THE
NATIONAL LAW REVIEW

Internet of Things: The Global Regulatory Ecosystem and the Most Promising Smart Environments Part II

compliance & risks

Article By
João Pedro Paro
Compliance & Risks

- Communications, Media & Internet
- Administrative & Regulatory
- Global

- China
- European Union
- All Federal
- Chile
- Colombia
- Brazil

Thursday, August 1, 2019

Regulatory Ecosystem

Hyperconnectivity is a real phenomenon and it is changing the concerns of society because of the kinds of interactions that can be brought about by IoT devices, which could be: i) People to people; ii) People to things (objects, machines); iii) Things/machines to things/machines.

It gives rise to different issues for people. According to a European Survey, 72% of EU Internet users worry that too much of their personal data is being shared online and that they have little control over what happens to this information[1]. It gives rise to inevitable ethical issues and its relationship with the techno environment.

The discussion on ethics that follows aims to provide a quick tour on general ethical principles and theories that are available as they may apply to IoT[2]. Law and ethics are overlapping, but ethics goes beyond law. Thus, a comparison of law and ethics is made and their differences are pointed out in the great work of Spyros G Tzafestas, who wrote *Ethics and Law in the Internet of Things World*. In this article, he considers that the risks and harms in a digital world are very high and complex, especially explaining those tech terms and their impact in our private life. Thus, it is of primary importance to review IoT and understand the limitations of protective legal, regulatory and ethical frameworks, in order to provide sound recommendations for maximizing good and minimizing harm[3].

Major data security concerns have also been raised with respect to 'cloud'-supported IoT. Cloud computing ('the cloud') essentially consists of the concentration of resources, e.g. hardware and software, into a few physical locations by a cloud service provider (e.g. Amazon Web Service)[4]. We are living in a data-sharing storm and the economic impact of IoT's cyber risks is increasing with the integration of digital infrastructure in the digital economy[5]. We are surrounded by devices which contain our data, for instance:

- **Wearable health technologies:** wearable devices that continuously monitor the health status of a patient or gather real-world information about the patient such as heart rate, blood pressure, fever;
- **Wearable textile technologies:** clothes that can change their color on demand or based on the biological condition of the wearer or according to the wearer's emotions;
- **Wearable consumer electronics:** wristbands, headbands, rings, smart glasses, smart watches, etc[6].

As a result of the serious impact IoT may have and because it involves a huge number of connected devices, it creates a new social, political, economic, and ethical landscape. Therefore, for a sustainable development of IoT, political and economic decision-making bodies have to develop proper regulations in order to be able to control the fair use of IoT in society.

In this sense, the most developed regions as regards establishing IoT Regulations and an ethical framework are the European Union and the United States both of which have enacted:

- Legislation/regulations.
- Ethics principles, rules and codes.

- Standards/guidelines;
- Contractual arrangements;
- Regulations for the devices connected;
- Regulations for the networks and their security; and
- Regulations for the data associated with the devices.

In light of this, the next section will deal with Data Protection Regulations, Consumer Protection Acts, IoT and Cyber Risks Laws, Roadmap for Standardization of Regulations, Risk Maturity, Strategy Design and Impact Assessment related with 2020 scenario, which is: 200 billion sensor devices and market size that, by 2025, will be between $2.7 trillion and $3 trillion a year.

Europe

The Alliance for Internet of Things Innovation (AIOTI) was initiated by the European Commission in order to open a stream of dialogue between European stakeholders within the Internet of Things (IoT) market. The overall goal of this initiative was the creation of a dynamic European IoT ecosystem to unleash the potential of IoT.

In October 2015, the Alliance published 12 reports covering IoT policy and standards issues. It provided detailed recommendations for future collaborations in the Internet of Things Focus Area of the 2016-2017 Horizon 2020 programme[7].

The IoT regulation framework in Europe is a growth sector:

- EU Directive-2013/40: this Directive deals with “Cybercrime” (i.e., attacks against information systems). It provides definitions of criminal offences and sets proper sanctions for attacks against information systems[8].
- EU NIS Directive 2016/1148: this Network and Information Security (NIS) Directive concerns “Cybersecurity” issues. Its aim is to provide legal measures to assure a common overall level of cybersecurity (network/information security) in the EU, and an enhanced coordination degree among EU Members[9].
- EU Directive 2014/53: this Directive “On the harmonization of the laws of the member states relating to the marketing of radio equipment”[10] is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU.
- EU GDPR: European General Data Protection Regulation 2016/679: this regulation concerns privacy, ownership, and data protection and replaces EU DPR-2012. It provides a single set of rules directly applicable in the EU member states.
- EU Connected Communities Initiative: this initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high-speed broadband (more than 30 Mbps).

United States

A quick overview of the general US legislation that protects civil rights (employment, housing, privacy, information, data, etc.) includes:

- Fair Housing Act (1968);
- Fair Credit Reporting Act (1970);
- Electronic Communication Privacy Act (1986), which is applied to service providers that transmit data, the Privacy Act 1974 which is based on the Fair Information Practice Principle (FIPP) Guidelines;
- Breach Notification Rule which requires companies utilizing health data to notify consumers that are affected by the occurrence of any data breach; and

- IoT Cybersecurity Improvement Act 2019: the Bill seeks “[t]o leverage Federal Government procurement power to encourage increased cybersecurity for

Internet of Things devices." In other words, this bill aims to shore up cybersecurity requirements for IoT devices purchased and used by the federal government, with the aim of affecting cybersecurity on IoT devices more broadly.

- SB-327 Information privacy: connected devices: California's new SB 327 law, which will take effect in January 2020, requires all "connected devices" to have a "reasonable security feature."

The above legislation is general, and in principle can cover IoT activities, although it was not designed with IoT in mind. Legislation devoted particularly to IoT includes the following:

- White House Initiative 2012: the purpose of this initiative is to specify a framework for protecting the privacy of the consumer in a networked work.

This initiative involves a report on a 'Consumer Bill of Rights" which is based on the so-called "Fair Information Practice Principles" (FIPP). This includes two principles:

1. **Respect for Context Principle:** consumers have a right to insist that the collection, use, and disclosure of personal data by Companies is done in ways that are compatible with the context in which consumers provide the data;
2. **Individual Control Principle:** consumers have a right to exert control over the personal data companies collect from them or how they use it.

China

Where we start to see the most advanced picture is in China. In 2017, the Ministry of Industry and Information Technology (MIIT), China's telecom regulator and industrial policy maker, issued the Circular on Comprehensively Advancing the Construction and Development of Mobile Internet of Things (NB-IoT) (MIIT Circular [2017] No. 351, the "Circular"), with the following approach in the opening provisions:

Building a wide-coverage, large-connect, low-power mobile Internet of Things (NB-IoT) infrastructure and developing applications based on NB-IoT technology will help promote the construction of network powers and manufacturing powers, and promote "mass entrepreneurship, innovation" and "Internet +" development. In order to further strengthen the IoT application infrastructure, promote the deployment of NB-IoT networks and expand industry applications, and accelerate the innovation and development of NB-IoT[11]

Nowadays China already has a huge packet of regulation on technological matters:

- 2015 State Council - China Computer Information System Security Protection Regulation (first in 1994);
- 2007 MPS - Management Method for Information Security Protection for Classified Levels;
- 2001 NPC Standing Committee – Resolution about Protection of Internet Security;
- 2012 NPC Standing Committee – Resolution about Enhance Network Information

Protection;
- July 2015: National Security Law - ‘secure and controllable’ systems and data security in critical infrastructure and key areas;
- 2014 MIIT – Guidance on Enhance Telecom and Internet Security;
- 2013 MIIT – Regulation about Telecom and Internet Personal Information Protection
- 2014 China Banking Regulatory Commission - Guidance for Applying Secure and Controllable Information;
- Technology to Enhance Banking Industry Cybersecurity and Informatization Development

Further, as if this were not enough, the Chinese government is being proactive and has several important laws and regulations in the Pipeline, as it can be seen from the list below:

- CAC: Administrative Measures on Internet Information Services;
- CAC Rules on Security Protection for Critical Information Infrastructure;
- Cybersecurity Law;
- Cyber Sovereignty;
- Security of Product and Service;
- Security of Network Operation (Classified Levels Protection, Critical Infrastructure);
- Data Security (Category, Personal Information);
- Information Security.

Finally, China established, in 2016, the National Information Security Standardization Technical Committee and its current work is developing a Standardization – TC260 (IT Security) on Technical requirement for Industrial network protocol and general reference model and requirements for Machine-to-Machine (M2M) security.

Latin America

The Latin American countries have different levels of development and this sets up a huge asymmetry between the domestic legal frameworks. The following is a quick regulation overview on Latin American countries:

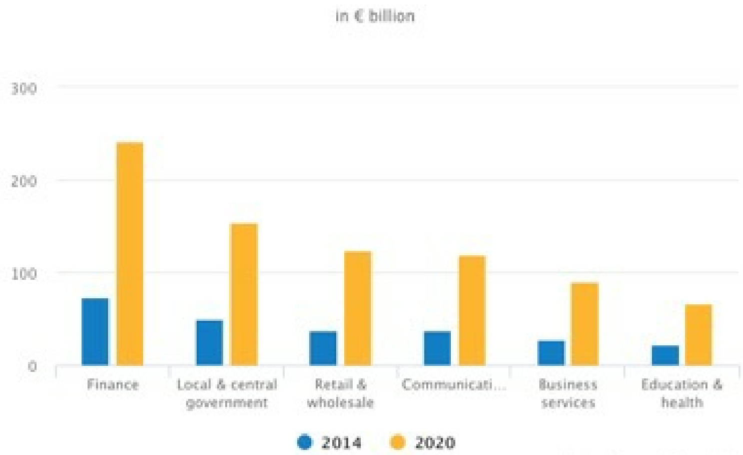
- Brazil has the "National IoT Plan" (Decree N. 9.854/2019) that aims to ensure the development of public policies for this technology sector and members of Brazilian parliament presented the bill No. 7.656/17 with the purpose of eliminating tax charges on IoT products;
- Colombia has a Draft of Law No. 152/2018 on the Modernization of the Information and Communication providing investments incentives to IT Techs (article 3);
- Chile has a new Draft Law Boletín N° 12.192-25/2018 on Cyber crimes and regulation on internet devices and hackers attacks;
- In 2017, Argentina launched a Public Consultation on IoT regarding regulations that must be updated and how to get more security and improve the technological level of the country[12] .

Most Promising Smart Environments

Smart environments are regarded as the space within which IoT devices interact connected through a continuous network. Thus, smart environments aim to satisfy the experience of individuals from every environment, by replacing the hazardous work, physical labor and repetitive tasks with automated agents. Generally speaking, sensors are the basis of these kind of smart devices with many different applications e.g. Smart Parking, Waste Management, Smart Roads and Traffic Congestion, Air Pollution, River Floods, M2M Applications, Vehicle auto-diagnosis, Smart Farming, Energy and Water Uses, Medical and Health Smart applications, etc[13].

Another way of looking at smart environments and assess their relative capacity to produce business opportunities is to identify and examine the most important IoT use cases that are either already being exploited or will be fully exploited by 2020.

For the purposes of this article, the approach was restricted to sectors consisting of the most promising smart environments to be developed up to 2020 in the European Market as displayed in the Chart below:



Source: European Commission

Vertical IoT Market Size in Europe

The conclusions of the last report of the European Commission are impressive and can help to understand the continuous development of the IoT market and how every market has to comply with the law and they will emerge facing a regulatory avalanche as mentioned in item 2 on the Regulatory Ecosystem.

Final Considerations: IoT as Consumer Product Health and Safety

IoT safety is becoming more important every day. On the one hand, as mentioned above, most concerns for IoT safety are primarily in the areas of cyber-attacks, hacking, data privacy, and similar topics; what is better referred to as security than safety. On the other hand, it can be approached by physical safety hazards which may result from the operation of consumer products in an IoT environment or system.

IoT provides a new way to approach business and it is not restricted to one or other market or topic. It is a ***metatopic*** or ***metamarket*** showing different possibilities and applications and will be spread in the near future.

In general, IoT products are electrical or electronic applications with a power source and a battery connected by a charging device. So long as the power source, batteries and charging devices are present we have the usual risks of electrical related hazards (fire, burns, electrical shock, etc.). Nonetheless, IoT makes matters more complicated as smart devices have the function to send commands and control devices in the real world.

IoT applications can switch the main electrical powers of secondary products or can operate complex motor systems and so on. Then they have to be accurate and might provide minimal requirements to care of consumer health and safety. Risk assessment and hazard mitigations will have to adapt to IoT applications reinventing new methods to assure regular standards of IoT usability. Traditional health and safety regulations might be up to date with this new technological reality to be effective at reducing safety hazards for consumer products.

To conclude, this article was intended to summarize two main issues: I) IoT as an increasing and cross topic market which will become a present reality closer to our daily lives; II) IoT will be regulated and become an important concern in consumer product health and safety.

See the first Installment of the IoT: Seizing the Benefits and Addressing the Challenges and the Vision of IoT in 2020.

[1] Nóra Ni Loideain. Port in the Data-Sharing Storm: The GDPR and the Internet of Things. King’s College London Dickson Poon School of Law Legal Studies Research Paper Series: Paper No. 2018-27.P2.

[2] Spyros G Tzafestas. Ethics and Law in the Internet of Things World. Smart Cities 2018, 1(1), 98-120. P. 102.

[3] Spyros G Tzafestas. Ethics and Law in the Internet of Things World. Smart Cities 2018, 1(1), 98-120. P. 99;

[4] Nóra Ni Loideain. Port in the Data-Sharing Storm: The GDPR and the Internet of Things. King’s College London Dickson Poon School of Law Legal Studies Research Paper Series: Paper No. 2018-27.P. 19.

[5] Petar Radanliev, David Charles De Roure and others. Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardization of Regulations, Risk Maturity, Strategy Design and Impact Assessment. Oxford University. MPRA Paper No. 92569, March 2019, P. 1.

[6] pSyros G Tzafestas. Ethics and Law in the Internet of Things World. Smart Cities 2018, 1(1), 98-120. P. 101; https://doi.org/10.3390/smartcities1010006

[7] More information available here.

[8] EUR-Lex Document 32013L0040. Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013. Available here.

[9] NIS Directive. The Directive on Security of Network and Information Systems.

[10] EUR-Lex Document 32014L0053. Directive 2014/53/EU of the European Parliament and the Council of 16 April 2014.

[11] Notice of the General Office of the Ministry of Industry and Information Technology on Promoting the Development of Mobile Internet of Things. Department of Industry communication letter [2017] No. 351.

[12] Available here.

[13] More examples

Source URL: https://www.natlawreview.com/article/internet-things-global-regulatory-ecosystem-and-most-promising-smart-environments