provide lots of information as per a service-type of

usage. This new approach changes the business model since the products are actually no longer paid once and the transaction is finished, but the product is now just a part of a larger contract between the company and the client, a contract that implies a continuous service offered by the company, based on the use of different IoT devices.

On the other hand, all these new IoT devices might prove very dangerous, if the security issues are not taken into account properly. Three year ago, in 2014, the researchers from Context Information Security proved that they could take control of the smart-light bulbs produced by LIFX [Warwick, 2014]. These light bulbs can be controlled from a smartphone application, and as a consequence, they have to be connected to the house's wireless network. The security researchers managed to hack into the light bulb and find out the Wi-Fi network password.

The famous Wikileaks case revealed that the CIA might have used internet connected webcams in order to coordinate a DDOS-like attack and bring down internet availability in certain areas [Olenik, 2017]. Even if one choses to believe it or not, the security concerns over IoT devices must be taken into consideration and the laws have to be amended or provided, in order to secure the people's privacy under these new circumstances.

1. Real-life cases of IoT integration and adapting law

The permanent constant that the internet has become for most of us, the reality of the huge number of smartphones connected to the internet, the establishing of internet connection as a law enforced right in Finland in 2010 [Tăbușcă, 2010] – all these facts have one thing in common, the Internet. Besides connecting people, the internet has become the new center stage of most businesses. Today, we can not only order food or books from an online store – we can even buy a Ferrari car, make bank transactions, apply for a top university, subscribe for a gym or get a professional medical diagnostic. Almost all businesses had to adapt to the new reality.

An example of a business model that changed (partly) from one-off payment to a subscription model can be easily found in the auto industry.

Two of the best-known names in the tire industry, Pirelli and Michelin, sell now tires filled with sensors that are able to collect data on the road conditions or vehicle performance, for the cars using those tires. This information can be sent to the driver as a road report, to the car electronic systems for improving efficiency or safety, and to the manufacturer for statistics and further development processes. That approach transforms the simple tire and make it part of a complex service offered to the customer, a service that implies the actual tires set and a set of value-added services, such as:

- Increased safety
- Decreased fuel consumption
- Estimates on malfunctions that are likely to happen
- Reducing the out-of-work time for the vehicle

All these changes bring around a set of new legal consequences that are directly linked to this new business model. The change in business model transforms the one-time type of relation between the company and the customer (the company sells the tire; the customer pays the price) into a continuous relation. This type of relationship implies an increased level of brand-loyalty for the customer, as he enters a sort of long-time relationship with the company that sells him the products and provides him a service for a

certain amount of time. Due to this fact, the companies will start to collect more and more data on their customers, in order to be able to provide better and more significant services to their customers.

Collecting the data, personal information on customers as well as technical data from their IoT devices, will put the companies in line for a lot of possible privacy issues.

Another legal aspect of IoT massive integration is brought by the customers' reliance on the IoT sensors. This thing brings new potential legal issues in case of sensors malfunctions. For example, a new and modern car is able to park itself without the driver being present. We get out of the car, launch the car manufacturer's application on our smartphone and command the car to park in a very clear and large enough parking space. The car maneuvers, gets into place and start going straight forward to close the gap to the car parked in front of it. But, surprise, the car does not stop at 40 centimeters of the other car – instead, it keeps going forward and collides with the other car. Who is to be blamed from the legal point of view? Of course, at first stage, the driver/owner. But, I (the driver/owner) paid a lot of money as an extra for this car, especially because it is able to park by itself, and the car is sold legally in my country based on the approvals of different state regulatory bodies. So, I can turn and receive compensations from the car manufacturer or from the state that approved the selling of these models? The car manufacturer, in turn, can go against a third-party supplier which delivered a faulty sensor, or against a software developer that left a bug in their automotive software? There are a whole new bunch of legal issues that have to be taken into account.

Another legal approach that we consider to be very useful in the near future is the use of cyber-risk insurance. With over 48 billion cyber-attacks reported for 2014, which caused an estimate of over 445 billion dollars damages, the attacks target to the IoT devices are a given.

One way of minimizing the IoT security risks is the approach known as "privacy by design". The most up-to-date law regarding the data protection issues – the European Union General Data Protection Regulation (EUGDPR) states that [EUGDPR, 2017] "…the principle of data protection by design require data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor."

This legal act means that a very strict process has to be implemented, from the very first stage of developing an IoT device up to the moment it is disposed of. This privacy by design paradigm is considered to be able to:

- Reduce the risk of IoT devices to be considered not compliant to the privacy laws enforced by the EUGDPR
- Reduce the possible legal issues coming from cyber-crimes, because the security breaches must be reported to the legal bodies only if the controller of the data cannot demonstrate that he took all necessary measures for securing the data processing
- Exclude legal issues with the e-data processed while not being critical to the delivered service, by using anonymization techniques

The same privacy by design approach became a requirement of the US legal bodies, namely the US Federal Trade Commission (FTC), and of the UK legal body (OFCOM).

The EUGDPR brings about several new things that are quite important for the legal view of the matter:

- The fines for privacy related breaches are increased to up to 4$ of the global turnover of the breaching entity
- A higher possibility of customers' claims (somehow similar to some US legal areas) because the act shifts the proving part on the investigated party
- A higher possibility of shareholders claims because of the potentially huge fines

The EUGDPR brings about a specific section for the M2M area (machine-to-machine). This section enlarges the area where privacy law applies to the processes that involve machine data, not only personal information data of a real person. The compliance with the law, from the privacy point of view, comprises now:

- The ability to control data
- The implementation of different organization procedures in order to guarantee the secure storage and processing of personal data, both in-house and by third-party agreements
- The use of secure solution in order to minimize the risks of illegal data access

All companies that want to make business in the EU e-space must implement measures to reduce the cyber-attacks risks and must prove compliance with the principal of ordinary diligence. The most important steps a company should make are:

- Adopting a cyber-security policy
- Investing into a cyber-risk insurance
- Use a privacy by design approach
- Employing a data protection officer

The new Data Protection Officer position is not only a guideline, but in some cases, is even mandatory. For example, if the main activity of the company is based on processing operations which require permanent monitoring of data subjects on a large scale – companies such as banks, telecommunication operators, insurance companies, hospitals – or if the main activity is based on processing large-scale amounts of special data – such as biometric or medical data - than the company must appoint a DPO. This position should be able to perform its tasks in an independent manner, without receiving internal instructions on how to do its job. The DPO, according to the EUGDPR, should:

- Collect information in order to identify the processing activities
- Analyze and check the law compliance of the processing activities
- Inform, advise and recommend to the company's management about the security/privacy issues related to the processing activities
- Cooperate with the legal authorities as a contact point on issues related to data processing

But, in the end, the DPO has only a support role - the decision maker remains the company's representative, which might take into account the DPO's recommendations or not.

2. IoT data storage and the security issues

The security gets to be an issue, again, when the subject involved is to be seen and implemented with the need of accessing information distributed on an open network. For IoT devices there is information that is sent through the network and need to be accessed using an open source type such as XML data that is available in plain text format.

Observing the way cookies work in the online environment, and how they impact the implemented commercial laws, triggers some attention that needs to be given to the use of IoT devices that are widely used… and which number of uses grows every day. The

rapid development and implementation demands great attention not only on how fast and how many uses the IoT devices offer but also on how to secure the integration of this devices.

Within the online environment, information stored in form of cookies is used to target commercial advertising for each independent user. As such, IoT devices use information such as user positioning and other properties of the used device. In this case, the information must be accessed through highly secured servers using highly encrypted data transfer.

Taking the example of smartphones that have a wide range of application types that use with each new model new sensor types, we anticipate the same type of evolution to be also present in IoT devices environment. These devices are more specific in supplied functions but with the same identified vulnerabilities as in the case of smartphones. The vulnerabilities can be of virtual type but also with immediate physical dangerous actions.

The virtual type of vulnerability implies that through a system flaw that gets implemented on the IoT device, another system or person can access the information for later use, use that comes in conflict with one's person considered intimacy and privacy. Here we can name a simple example, like using an IoT device that permits one's physical access in a building or a service. That information at first sight can be of no security importance but, if a hacker gets that information, he can use it to plan unthinkable actions. By knowing a person's frequency of actions means that we've entered the privacy space of that person.

The physical type of immediate vulnerable action implies taking over by an unauthorized person of the functions implemented onto an IoT device. A simple scenario implies using an IoT device that is implemented on an automobile and has functions that can manage the way that the cat is driven. Some of today's cars can park themselves using a combination of hardware and software that is connected to the automotive functions of the car. A vulnerability in such an IoT implementation can have immediate dangerous implications such as minor or major accidents.

Another challenge in the security of the IoT implementation comes from the NoSQL type of databases [DBBestTechnologies, 2016] that are likely to be used, due to technical specifications. Knowing vulnerabilities and security implementations for SQL databases have a long history in client/server applications. Data management for IoT devices has proven that there should be more flexibility and speed in analyzing and managing of data. As part of the security paradigm, but also as type o structure, the SQL type of database is defined as an ACID principle known also as for implementing atomicity, consistency, isolation and durability. For this principle, the relational database system has a history in securing e-human and other sensitive commercial information.

Taking the example of an IoT scenario involving collecting of data from within a connected car - the IoT requirements state a use of more than 50Gb of information to be stored for each simple car travel, for each 2 hours of driving. This kind of information demands security but also more flexibility in data management and storage. NoSQL tends to be a new standard in the use of databases for IoT devices. NoSQL implementation gives more flexibility and speed in data analysis but need also detailed security algorithms to secure the transferred data. NoSQL stands for a BASE principle of defining databases that stand for basic accessibility of data, flexibility of handling data, and eventual consistency. This principle is more suitable for IoT development and growth of implementation but secure actions must be implemented to offer the e-human need of security in this flexible environment.

Security basically resumes in this needed flexible environment of IoT to adapt the complexity of security components and protocols to the final function of the IoT device depending on what the device is needed for and who is using it.

Dividing security on each layer of IoT device implementation is crucial in order to offer strong targeted and flexible uses. This need derives from the character of interconnected systems. Like any simple application that has many subroutines that need security protection on all levels, so are the IoT devices which are implemented in complex systems that need the interoperability of more than one single IoT device. Using more interconnected IoT devices to make a complex system work needs security protocols that operate on different levels. Each level should consider the security of different final uses that at final point affect the e-human right to security and intimate privacy.

3. IoT and the new legal issues

Any change of the business models, including the introduction of heavily e-business processes, always brings about a change in legal issues related to that.

According to the estimates available on the internet today, in 2017 we have around seven billion IoT devices deployed and the 2021 number is set for over twenty-two billion of such devices. All these devices are somehow related to private information: the IoT controlled heating system can show someone that the house is or not inhabited at some point, the IoT solution for medication can show someone your medical record, the IoT refrigerator can show someone your eating habits and diet, the IoT car beacon can show someone where you are at a given moment etc. All these data can bring huge privacy issues to the table.

According to our opinion, these possible legal issues can be categorized into five distinct areas:

1) Information exists to be used – all the collected data is going to be used at some point. Even if, in some cases, different companies could just collect data to start their databases, at some point it is just logical that the data will be used. The usage of that data at a later date might imply a breach of the initial scope of collecting that data.

2) Privacy issues increase exponentially – usually, a lot of personal information data used to be collected from the financial system (bank accounts, loans, online banking) but now data is to become available from hundreds of IoT sources, thus increasing a lot the number of possible breaches.

3) Cybersecurity becomes a very important issue – as proved time and again, no technology is 100% secure. The cybercrimes will no doubt advance from PCs and servers to attacking refrigerators, TVs or garage doors.

4) Modification of legal means related to data ownership – there might be a real need for updating the antitrust regulations, the copyright laws and, mandatory, to take into account the new European Union General Data Protection Regulation, brought to live in 2017.

5) Third party agreements – these widely used acts need to be heavily updated in order to provide direct and clear accountability for any privacy breach, regardless of the fact that this was due to the main data collector or a third party which just uses the data collected by another primary contact.

Besides the legal issues brought by collecting data from the retail IoT devices, there is a real legal issued appearing even for the enterprises that do not use IoT in their relation to their clients. Even introducing IoT devices inside a company's headquarters can

bring possible legal issues. The legal departments of such companies need to make sure that the employees contracts cover the electronic collection of their data by the employer, and, if not, find solutions to update those documents as to cover as good as possible this side. Since IoT is, by itself and by the link to the Internet, not bound to any localized country or border, the entire regulatory system might be somehow considered as a grey area. There is a distinct possibility that one's data are collected by a beacon in an airport in Taiwan, sent to a big data analysis company in US, the results of the analysis are sent into UK and the person is being asked at his workplace in Spain about the visit in Taiwan.

The European Union seems to be at least a step ahead of the rest of the world, encompassing quite a lot of issue related to IoT within its new EUGDPR act.

4. Conclusion

Within this article we aimed to provide a picture of the present situation of the IoT environment, in relationship with the legal issues that have aroused in direct link with the explosive use of internet connected devices.

Most probably, in the next couple of years, the mandatory insurance policies for cars will comprise a "cyber-risk" section, the house insurance policies will have a premium for smart-house systems and the companies will buy different types of such anti-cybercrime insurance policies.

Human use of modern technology will always bring new legal implications. But, despite the possible legal issues related to IoT, the IoT technology and its environment are still here, with a bright future that takes shape as we speak. Technology developers are permanently improving different aspects, such as connectivity, applications and security protocols. These things, combined and applied to all IoT devices, will help alleviate more and more security and privacy issues. The virtually world-scale focus on the "privacy by design" paradigm is considered one of the best solution today. This concept involves seven steps [Kim, 2016] that, ideally, would help us in the quest for a better and safer human security environment:

- Be proactive, not reactive
- Privacy at maximum should be the default setting
- Privacy has to be embedded into design
- Secure functionality without any trade-offs
- End-to-end security, from the first development stage to the final disposal
- Visibility and transparency
- Respect for the user privacy

While, historically, the IoT can be considered as being just in infant, this paradigm can become either a huge success (like the credit/debit cards we all use today) or a huge disappointment (remember the Google Glass project?).

We can finish with a phrase of an internet giant, the father of the World Wide Web, Sir Tim Berners-Lee "I want a web where I'm not spied on, where there's no censorship". These words, from a 2014 interview published in the British newspaper The Guardian, might be even considered as a call for a new bill of rights, comprising the E-Human Rights concept.

References

DBBestTechnologies (2016) *„Database decisions for the Internet of Things"*, available on-line at https://www.dbbest.com/blog/database-decisions/

EUGDPR (2017) *„ EU General Data Protection Regulation"*, available on-line at http://www.eugdpr.org/key-changes.html

Kim, I. (2016) *„The Internet of Things: A Reality Check for Legal Professionals"*, available on-line at http://www.lawpracticetoday.org/article/the-internet-of-things-a-reality-check-for-legal-professionals/

Olenik, D. (2017) *„IoT liability: Legal issues abound"*, available on-line at https://www.scmagazine.com/iot-liability-legal-issues-abound/article/647579/

Tăbușcă, S.M. (2010) *„The Internet Access as a Fundamental Right"*, Journal of Information Systems and Operations Management, vol. 4, no. 2: p. 206-212

Warwick, A. (2014) *„New technologies: a source of threat as well as a solution"*, available on-line at http://www.computerweekly.com/news/2240224012/IoT-smart-light-bulbs-get-security-update