경제규제와 법(Journal of Law & Economic Regulation)
제9권 제1호 (통권 제17호). (Vol. 9. No. 1). 2016. 5. pp.69~93

Special Issue Internet of Things : Legal Issues and Challenges towards a Hyperconnected World

Clouds of Things : Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom[†][*]

Guido Noto La Diega[**]

목차

〈ABSTRACT〉

The article critically analyses the Internet of Things (IoT) and its intersection with cloud computing, the so-called Clouds of Things (CoT). 'Things' are understood as any physical entity capable of connectivity that has a direct interface to the physical world (i.e. a sensing and/or actuating capability). From another perspectives (especially product liability), Things can be seen as an inextricable mixture of hardware, software, and services.

Alongside a clarification of the essentials, the six factors of the CoT complexity are described and light is shed on the regulatory options (regulation, co-regulation, self-regulation, holistic approach, fragmentation).

Focussing on the British legal systems, the article reports on the state of the art of CoT deployment in the United Kingdom and deals with

[†] 투고일자 2016. 3. 13, 게재확정일자 2016. 5. 30.

[*] This article constitutes the revised and developed version of G. Noto La Diega, British perspectives on the Internet of Things. The Clouds of Things-Health use case, in Internet of Things: Legal Issues and Challenges towards a Hyperconnected World, Proceedings of the International Conference of the Center for Law & Public Utilities, Seoul National University, Honolulu (US), 27.11.2015, 45-150.

[**] Associate Lecturer in Law, Leader for Intellectual Property Law at the Buckinghamshire New University; President of 'Ital-IoT'; cultore della materia of intellectual property and private law at the University of Palermo (on leave). Special thanks to Professor Ian Walden (Queen Mary University of London) and Dr. Jatinder Singh (University of Cambridge Computer Laboratory), for the collaborative multidisciplinary research conducted, respectively, on IoT contracts for domotics and IoT-health. I am beholden to all the participants to the Honolulu conference for their valuable contributions; Professors Pierre-Jean Benghozi (Université Paris-Saclay and ARCEP), Seong-Wook Heo (Seoul National University), Hee-Jung Lee (Korea University), Won-Woo Lee (Seoul National University), Jong-In Lim (Korea University), Deirdre Mulligan (UC Berkeley), Hans-Heinrich Trute (Universität Hamburg), Melissa Hye-Sun Yoon (Hanyang University), Director Sung Joo Kang (Internet Convergence Policy Bureau, Ministry of Science, ICT and Future Planning) and Mr Hanno Lee (Naver) deserve an honourable mention. Views and mistakes, however, are solely my responsibility. Comments can be addressed to noto.la.diega@gmail.com or tweeted to @guidonld.

some of the main technical and legal issues emerging from CoT. Particularly, the core will be data protection, privacy, and consumer law. Indeed, these themes are considered the most relevant by the regulators.

By mastering the relevant legal issues and following the example of the United Kingdom, the Republic of Korea will be able to unleash its extraordinary potential as to the IoT, thus retaining its position as the smartest country in the world.

Keywords: Internet of Things, Clouds of Things, cloud computing, repurposing, regulation

Ⅰ. Introduction

Labelling a technological development as a 'revolution'[1] is as dreadfully common as it is saying that the 'revolution' will lead to 'disruptive' innovation.[2] The Internet of Things (IoT)[3] is a noteworthy phenomenon, if only because of its outstanding economic impact and social potential.[4] However, it is too soon to assess the degree to which it will change our lives and, from a legal perspective, if and to what extent existing rules will have to change and new rules will have to be tailored.

Consequently, avoiding any naïf eulogy, this

[1] Cf. Internet of Things, ITU (International Telecommunication Union), *The Internet of Things*, ITU Internet Reports 2005, November 2005, available at http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf, whereby "[t]he Internet of Things is a technological revolution that represents the future of computing and communications, and its development depends on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology". See also Technology Strategy Board, *Internet of Things (IoT) and Machine to Machine Communications (M2M) Challenges and opportunities: Final paper*, May 2013, available at https://connect.innovateuk.org/documents/3077922/3726367/IoT+Challenges,%20final+paper,%20April+2013.pdf/38cc8448-6f8f-4f54-b8fd-3babed877d1a, according to which the IoT "describes the revolution already under way that is seeing a growing number of internet enabled devices that can network and communicate with each other and with other web-enabled gadgets."

[2] Cf. S. Amyx, *Why the Internet of Things Will Disrupt Everything*, July 2014, http://www.wired.com/insights/2014/07/internet-things-will-disrupt-everything/ and SRI Consulting Business Intelligence, *Disruptive Technologies Global Trends 2025*, Appendix F: The Internet of Things, available at http://www.internet-of-things.eu/resources/documents/appendix-f.pdf. For a recent critique to Clayton M. Christensen's idea of disruptive innovation (first sketched in his *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, 1997) see A.A. King-B. Baatartogtokh, *How Useful Is the Theory of Disruptive Innovation?*, in *MIT Sloan Management Review*, Fall 2015, available at http://sloanreview.mit.edu/article/how-useful-is-the-theory-of-disruptive-innovation/.

[3] There are several phrases used sometimes to denote the same concept or kindred ideas. The main ones are industrial internet, smart devices, connected things, ubiquitous computing, physical computing, physical Internet, cyber-physical systems, smart spaces, everyware, future Internet, Internet of Everything, pervasive computing, pervasive Internet, ambient intelligence, ambient media, haptic computing, Machine to Machine (M2M), radio-frequency identification (RFID), Connected Environments, smart cities, Spimes, Connected World, Wireless Sensor Networks, Situated Computing, web of things, semantic web, web 3.0, net of things, quantified self. Indeed some of them identify species of the IoT (e.g. quantified self), some others neighbouring areas (e.g. M2M), whilst most of them are not accurate and should be avoided in scientific discourses. As to the latter, I call on the scientific community in order not to use the adjectives 'smart' and 'intelligent' any longer. Indeed, apart from the fact that many CoT applications are rather daff, intelligence and smartness are tipically human attributes, therefore one ought to avoid the sin of anthropomorphism. Moreover, it is a question of semantic strategy. The criticised adjectives have nowadays the sense to distinguish old generation things by Things (e.g. an old meter versus a smart meter). In a few years, however, most object will be created as capable of connectivity and with sensing and/or actuating possibilities, therefore one does not want to look obsolete in the short run.

[4] The Federal Trade Commission (FTC) expresses a balanced opinion in FTC Staff report, *Internet of Things. Privacy & Security in a Connected World,* January 2015, 48, where it recognises "that this industry is in its relatively early stages." There are umpteen reports on the dimension of the phenomenon; recently, research has suggested that over half of the UK businesses plan to employ a chief IoT officer in the next year to help plan and manage their growing IoT spend (A. Scroxton, *Half of UK businesses looking for internet of things lead roles*, in *ComputerWeekly.com*, 17-2-2016).

work has the modest purpose of defining the IoT and its intersection with cloud computing, the so-called Clouds of Things (CoT). Alongside a clarification of the essentials, I will describe the six factors of CoT complexity, as well as the regulatory options (regulation, co-regulation, self-regulation, holistic approach, fragmentation).

Focussing on the British legal systems, I will report on the state of the art of CoT deployment in the United Kingdom[5] and deal with some of the main technical[6] and legal issues[7] emerging from CoT. Particularly, the core will be the themes considered more relevant by the regulators, namely data protection, privacy, and consumer law.

By mastering the relevant legal issues and following the example of the United Kingdom, the Republic of Korea will be able to unleash its extraordinary potential as to the IoT,[8] thus retaining its position as the smartest country in the world.[9]

President Park Geun-Hye's announcement of 18 May 2016 to ease regulations on drones, self-driving vehicles and the biotech sector moves in this direction.

Ⅱ. Internet of Things: Definitions and Regulatory Options

Unlike the cloud,[10] there is not a commonly accepted definition nor a taxonomy of the IoT.[11] However, the latter has been recently defined by ISO and IEC as "An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react."[12] Whereas the

[5] This work takes a private law perspective, but the United Kingdom has dealt with the IoT also as to different fields of law. An interesting example is provided by Home Office, Internet of things: potential risk of crime and how to prevent it, 10.3.2015, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/410117/Internet_of_things_-_FINAL.pdf.

[6] The relevant literature is abundant, but a very good sample is provided by J. Singh–T. Pasquier–J. Bacon–H. Ko–D. Eyers, *Twenty security considerations for cloud-supported Internet of Things*, in *Internet of Things Journal, IEEE*, 2015, 99, 1.

[7] As to the legal issues, we will not go into details, referring for what is not henceforth deepened to Hon, W. Kuan and Millard, Christopher and Singh, Jatinder, Twenty Legal Considerations for Clouds of Things (January 4, 2016). Queen Mary School of Law Legal Studies Research Paper No. 216/2016. Available at SSRN: http://ssrn.com/abstract=2716966.

[8] As said by Ministry of Science, ICT, and Future Planning (Republic of Korea), *Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution*, 8.5.2014, available at http://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf, even though the Republic of Korea lags someway behind major countries globally in terms of IoT competitiveness, it has enough potential (2nd following the United States) to stand as a leader of the global market with its top-class ICT infrastructure and manufacturing capacities.

[9] OECD, *Science, Technology and Industry Scoreboard 2015*, 19.10.2015, available at http://www.oecd.org/sti/oecd-science-technology-and-industry-scoreboard-20725345.htm.

[10] P. Mell–T. Grance, *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-145, 2011, 2, available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[11] In March 2015, I made a survey of the existing definitions of the IoT and I collected 64 definitory attempts, none of which entirely convincing. I would be surprised if this number was doubled now. NIST (National Institute of Standards and Technology) is working on some definitions. It is notable that the *Draft Framework for Cyber-Physical Systems* of September 2015 refers for the definition of 'thing' to that of 'physical entity', which in turn is defined with no reference to the physical component (also virtual things can be subject to monitoring and control actions; entities have not to be physical as they include, for instance, subsystems). See the full text here http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf.

[12] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1, *Internet of Things (IoT): Preliminary Report 2014,* Geneva, 2015, § 4.1 (http://www.iso.org/iso/internet_of_things_report-jtc1.pdf). Its Special Working Group 5 (SWG 5 'Internet of Things') established, among

ISO/IEC formula can be roughly accepted as a starting point, the Microsoft Cloud Computing Research Centre prefers to look at the Thing,[13] understood as any physical entity capable of connectivity that has a direct interface to the physical world (i.e. a sensing and/or actuating capability)[14]. From another perspectives (especially product liability), Things can be understood as an inextricable mixture of hardware, software, and services.[15]

Things may be attached (e.g. wearables) or embedded (e.g. pacemakers)[16]. They are usually composite, smartphones and connected cars being the simplest examples.[17] Virtual entities are not Things, notwithstanding the ITU's definition, whereby a Thing is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks."[18] Human beings and animals are not Things. Not yet, at least. It is indeed likely that evolutions in artificial enhancement techniques (AE) and in implants technologies will be at some point developed so that every part of the human body will (be able to) be substituted by artificial organs and tissues and damaged faculties will be healed through chips. When this will become real – this is not science fiction! – It will not be clear the moment when we will not be human, having become androids and thus Things. When that day will come, we will not dispute on what 'Thing' means, but on what 'human' means.[19]

Given the complexity of the relevant ecosystem(s), one solution to simplify is to break it

other things, the Ad Hoc Group 1 (AHG1) to work on 'Develop[ing] a common understanding of IoT'. AHG1 produced the definition, which was then adopted by SWG 5.

[13] I will refer to 'Thing' to distinguish it by ordinary 'things'.

[14] Hon-Millard-Singh (7), 4.

[15] See more broadly Noto La Diega, Guido and Walden, Ian, Contracting for the 'Internet of Things': Looking into the Nest (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016. Available at SSRN:http://ssrn.com/abstract=2725913.

[16] Things may also not have any physical contact with human being. Let us think to robots. Proximity, however, is usually a peculiar characteristic of Things. This brings me back to an idea expressed by Walter Benjamin in *Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit*, in *Zeitschrift für Sozialforschung*, 1936, 5, I, 41-68, available at http://www.arteclab.uni-bremen.de/~robben/KunstwerkBenjamin.pdf and translated at https://www.marxists.org/reference/subject/philosophy/works/ge/benjamin.htm; in fact, according to Benjamin "*Die Dinge sich räumlich und menschlich »näherzubringen« ist ein genau so leidenschaftliches Anliegen der gegenwärtigen Massen wie es ihre Tendenz einer Überwindung des Einmaligen jeder Gegebenheit durch die Aufnahme von deren Reproduktion ist*" (italics of the text), that is to say "*the desire of contemporary masses to bring things "closer" spatially and humanly, which is just as ardent as their bent toward overcoming the uniqueness of every reality by accepting its reproduction.*"

[17] A smartphone contains a large number of sensors and a damage may occur as a consequence of a defect or inaccuracy of any of the said components of the Thing (sub-thing). It is not always clear if the liability should fall on the main actor responsible for the composite Thing or if the sub-things's actors should be liable. Generally speaking and unless a contrary evidence is provided, I am in favour of the first hypothesis, because i. The final manufacturer has a duty to double-check the security and safety of the composite Thing both when placing it on the market and during the provision of the services; ii. It could prove impossible for the customer to track the supply chain and find the responsible for the single sub-thing. The conclusion may be different depending on the openness or closure of the system (e.g. Apple can control third-parties apps through its store, whereas Android stores are open, thus not allowing the same control). Courts may also give some relevance to the number of sub-things present in the composite thing (an airplane is not the same as a light bulb) and the kind of activity for which the Thing is used (a defibrillator can save a life and therefore higher standards of security and stricter scrutinies are required).

[18] International Telecommunication Union Standardization Sector (ITU-T), *Overview on the Internet of Things*, Y.2060, 06/2012, § 3.2.3, downloadable at https://www.itu.int/rec/T-REC-Y.2060-201206-I/en.

[19] At the same time, Things will become more and more autonomous, thanks to the developments of machine learning techniques and the so-called artificial intelligence. Beware though. Things will not be human-like. They may also look like humans, but this is will be the result of human anthropocentricism. When (not if) Things will be entirely and properly autonomous, their intelligence will not have much in common with the human intelligence.

down by adopting a sectorial taxonomy, whereby one ought to consider separately health (e.g. robot surgery), city planning ("smart" cities), manufacturing (e.g. 3D printing), distribution (see especially the use of RFID, radio-frequency identification to track the supply chain), transport (e.g. driverless cars and vehicle-to-vehicle systems), energy (e.g. "smart" grids and meters), leisure (e.g. games, drones), and agriculture (irrigation systems), just to name the main ones.

This complexity made Professor Hans-Christian Trute[20] criticise my proposal for a holistic regulation of the IoT (I was referring to some clarifying guidance, not to any form of specific hard law tool as it would be a ridiculous IoT law).[21] The objection does not fall necessarily short. However, there is a significant overlapping between most of the sectors (one need only think to drones and BYOD, which can potentially fall under any category). This is inter alia demonstrated by the fact that regulators denounce that they encounter lack of competence when trying and regulating the IoT, mainly because of these overlapping, whose counterpart is the overlapping of competences between different regulators (e.g. communications and data protection).[22]

Moreover, and maybe most importantly, a critical characteristic of IoT systems is repurposing. I understand 'repurposing' as the phenomenon whereby Things are made and/or provided for certain purposes, whilst they end up serving other (potentially unforeseen) purposes, mainly because: i. The communication within the relevant subsystem and among subsystems processed in the cloud can lead to perform actions and produce information of which the single Thing was not capable of; ii. Under certain conditions (e.g. emergency) the system may reconfigure either in an automated fashion or user initiated.[23]

Consequently, what is the best regulatory option for the IoT? Recent studies have shown that self-regulation is not a satisfactory option.[24] Traditional regulation, however, would lack the necessary flexibility required by the constantly changing technological landscape. Therefore, co-regulation seems the appropriate option,[25] providing a clear general framework of rules, whose implementation is left to the private stakeholders. This said, how to strike a balance between a one-size-fits-all regulation of the IoT and a fragmented one? The relevant good practice is provided by Italy, which has recently established a permanent committee on machine-to-machine (M2M) communication[26], where regulators and

[20] When I do not specify further, I refer to the debate originated by the Hawaii conference on the Internet of Things.

[21] According to the FTC (4), 50: "while IoT specific-legislation is not needed, the workshop provided further evidence that Congress should enact general data security legislation [as well as] broad-based (as opposed to IoT-specific) privacy legislation.".

[22] Professor Pierre-Jean Benghozi said that this is the case of France (he is commissioner of ARCEP, the *Autorité de Régulation des Communications Électroniques et des Postes*).

[23] The purpose plays a fundamental role from a legal perspective, especially as to the rules of liability and data protection. However, these aspects will be the subject of another research.

[24] According to McCarthy, D. & Morling, P. (2015). *Using Regulation as a Last Resort: Assessing the Performance of Voluntary Approaches*. Royal Society for the Protection of Birds: Sandy, Bedfordshire, 10, most self regulatory schemes (82% perform poorly. *Contra*, FTC (4), 49, where the US regulator "agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices."

[25] Co-regulation is the best option also according to European Commission*, IoT Architecture*. Available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1750.

[26] Machine-to-Machine communications, also known as Machine Type Communication (MTC), is "a rapidly growing area with the potential to significantly affect mobile tele-

ministers can coordinate their initiatives.[27]

The UK Government Chief Scientific Adviser (GCSA)[28] has specified that "[l]egislation should be kept to the minimum required to facilitate the uptake of the Internet of Things",[29] but there would be novel regulatory challenges (mainly privacy and liability-related), therefore "[g]ood regulation and legislation will be needed to anticipate and respond to new challenges."[30] I do not entirely agree with top-down, ex-ante, hard law instruments.

The approach should be gradual, empirical and problem-based. Nevertheless, I welcome the intent to consider "systematically the impact of emerging technologies in policy, delivery and operational planning."[31] More generally, I agree with those scholars who have recently pointed out that any global online activity can only be regulated properly only after we develop an international consensus at a high level, based on fundamental normative principles rather than on detailed prescriptions for behaviour.[32] However, we know how slow the formation of an international consensus can be and we have to act, otherwise we risk closing the stable door after the horse has bolted.

Ⅲ. Clouds of Things

As said above, I will refer mainly to CoT[33],

communication networks. M2M communications encompasses a number of areas where devices are communicating with each other without human involvement." (ITU-T, Impact of M2M communications and non-M2M mobile data applications on mobile networks, 15.6.2012, http://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-IOT-2012-M2M-PDF-E.pdf) There is not agreement on whether M2M ought to be considered as a precursor of the IoT or as one of its species. For instance, the Commission Staff Working Document "Impact Assessment Accompanying the document *Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012 {COM(2013) 627 final} {SWD(2013) 332 final}*, 11.9.2013, SWD(2013) 331 final, 8.2.2, whereby "[a]n increasing number of sectors is set to introduce the "Internet of Things" or machine-to-machine (M2M) technologies, whereby devices are connected and interact through connectivity". On the contrary, J. Höller et al., *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*, Oxford (MA), 2014, 14, argue that "[t]he IoT is a widely used term for a set of technologies, systems, and design principles associated with the emerging wave of Internet-connected things that are based on the physical environment […] In contrast to M2M IoT also refers to the connection of such systems and sensors to the broader Internet, as well as the use of general Internet technologies."

[27] On 25.11.2015, the *Comitato permanente per i servizi di comunicazione Machine to Machine* (permanent committee for M2M communication services) has been launched. Its members are the *Autorità Garante delle Comunicazioni* (AGCOM, the communications regulator), the *Autorità per l'energia elettrica, il gas e il sistema idrico* (electricity, gas, water authority), the *Autorità di Regolamentazione dei Trasporti* (transports authority), the *Agenzia per l'Italia Digitale* (agency for the digital agenda) and the *Ministero dello Sviluppo Economico* (Ministry of Economic Development). See AGCOM, Delibera n. 459/15/CONS, available at http://www.agcom.it/documents/10179/2409164/Delibera+459-15-CONS/6c9ac9f2-e46f-4df6-9f25-66205d6b7620?version=1.0.

[28] The GCSA is the personal adviser on science and technology-related activities and policies to the Prime Minister and the Cabinet.

[29] GCSA, *The Internet of Things: making the most of the Second Digital Revolution,* 18.12.2014, 9 (also known as the *Blacket Review*).

[30] GCSA (29), 9.

[31] ibid.

[32] C. Reed-D. Stefanatou*, Legal and Regulatory update – embedding accountability in the international legal framework*, forthcoming. Thanks to the Authors for sending the manuscript.

[33] 'Clouds of Things' have been the object of the 2nd annual Symposium of the Microsoft Cloud Computing Research Centre, held in Windsor on 26-27.10.2015. S. also the works of the CoT conferences http://cloudofthings.org/ and also the Cloud of Things platform, which enables businesses to develop self-branded IoT solutions (it delivers software development kits (SDKs) for endpoint devices, an insight-driven big-data cloud backend and an engine that automatically generates source-code for mobile control applications, s. https://www.cloudofthings.com/welcome/). Even when I will refer to the IoT and unless otherwise specified, it is understood that I refer to the Clouds of Things.

i.e. "ecosystems in which there are communications between things and clouds, including M2M communications mediated by cloud."[34] Even though part of the IoT is currently not based on cloud technologies, these are becoming more and more common and they raise noteworthy issues.

The relation amongst the IoT and cloud computing has been heretofore fuzzy.[35] The flaws of the relevant literature become apparent as soon as one reads the only existing book on the legal aspects of the IoT, where it is openly stated that "things in the real world and their deployment in the IoT are not addressed by cloud computing"[36], against those who affirm that the cloud is what has made the IoT possible.[37] A position in the middle of the opposite maximalisms should be taken.

There is indeed a close link between the considered technologies: even though today not every IoT application is 'cloudy', the cloud is going to be more and more the natural enabler of the IoT, first of all due to its role of mediator and coordinator between Things. One need think then to big data[38], analytics[39] and the constrained on-board (processing, storing, and battery) capacity of Things that makes fundamental the cloud outsourcing. Moreover, especially if one considers the system at a large-scale level, it is obvious that the cloud is the cornerstone of the developing social network of things[40] and its coessential open sharing[41]. Furthermore, cloud accessibility addresses the fact that many Things are wore (or anyhow part of our everyday life), hence it is crucial for the user(s)[42] to be able to access the services and the applications regardless their temporary geographical location.[43] Finally, new

[34] Hon-Millard-Singh (7), 7.

[35] I agree with A. Botta et al., *On the Integration of Cloud Computing and Internet of Things*, 2014 International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, 27-29.8.2014, 23, that the literature focuses on IoT and cloud separately, whilst one ought to clarify the integration of those technologies (which they call 'CloudIoT') that is the basis for new challenges and issues.

[36] R.H. Weber-R. Weber, *Internet of Things. Legal Perspectives*, Springer, Heidelberg-Dordrecht-London-New York, 2010, 17.

[37] Harvard Business Review, *Internet of Things: Science Fiction or Business Fact?* Harvard Business Review Services Report, 2014, 1, where the factor is read jointly with the rapid proliferation of connectivity and miniaturization of sensors and communications chips.

[38] Cf. M. Aazam et al, *Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved*, 2014 (Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014, 414), where it is observed that the IoT is 'becoming so pervasive that it is becoming important to integrate it with cloud computing because of the amount of data IoT's could generate and their requirement to have the privilege of virtual resources utilization and storage capacity, but also, to make it possible to create more usefulness from the data generated by IoT's and develop smart applications for the users.'

[39] For instance, without the cloud it would be hardly feasible an analysis of data collected by multiple sensors and multiple Things.

[40] Cf. L. Atzori et al., *The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization*, in *Computer Networks* 56 (2012) 3594 and P. Deshpande et al., *M4M. A model for enabling social network based sharing in the Internet of Things*, in *7th International Conference on Communication Systems and Networks (COMSNETS)*, 6-10.1.2015 Bangalore, India, IEEE Proceedings, 2015. For the basic concepts of the social Internet of Things s. http://www.social-iot.org/.

[41] One example of this conflation is the so-called cloud manufacturing, i.e. '*a new direction for manufacturers to innovate and collaborate across the value chain via cloud-based technologies*' (Y.-K. Lu-C.-Y. Liu-B.-C. Ju, *Cloud Manufacturing Collaboration: An Initial Exploration*, 2012 Third World Congress on Software Engineering, Wuhan, 6-8.11.2012, 163).

[42] Along with availability, elasticity, and improved resource utilisation, multitenancy is an intrinsic characteristic of cloud computing according to *Advances in Clouds. Research in Future Cloud Computing*, Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit, edited by L. Schubert and K. Jeffery, 2012, 12 (available at http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-finalreport-experts.pdf), but it is all the more important also for the IoT.

cloud technologies decrease the footprint of a virtual machine by approximately two orders of magnitude, allowing clouds to run on very small Things.[44] Other recent computing paradigms let foresee a growth of CoT, namely cloudlets,[45] fog computing,[46] and personal clouds.[47]

Evidence of the theoretical importance of CoT is provided, for instance, by the conferences on the topic[48] or also by ClouT[49], a joint European-Japanese project aiming at defining and developing a common virtualisation layer, allowing the access and management of Things, as well as cloud services. In that context, it has been demonstrated that CoT infrastructures can be cheap, easy to maintain, open-source based, compatible and interoperable with different platforms and services.[50]

We are on the verge of a shift from ubiquitous computing, to ubiquitous sensing and ubiquitous actuating. Obviously enough, new challenges arise, for instance because it emerges the need for "novel network architectures that seamlessly integrate the cloud and the IoT, and protocols that facilitate big data streaming from IoT to the cloud."[51] At the same time, not every cloud-related legal issue exists or has the same meaning

[43] It is interesting the work of Y. Benazzouz et al., *Sharing User IoT devices in the Cloud*, IEEE World Forum on Internet of Things (WF-IoT), 2014, 373, where they propose an IoT centric social device network based on a cloud computing model precisely because it provides a virtual execution environment thanks to its decentralized nature, high reliability and accessibility from anywhere and at any time.

[44] Cf. http://unikernel.org/.

[45] According to S. Bouzefrane et al., *Cloudlets Authentication in NFC-Based Mobile Computing, in 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 8-11 April 2014, 268-269, it is a "multicore computer installed in the public infrastructure with connectivity to remote cloud servers. Hence, the cloudlet is used by the mobile device to offload its workload while ensuring low delay and high bandwidth." The term was coined by M. Satyanarayanan et al., *The case for VM-based cloudlets in mobile computing*, IEEE Pervasive Computing 8 (2009), 14-23. Recent studies focus on the use of cloudlets (or edge computing) for the IoT (s., for instance, M. Satyanarayanan et al., *Edge Analytics in the Internet of Things*, in IEEE Pervasive Computing, Volume:14, Issue: 2, Apr.-June 2015, 24-31, which describes the GigaSight architecture, a federated system of VM-based cloudlets that perform video analytics at the edge of the Internet, thus reducing the demand for ingress bandwidth into the cloud.

[46] The term was coined in 2012 by researchers of Cisco;s. especially F. Bonomi et al., *Fog Computing and Its Role in the Internet of Things*, http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf, according to which "Fog Computing extends the Cloud Computing paradigm to the edge of the network, thus enabling a new breed of applications and services. Defining characteristics of the Fog are: a) Low latency and location awareness; b) Wide-spread geographical distribution; c) Mobility; d) Very large number of nodes, e) Predominant role of wireless access, f) Strong presence of streaming and real time applications, g) Heterogeneity." More recently, S. Sarkar-S. Chatterjee-S. Misra, *Assessment of the Suitability of Fog Computing in the Context of Internet of Things*, in *IEEE Transactions on Cloud Computing*, Volume: PP, Issue: 99, 1.10.2015, 1 as the number of applications demanding real-time service increases, the fog computing paradigm outperforms traditional cloud computing (the overall service latency for fog computing decreases by 50:09%). Therefore, in the context of IoT, with high number of latency-sensitive applications fog computing is better than traditional cloud techonologies.

[47] With the personal cloud, there is a shift from a Thing-centric mobile cloud computing, to a user-centric cloud computing experience where users are able to access their digital assets and services via apps across multiple Things in a seamless manner (A. Kazi-R. Kazi-R. Deters, *Supporting the personal cloud*, in *2012 IEEE Asia Pacific Cloud Computing Congress (APCloudCC)*, 14-17 Nov. 2012, 25-30).

[48] Along with the conferences cited sub note 23, s., e.g., the works of the three conferences 'Future Internet of Things and Cloud (FiCloud)' (http://www.ficloud.org).

[49] As one can read on the website http://clout-project.eu/, the overall concept of ClouT is leveraging cloud computing as an enabler to bridge the IoT with the Internet of People via the Internet of Services, to establish an efficient communication and collaboration platform exploiting all possible information sources to make the cities "smarter" and to help them facing the emerging challenges such as efficient energy management, economic growth and development (s. also https://vimeo.com/112706883).

[50] We refer essentially to P. Wright-A. Manieri, *Internet of Things in the Cloud. Theory and Practice*, CLOSER 2014, 4th International Conference on Cloud Computing and Services Science, Barcelona, 3-5.4.2014.

[51] *IEEE Internet of Things Journal Special Issue on Cloud Computing for IoT.*

in an IoT context. One need only consider that security is important in both cases, but whereas hacking a cloud can merely affect data[52] (albeit breach of personal data can be a substantive nuisance), accessing and remotely controlling Things can potentially impact the world jeopardising people's health and life.[53] And the cloud can play a critical role also to strengthen the security of a system, especially thanks to its role of mediator and coordinator. In fact, if data have to go through a cloudy validation process, the cloud can disconnect malicious Things or ignore their inputs; it can also let only valid data access the system, thus ensuring data integrity.[54]

Ⅳ. The Complexity of the Clouds of Things Ecosystem

I believe that the factors of the complexity of CoT are at least six. I have already mentioned the sectorial fragmentation.

The second factor can be well depicted as the Internet of Silos problem. The infancy state of certifications and the lacks of common standards and protocols render interoperability hard.[55] Interoperability is a critical aspect of CoT, whose essence is the creation of a system of Things that sense, communicate and actuate. When it comes to the CoT, one ought to look at the system and not at the single Thing. The 'system' dimension can be hindered by the fact that, unlike the cloud,[56] currently[57] each of the services in the different CoT sectors is in a silo; hence, one can hardly connect information between the relevant Things and services. Even though efforts have been made in terms of creating an environment favourable to the communication between CoT systems,[58] at the moment no one is able to offer third-party integration of CoT services. In this work, I take a long-run view; hence, I will assume that communication among systems works

[52] By 'cloud' here we mean the use of cloud computing in itself, not as a mediator of IoT communication. It is clear that if the cloud is controlling Things – either directly through commands, or indirectly describing 'events' that real-world things action – 'hacking the cloud' can cause real-world security issues.

[53] GCSA (29) refers to two examples: a cyber-attack that allowed to control steering and braking of a car and an hacker shouting at a sleeping child using a baby monitor. There are, however, many other examples: s., e.g., http://www.theregister.co.uk/2015/02/11/anonymous_hacks_fuel_station_monitoring_system/ about petrol stations. While we wait for general guidelines on cybersecurity, ENISA, the European Union Agency for Network and Information Security, has recently published a study that aims at securing domotics environments from cyber threats by highlighting good practices that apply to every step of a product lifecycle. See ENISA, *Security and Resilience of Smart Home Environments*, 1.12.2015, available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructu tures/smart-homes/security-resilience-good-practices.

[54] Singh et al. (6), 1.

[55] S., for instance, K. Kreuzer, *Eclipse Technologies for the Internet of Things and the Smart Home*, 12.5.2013, http://kaikreuzer.blogspot.co.uk/2013/05/eclipse-technologies-for-internet-of.html, where, apropos what he calls *cloudy things*, he stresses that 'these gadgets are connected to the Internet, but effectively they are totally disconnected from each other.' (it is though disputable his tripartition of the IoT in M2M, cloudy things and Intranet of Things). Cf. also B. Di Martino-G. Cretella-A. Esposito, *Advances in Applications Portability and Services Interoperability among Multiple Clouds*, in *IEEE Cloud Computing*, march/april 2015, 22, who, among other things, suggest the use of some ready-to-go solutions for portability and interoperability (namely, Docker, ElasticBox and Cloudify).

[56] One need only think that all websites on the Internet are connected and possibly linked, and all e-mail systems (whether webmail or desktop e-mail client) are in principle inter-working.

[57] This is only a state-of-the-art consideration: it is foreseeable that this will not be an issue at least in the long run.

[58] See, for instance, Google Weave, which reportedly provides seamless and secure communication between Things both locally and through the cloud; it shall drive interoperability across manufacturers (e.g. Nest) through a certification program that Things makers must adhere to. See more at https://developers.google.com/brillo/?hl=en.

without any particular obstacle.

Thirdly, there is the technical complexity.[59] At a high level, this means that the technologies involved are often unknown to the general public, which may now be familiar with the meaning of cloud computing, but could still not understand what RFID, near-field communication (NFC) or low energy Bluetooth (LEB). Education is needed to raise awareness and therefore trust in CoT. Technical complexity means also that computer scientists and engineers are still struggling with some technical aspects, for instance those related to the hardware constraints (small interfaces, reduced energy autonomy, difficulties in encryption), multi-tenancy (every Thing can be controlled by several people in numerous – potentially conflicting – ways), and the importance of tracking the data throughout the systemic flow, thus ensuring integrity and validity (e.g. IFC, sticky policies, etc.).

The fourth factor is what I call the contractual quagmire. At the Microsoft Cloud Computing Research Centre, Professor Ian Walden and I have studied a domotics scenario through an empirical research on the 'legals'[60] of Nest Inc., a CoT company providing thermostats, smoke alarms and cams. I will make use of the results of that research[61] This research has shown inter alia that against one single (simple) product, there are umpteen contracts, licences, notices, etc. These documents are difficult to find (sometimes they are not published) and they are nearly impossible to read and jointly interpret, not providing a uniform level of protection. Moreover, the CoT provider tends to waive any kind of responsibility also playing upon the corporate ramifications and, most importantly, a phony separation of software, hardware and services (whereas the Thing is an inextricable mixture of the three).

Fifthly, there is the regulatory jungle. A myriad of documents (opinions, guidelines, communications), none of which binding, generally lacking both the encompassing and coherent structure of the holistic approach and the granularity and concrete articulation of the sectorial approach.[62]

[59] Interoperability can be understood as a technical issue, but it is certainly more than that.

[60] The legals are all the legal documents relevant for those who purchase the Thing.

[61] Noto La Diega-Walden (15).

[62] Cf., to name only the main European documents on a single CoT sector (health), Directive 2011/24 on the application of patients' rights in cross-border healthcare; Green Paper on Mobile Health, 10.4.2014 (s. opinions ECOSOC 14.9.2014, CoR 4.12.2014); EDPS, opinion 1/2015 on Mobile Health, 21.5.2015; Comm. Staff WD on the existing EU legal framework applicable to lifestyle and wellbeing apps, 10.4.2014; Council EU, Conclusions on Safe and efficient healthcare through eHealth, 1.12.2009; 29WP, Health data in apps and devices, Annex to the letter to the Commission on 5.2.2015; 29WP, Opinion 3/2012 on developments in biometric technologies, 27.4.2012; 29WP, Working document on biometrics, 1.8.2003; 29WP, Opinion 6/2000 on the Genome Issue, 13.7.2000; Commun. "e-Health Action Plan 2012-2020 – Innovative healthcare for the 21st century", 6.12.2012 (s. Comm. Staff WD 6.12.2012, opinions EDPS 27.3.2013, ECOSOC 22.5.2013 and CoR 3.7.2013); Commun. on telemedicine for the benefit of patients, healthcare systems and society, 4.11.2008 (s. opinion ECOSOC 15.7.2009); Commun. "e-Health – making healthcare better for European citizens: An action plan for a European e-Health Area", 30.4.2004 (s. opinion CoR 17.11.2004); Commission White Paper "Together for Health: A Strategic Approach for the EU 2008-2013", 23.10.2007; Commission Implementing Decision "providing the rules for the establishment, the management and the functioning of the network of national responsible authorities on e-Health", 22.12.2011; Commission Recommendation on cross-border interoperability of electronic health record systems, 2.7.2008; Council conclusions on a safe and efficient healthcare through e-Health, 1.12.2009; Council conclusions on early detection and treatment of communication disorders in children, including the use of e-Health tools and innovative solutions, 2.12.2011; ETSI, Applicability of existing ETSI and ETSI/3GPP deliverables to e-Health, May 2007; ETSI, e-Health; Architecture; Analysis of user service models, technologies and applications supporting e-Health, February 2009; CoR, Opinion "Active ageing: innovation — smart health — better lives", 4.5.2012; eHealth Network, Guidelines on ePrescriptions dataset for electronic ex-

Too many, too vague.

The last but not least important factor of complexity pertains to the actors of CoT: who are they and which kind of relationships bind them? There is an extremely high number of actors involved in the supply chain and the relations between them can be both contractual as well as non-contractual. I will use the domotics scenario above illustrated to shed light on the CoT supply chain.

One of the main flaws of literature on IoT and CoT is that one gets the impression that everything is about the Thing, forgetting that human beings are and must be at centre of technologies aspiring to be sustainable and empowering. Therefore, let us start from the end-user (the patient, in the CoT-health use case), who is the main data subject (and sometimes data controller as well). The end-user, that is to say the end-user*s*. This is due mainly to two factors. First, multi-tenancy, which is an important characteristic of both cloud computing and IoT. In fact, the person[63] that concludes the CoT contracts the end-user may be the contracting customer, but the Thing may be used by the family members, temporary guests, friends, employees, etc. By the by this can create problems, as the Thing may receive inputs which are in contrast and damages may follow. The second factor is that one can own the Thing, but one can as well be a tenant. The difference may have also practical consequences. In terms of UK contract law, statute implies a term into the contract that the purchasers of a good (not the tenant) will “enjoy quiet possession”,[64] which term would be potentially breached if the Thing were disconnected or if some of its functionalities were taken away.[65]

If the end-users have generally not substantive power in the supply chain, the situation changes when it comes to the manufacturer of the Things. Better said, again, the manufacturer*s*. As said above, most Things will be composite, with different manufacturers responsible for the “Thing of Things”. Even when there is simply one Thing, during the process of manufacturing several different people will be involved, contributing components and facilitating the production process.

Even though startups and SMEs can play a critical role in some CoT sectors, it is clear that the production of products with hardware components can require costs that are not bearable by small businesses. At any rate, one can see how the IT transnational corporations are dominating the CoT. This has at least two effects on the relevant

change, 18.11.2014; eHealth Network, Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange, 19.11.2013; European Commission Decision C (2015)6776, Horizon 2020 Work Programme 2016-2017. 8. Health, demographic change and well-being 13.10.2015.

[63] A separate issue is that of the use of Things to contract. On Things that sell Things and Things that sell themselves see Hon-Millard-Singh (7), 12-13. An aspect which seems to preoccupy lawyers when it comes to artificial intelligence is their substitutions with machine (which they claim impossible, mainly given the creative nature of negotiations). More interesting aspects of the impact of AI on the law regard the conclusion of contracts by entirely autonomous systems (can they bind the natural or legal persons behind them?) and the liability for autonomous actions (in simple terms, now it would be probably seen as insane the arrest of robots, whereas it will not be the same when there will be the said convergence between Things-enhanced and Things-implanted human beings and autonomous Things).

[64] E.g. UK, Sale of Goods Act 1979, s. 12(2)(b).

[65] See *Rubicon Computer Systems Ltd. v United Paints Ltd* (2000) 2 T.C.L.R. 453. Noto La Diega-Walden (15), 6 calls it “the disconnected IoT device issue”. We have not touched another interesting, albeit not present, problem. I mean the right to be disconnected. Let us imagine a society where every thing is connected and private Things produce data flows and actions that necessarily interfere with public Things’s flows and actions. In such a scenario, can the citizens claim a right to be disconnected, notwithstanding the scale effect of decision of the kind?

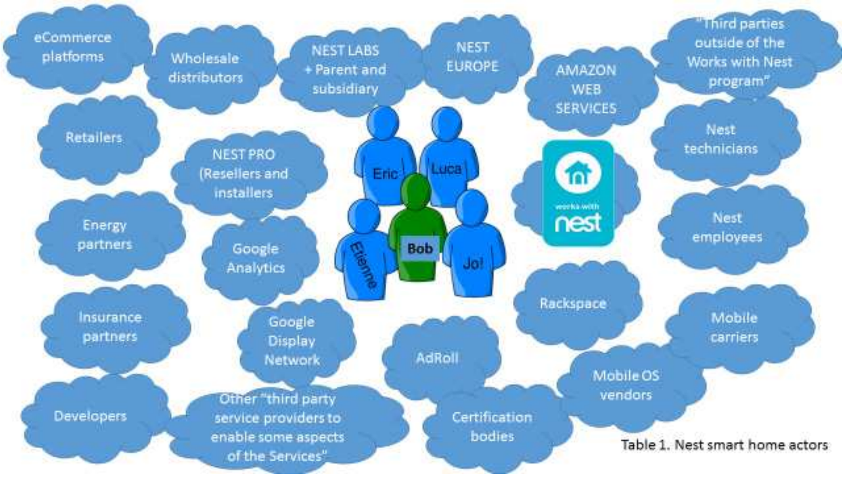

Table 1. Nest smart home actors

supply chain. Firstly, it is often difficult for the customer to understand the corporate structure of the companies involved. For instance, Nest Inc. has been bought by Google Inc., which is then become part of the multinational conglomerate Alphabet Inc., which controls also Calico, Google Capital, Google Fiber, Google Life Sciences, Google Ventures, Google X (that have their own subsidiaries). Nest Inc. controls Nest (Europe) Ltd. and has recently bought Dropcam Inc. The customer cannot always easily understand the identity of the party (or parties) with whom they are entering into a contract.

Secondly, consumer law and competition law have evolved in a direction that favours vertical integration arrangements. This is mainly due to the importance attributed by the law to pre-sale and post-sale services. One will not be surprised, then, when they find out that many CoT enterprises have their own resellers, retailers, wholesale distributors, and installers.

CoT is not only about hardware and software, but also about services[66]. A cloud provider may be used for web storage, whilst another cloud provider for redundancy. There are also the analytics tools critical for big data, online payment service providers, and advertising services providers. Alongside the main service (i.e. heating/smoke detecting in the Nest use case), the CoT provider partners with other enterprises offering collateral services. For instance, Nest is partnered with insurance companies as to the 'Safety Rewards' service,[67] with energy providers as to Rush Hour Rewards and Seasonal Savings.[68]

To complete the supply chain picture, one should also mention the website developer and webmaster, the 'app' store, the embedded software developer, the software providers, the facilitators of communication between things, the rights-holders, the eCommerce platforms, and the network

[66] In Noto La Diega-Walden (15), 11, we claim that the Thing is an inseparable mixture of hardware, software and service.

[67] Nest will let the insurer know that the smoke alarm is installed and working. In exchange, the insurer will take up to 5% off the insurance premiums.

[68] These services are based on machine learning technologies (so-called 'Auto-Tune'), which justifies the use of cloud computing (Auto-Tune "needs a huge amount of memory, storage and processing power, all maintained in the cloud", https://nest.com/support/article/What-is-Auto-Tune). The liability issues arising by AI and machine learning are out of the scope of this research.

operators.

The CoT, however, is not (only) about the single Thing. It is about the system, the network of Things, the communication within the system and between the subsystems. Consequently, one has to move from the number of actors named above and multiply it for the homologous actors of the interoperable apps and Things. Being aware of all the actors involved, let alone allocating responsibilities and liabilities (not only for data protection purposes), is not easy.

The complexity of the supply chain grows even more in certain sectors, such as the healthcare one. In fact, to the number obtained by the above descripted operations, one has to add doctors (physician, surgeon, physiotherapists, etc., but also the team), the national health service, hospitals (especially the hospital manager), GP Services, nurses, other employees (e.g. A&E), researchers, pharmacies, pharmaceutical companies, caregivers, data processing specialists, social security administrators, the patient's family and friends, biomedical laboratories, radiology centres, other specialty clinics, laboratory technologists, medical gas companies, other ancillary services, accountable care organizations (ACOs), health information exchange (HIEs), regional health information organizations (RHIOs), other care delivery organizations, providers of medical devices, drugs, etc. And I am probably leaving out several actors.

The intricacy of the environment does not help transparency and accountability, which are critical to build the citizen's trust in the CoT. Public and private stakeholders should cooperate to simplify contracts and regulations and to develop standards and protocols that ensure interoperability and security.

Ⅴ. Deployment and Regulation in the United Kingdom

CoT is already a visible reality in the UK. There are currently in excess of 40 million devices in the IoT within the UK. A study[69] predicted that this figure will grow more than eightfold by 2022, when the IoT will consist of 320 million devices and more than a billion daily data transactions.

The main example of this is that by the end of 2020, around 53 million "smart" meters will be rolled out as standards in all the houses of the Kingdom.[70] The government intends to protect the consumers by ensuring that there will be no sales during the installation visit and that installers must provide energy efficiency advice as part of the visit and they will need the consumer's permission in advance of the visit if they are to talk to them about their own products. As to privacy, suppliers will have to get the consumer's consent to access half-hourly data, or to use data for marketing purposes, but they can access daily data unless there is an explicit objection. It is noteworthy, from an antitrust/lock-in perspective, that consumers have the right to share data with third parties (such as switching sites) if they want to

[69] Aegis Systems Ltd–Machina Research, *M2M application characteristics and their implications for spectrum. Final report*, 2606/OM2M/FR/V2, 13.5.2014, available at http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/M2M_FinalReportApril2014.pdf. The report has been commissioned by Ofcom.

[70] See Department of Energy and Climate Change, *Smart meters: a guide*, 22.1.2013 (last updated 8.10.2013) at https://www.gov.uk/guidance/smart-meters-how-they-work. The number is potential, given the opt-in system chosen by the Government. See also Department of Energy & Climate Change–Ofgem (Office of Gas and Electricity Markets, UK regulator of energy), *Smart meters: information for industry and other stakeholders*, 22.1.2013, available at https://www.gov.uk/guidance/smart-meters-information-for-industry-and-other-stakeholders.

receive advice on the best tariff (a sort of portability right). From 2016 third parties will be able to access smart meter data remotely if the consumer gives them permission to do so.

The British reality of the IoT is about to grow significantly thanks to substantive public investments. Indeed, on 8.7.2015, the UK has passed its summer budget. At a cursory glance, it would seem that it provides £40 million for the IoT, with a focus on healthcare, social care and smart cities; its main implementation is IoTUK.[71] Ultimately, there are also £140 million for "infrastructure & cities of the future" and £100 million for "intelligent mobility". An important financial commitment ranging overall £280 million ($421 million). More recently, Ofgem (the UK regulator of the energy sectors) has announced £62.8 million to deliver smarter energy network for consumers.[72]

At the 2014 CeBIT Trade Fair in Hanover, the Prime Minister commissioned the GCSA to review how the UK could exploit the potential of the IoT. An advisory group, seminars and evidence from more than 120 experts in academia, industry and government have informed the review "*The Internet of Things: making the most of the Second Digital Revolution*" (also known as the *Blackett Review*)[73], published on 18.12.2014. It covers five sectors (transport, energy, healthcare, agriculture, buildings) and has three main goals. The first is to explain what government can do to help achieve the potential economic value of the IoT. The second is to set out what IoT applications can do to improve the business of government - maintaining infrastructure, delivering public services and protecting citizens. The third is to draw recommendations from this evidence. Indeed, the GCSA recommends ten actions about leadership, commissioningspecturm and networks, standards, skills and research, data, regulation and legislation, trust, coordination.

In the meantime, on 23.7.2014, the Office of Communications (Ofcom, the UK communications regulator) has published a call for inputs on "*Promoting investment and innovation in the Internet of Things*", aimed aimed to identify potential barriers to investment and innovation in the IoT (and on the role of the regulator).[74] The "*Summary of responses and next steps*"[75] has been delivered on 27.1.2015 and covers (in increasing order of importance according to stakeholders) network addressing, spectrum, network security and resilience, privacy and data protection. In the next paragraphs I will use these guidances to present a picture of IoT privacy, data protection, and consumer law in the UK; therefore, here I will merely give a short account of the other aspects.

Understandably enough, netword addressing is not of great importance, as telephone numbers are

[71] The IoTUK programme is an overarching and collaborative three year programme, as part of the Government's £40 million mentioned investment to maximise the UK's capabilities in the IoT. Powered by the Digital Catapult and the Future Cities Catapult, IoTUK seeks to increase the adoption of high quality IoT technologies and services throughout businesses and the public sector. The organisations include a city demonstrator, a research hub focussed on security and trust, a hardware accelerator, as well as a healthcare test bed. See more at http://iotuk.org.uk/about-us/.

[72] The announcement has been made on 30.11.2015 (see https://www.ofgem.gov.uk/publications-and-updates/ofgem-announces-62-8-million-deliver-smarter-energy-network-consumers).

[73] GCSA (29).

[74] The full text is available at http://stakeholders.ofcom.org.uk/binaries/consultations/iot/summary/iot-cfi.pdf.

[75] The summary of responses is available at http://stakeholders.ofcom.org.uk/binaries/consultations/iot/statement/IoTStatement.pdf.

"unlikely to be required for most IoT services". Ofcom, however, will monitor the progress of Internet service providers (ISPs) in migrating from IPv4 to IPv6 connectivity.

As to the spectrum, there are some ongoing initiatives such as the liberalisation of licence conditions for existing mobile bands, but even though they meet the actual demand of spectrum, this could not be the case in the long term. I would point out that recently Ofcom has launched a consultation on "More Radio Spectrum for the Internet of Things";[76] closed on 12.11.2015, the report has not been published yet. Its goal is to encourage M2M applications to use spectrum that will enable them to connect wirelessly over longer distances. This very high frequency (VHF) spectrum has different properties to other frequencies, already in use for the IoT, and can reach distant locations which other frequencies may not.

With computing becoming ubiquitous and with big data, it is unsurpring that network security and resilience are critical. Ofcom reports a growing demands both in terms of the resilience of the networks used to transmit IoT data and the approaches used to securely store and process the data collected by Things. As to cybersecurity, under the Digital Single Market strategy,[77] the European Commission is about to initiate the establishment a Public-Private Partnership on cybersecurity in the area of technologies and solutions for online network security. It will also launch an integrated standardisation plan to identify and define key priorities for standardisation with a focus on the technologies and domains that are deemed to be critical.

Before narrowing down to data protection and consumer law, one has to point out that, alongside legal instruments on the IoT as a whole, there also sectorial ones - such as the guidance issued by ICO on RFID[78] and the Smart Energy Code[79] - and horizontal ones, such as the the Consumer Rights Act 2015 (CRA). Even though the latter is not IoT-specific, it reflects this new market reality and provides interesting tools for the consumer, therefore I will take it into account in the following analysis.

Ⅵ. Data Protection and Privacy

When it comes to CoT, there is an undisputable interest for the data protection and privacy aspects (surprisingly, not so much for the security ones). This is due mainly to four factors. Firstly, the data processed are potentially almost always personal data because the Things are in/or the human

[76] The full text of the consultation is available at http://stakeholders.ofcom.org.uk/binaries/consultations/radio-spectrum-internet-of-things/summary/more_radio_spectrum_internet_of_things.pdf.

[77] European Commission, communication "A Digital Single Market Strategy for Europe", COM (2015) 192 final, issued on 6.5.2015.

[78] ICO, *Data Protection Technical Guidance Radio Frequency Identification*, 9.8.2006, available at https://ico.org.uk/media/for-organisations/documents/1590/radio_frequency_indentification_tech_guidance.pdf.

[79] The Smart Energy Code (SEC) came into force on 23 September 2013, when the Data Communication Company's (DCC) licence was granted (when the UK Government launched the smart meters plan, they introduced a new licensable activity relating to communications between suppliers and other parties and smart meters in consumer premises). The SEC is a multiparty contract which sets out the terms for the provision of the DCC's services and specifies other provisions to govern the end-to-end management of smart metering in gas and electricity. There is a consultation ongoing on the new content of the SEC, for Ofgem's response see https://www.ofgem.gov.uk/publications-and-updates/ofgem-s-response-department-energy-and-climate-change-s-july-2015-consultation-new-smart-energy-code-content-and-related-supply-licence-amendments.

body or abund in private spaces (e.g. domotics), thus being capable of gathering information hitherto unavailable to the public (and to law enforcement agencies, LEAs). Secondly, Things process enormous amounts of data (so-called big data). Thirdly, Things can potentially constantly communicate with other Things, systems, and people, hence the problem of the "weakest link" and of recombination (e.g. the cross-device identificatio n[80] and the adoption of IPv6).[81] Lastly, there is an increasing problem related to surveilance. As examples one may think to the Schrems ruling whereby the European Court of Justice declared invalid the Safe Harbour agreement following the Snowden case[82], the proposal for a EU directive on the use of Passenger Name Record (PNR),[83] the UK draft Investigatory Powers Bill[84] and the widespread use of automatic number plate recognition (ANPR) systems by UK police forces, which "represents one of the largest surveillance systems in the world."[85] The increase of surveilance is assertedly connected to counter-terrorism. In fact, 239 specific EU laws and policy documents have been adopted in the name of counter-terrorism between 2001 and 2013. Of those, 88 are legally binding.[86]

Europe in aware of these problems. See, for instance, the General Data Protection Regulation adopted on 27 April 2016. Under its recital 30, 'Natural persons may be associated with Online identifiers provided by their devices, applications, tools and protocols, such as Internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.[87]

[80] On the use of high-frequency sounds to covertly track across a range of devices s. C. Calabrese et al., *Comments for November 2015 Workshop on Cross-Device Tracking*, Letter of the Center for Democracy & Technology to the Federal Trade Commission, 16.10.2015, available at https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf.

[81] Unlike IPv4, with IPv6 every Thing will be uniquely identified, hence the latter can be easily considered as personal data.

[82] Judgment of the Court (Grand Chamber) of 6.10.2015, C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650. The Court found that the US do not provide an adequate level of protection to the personal data of overseas citizens.

[83] Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, ST 14024 2015 INIT - 2011/023 (OLP). On 4.12.2015, an agreement has been met. The PNR system allows access to passenger information i.e. names, contact details and credit cards. Details are collected from European carrier flights entering or leaving the Union and from carriers between member countries. According the EU privacy regulator, the European Data Protection Supervisor, it is "the first large-scale and indiscriminate collection of personal data in the history of the European Union" (N. Nielsen, EU counter-terror bill is 'indiscriminate' data sweep, in EuObserver, 9.12.2015, available at https://euobserver.com/justice/131457). See EDPS, Opinion 5/2015, *Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, 24.9.2015, where it observed inter alia that "non-targeted and bulk collection and processing of data of the PNR scheme amount to a measure of general surveillance" (par. 63).

[84] Draft Investigatory Powers Bill, November 2015, please see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf. Similar laws are being passed in other countries especially after the ISIL attacks of Paris.

[85] And it happens without any legal proper framework according to the UK's surveillance camera commissioner (http://www.v3.co.uk/v3-uk/news/2437161/uk-number-plate-monitoring-one-of-the-worlds-biggest-surveillance-systems).

[86] B. Hayes-C. Jones, *Report on how the EU assesses the impact, legitimacy and effectiveness of its counterterrorism laws*, Statewatch SECILE report, December 2013, 28, available at http://www.statewatch.org/news/2013/dec/secile-how-does-the-EU-assess-its-counter-terrorism-law.pdf, that recognise, among others, that "much greater weight appears to have been ascribed to the needs and assessments of law enforcement and security agencies than the other stakeholders".

Minimising concerns requires first of all ensuring that data are encrypted both in transmission and storage. In fact, one may think that given the power constraints of Things, encryption should be avoided since energy consuming. On the contrary, researchers have shown that, for instance, the Advanced Encryption (AES) Algorithm instead of consuming power, can save it.[88]

Moreover, one has to look into the Thing, to secure its components, and outside the Thing to secure all the communications. New methods of authentication, such as the multi-factor one, are critical.[89] Securing a system does not mean closing it. It is true that openness can to some extent lead to vulnerabilities, but these can be addressed in other ways and at any rate closing the system (thus hindering interoperability) equates with creating (that is to say reinforcing) the Internet of Silos.

Furthermore, businesses have to bind their employees to confidentiality agreements to ensure that the information is not sold to third parties.

Ofcom's statement on the IoT is rather unsatisfactory when it comes to the data protection and privacy aspects. Indeed, on the one hand the note that, insofar as the IoT involves the processing of personal data, it will be regulated by existing legislation such as the Data Protection Act 1998 (DPA). On the other hand, they call for the introduction of a common framework that allows consumers easily and transparently to authorise the conditions under which data collected by their Things are used and shared by others. A compromise position. At any rate, it is true that there is a lack of clarity about the conditions and purposes of processing. A recent research on apps permission in the Google Play store[90] has in fact shown that apps can seek 235 different kinds of permissions from smartphone users. Consumers are concerned with this issues, consequently, among all smartphone app users, six-in-ten downloaders have chosen not to install an app when they discovered how much personal information the app required in order to use it.

Even though the ICO has not issued an ad-hoc guidance, its response to the Ofcom's consultation of 1.10.2014 contains many useful indications.

In the UK, the rule is that unless a particular individual is identified - or is reasonably likely to be identified - by the subject collecting the information from the Thing, the information will not constitute personal data. I would add that given that multi-tenancy is a characteristic of both the cloud and IoT, one can not always know who is actually using the Thing. It is nonetheless true that inferential data grow in importance as a con-

[87] 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).

[88] Cf. F. Rao–J. Tan, *Energy consumption research of AES encryption algorithm in ZigBee*, in *International Conference on Cyberspace Technology (CCT 2014)*, 8–10 Nov. 2014, Beijing, 1–6, that demonstrate the fact that improved AES algorithm can not only reduce the code size, but also reduce the overall energy consumption of ZigBee networks.

[89] The bifactorial authentication will be increasingly insufficient. For instance, a malware hitting Android phones can intercept incoming SMS text messages, thus allowing to steal the one-time passwords (OTPs) often sent by banks as a form of two-factor authentication. See ABS, *Consumer advisory on malware targeting mobile banking*, 1.12.2015, available at http://www.abs.org.sg/pdfs/Newsroom/PressReleases/2015/MediaRelease_20151201.pdf. Cf. E.J. Kennedy–C. Millard, *Data Security and Multi-Factor Authentication: Analysis of Requirements Under EU Law and in Selected EU Member States*, Queen Mary School of Law Legal Studies Research Paper No. 194/2015, 30.4.2015, available at http://ssrn.com/abstract=2600795.

[90] K. Olmstead–M. Atkinson, *Apps Permissions in the Google Play Store*, 10.11.2015, available at http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/.

sequence the recombination of the data produced by all the Things of the system.

The DPA does not apply to every processing in the IoT, but I am not entirely convinced by the division proposed by the ICO between personal Things and less personal Things. The former, epitomised by the smartphone, produces personal data anche who collects the data is a data controller and therefore subject to the DPA. A TV would be the paradigm of a non-personal Thing, consequently the relevant processing would not be subject to the DPA.

The fact is that with the IoT the roles of data controller and data processor change dynamically and it is often impossible to identify the controller, even though tools such as information flow control (IFC) can help. Moreover, there is what I have *supra* called repurposing, therefore, a TV can be designed not to process personal data, but it can end processing very personal (even sensitive, e.g. health-relate) data.

Anyway, in the event the DPA does not apply, ICO suggests the introduction of industry codes of practice or other soft-law instruments. An interesting, albeit sector-specific, example is provided by the Draft Code of Conduct on privacy for mobile health (mHealth) applications.[91]

An aspect which ICO commendably stresses is that Things may not have a physical interface at all with which an individual can interact. Consequently, acquiring a valid informed consent can be difficult. It is true, but sometimes technology solves the problems it creates. One example is provided by holographic computers: a hologram could easily substitute a traditional interface.[92]

However, given the limited spread of holographic technologies, in the case of Things with small interfaces or with a lack of interface, one may need to access the information from another Thing such as a laptop. Therefore, the configuration software running on the computer will need to be coded securely.

Now, generally speaking it is true that the more limited the physical interface is, and the more complicated the underlying technical situation is, the more important it is that the Thing embodies the principle of privacy by design and privacy by default set forth by the GDPR. Nonetheless, at least three problems arise. Firstly, a strong implementation of the said approaches may create closed systems, thus hindering interoperability, innovation, and the functioning itself of IoT systems. Secondly, in order to embody privacy in the design, the manufacturer or the developer should be able to know beforehand the purposes of the processing, which is not always true, due to the here analysed repurposing. Thirdly, deep learning and AI technologies are becoming widely adopted, with the consequence, as to the point at issue, that the Things can reprogram themselves,

[91] The draft of this industry code has been presented by the editor Hans Graux of time.lex on 7.12.2015 and is available at http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=12378. A debatable choice is the one to impose the obligations only on the developer.

[92] See e.g. https://www.microsoft.com/microsoft-hololens/en-us. The use of holograms for law implementation should be further explored. For instance, holographic technologies can be used for anti-counterfeiting purposes. See. P.S. Divya-M.K. Sheeja, *Security with holographic barcodes using Computer generated holograms*, in *2013 International Conference on Control Communication and Computing (ICCC)*, 13-15.12.2013, IEEE, Thiruvananthapuram, 162-166. Thanks to the new definition of trade marks provided by the European trade marks reform package, holograms will be able to be registered as a trade mark. See art. 3(b) of the Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks (not yet implemented by the Member States), whereby the requirement of the graphical representation has been deleted.

thus expelling the privacy settings.

If, on the one hand, the users risk not be properly informed, on the other hand phenomena such as repurposing and combination of data and technologies such as predictive analytics and augmented reality, especially in a CoT and big data context, may give rise to the opposite, albeit intertwined, problem of the overload of information. The end-result is the same, since the users will not be properly informed.

Another important data protection principle is the seventh, whereby one should take appropriate technical and organisational measures against the unlawful processing and the loss of personal data. However, in the complex CoT ecosystem, if there is a security flaw it is not always easy to track down to the actual responsible actor.

Who owns old models of smartphones and tablets is well aware of another problem. Software lifecycles are by far shorter than the hardware ones and software projects become soon unsupported. If security updates are longer provided, there is an increasing security risk, let alone the fact that old Things stop to function because of this discrepancy. One solution may be making openly available the specifications of the hardware (OSH, open-source hardware). One can infer another solution from the fact that Chrysler had to recal 1.4 million cars for a bug fix in July 2015. I refer to the OTA, over-the-air updates, that is the wireless delivery of new software or data. However, one has to make sure that such backdoors are used only for security issues, which does not seem to be the case in the last Microsoft update. A lesson may be learnt also from the current fight between Apple and th FBI, where the company has refused the requeste of the federal agency to force a terrorist's iPhone. In Tim Cook's words, "the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession."[93)]

The ICO concludes by pointing out that, given that there will be fifty billion Things by 2020, the migration from IPv4 to IPv6 will be critical. With approximately two to the power of one hundred twenty four addresses (2^{124}), IP addresses will identify any Thing in space and time, thus likely becoming personal data.

While I was at the final stage of the revision of this paper, the ICO has issued a code of practice focused on the need to actively provide privacy notices.[94)] This code shows a more mature approach to the IoT (to which a section is dedicated) and the awareness of its peculiar characteristics, since it is specified that "[o]ften several data controllers will be involved in processing personal data and they will each have obligations to provide privacy notices to the user." The code makes the example of a fitness Thing and points out that both the manufacturer, the developer of a third-party app, the social-networking platform, and the health insurance company. It is notable the proposal to supplement the individual privacy

[93)] T. Cook, *A Message to Our Customers*, 16.2.2016, at http://www.apple.com/customer-letter/.

[94)] The code has been issued on 2.2.2016 by the Information Commissioner under section 51 of the Data Protection Act 1998. A related consultation on "Privacy notices, transparency and control - a code of practice on communicating privacy information to individuals" is ongoing and will close on 23.3.2016. The text is available here https://ico.org.uk/media/about-the-ico/privacy-notices-transparency-and-control-0-0.pdf.

notices by “a collaborative resource that brings all of the privacy information together into an end to end resource for the user.” Hopefully, companies will take advange of the collaborative potential of CoT.

Privacy and data protection are at the core also of the mentioned *Blackett Review*. The GCSA is not particularly enlightening on the poin, since it limit itself to underline the dimension of the phenomenon (twenty-five billion Things v seven billion three hundred million people) and the great potential for harm to security and privacy (it reports the baby monitor hacking).[95] As a policy recommendation, one could not disagree with the invitation to keep legislation to the minimum required to facilitate uptake.

Ⅶ. Consumer Protection and Property

In the ordinary language, data protection and privacy can be viewed as a part of the consumers protection. Technically, however, the former applies to the relationship between data subjects and data controller (and, especially with the GDPR, with the data processor), whilst the latter applies to the B2C relationships.[96]

A recent report has identified many challenges from a consumer law perspective, namely the development of hybrid products; the erosion of ownership norms; remote contract enforcement; lack of transparency; complex liability; lock-in to products and systems; locked out of alternatives; and security.[97]

The Consumer Rights Directive (‘CRD’)[98] looks rather influenced by the CoT developments. Indeed, digital content supplied in a tangible medium (in other terms, in Things) is now defined as ‘good’ (art. 2(3)). Moreover, ‘digital content’ means data which are produced and supplied in digital form “irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through *any other means*.” (recital 19, italics mine). One can access the content of their Thing from all the other Things they own and still they can make use of the remedies of the CRD.

Under art. 5(1)g)-h) and art. 6(1)r)-s), before the consumer is bound by a contract or any corresponding offer, the trader shall provide the consumer with the information about functionality and interoperability (for the contracts other than distance or off-premises ones, this goes with the proviso “if that information is not already apparent from the context”.) It may be useful to point out that the former means “the ways in which digital content can be used, for instance for the tracking of consumer behaviour” (recital 19), the latter, in turn, is defined as “the standard hardware and software environment with which the digital content is compatible” (ibid). Even

[95] See (53).

[96] The directives refer to consumer-trader relationship. Under art. 2(1) of the CRD, ‘consumer’ means “any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession”, whereas ‘trader’ means “any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive” (art. 2(2) CRD).

[97] Consumers International, Connection and protection in the digital age. The Internet of Things and challenges for consumer protection, April 2016.

[98] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

though, then, technical protection measures (TPMs) are more a matter of intellectual property law, it is commendable that the obligations of information cover them as well (art. 5(1)g) and 6(1)r)), given that not only they exacerbate the imbalance of power in B2C relationships, but they risk to contribute to the fragmentation of CoT, thus leading to the Internet of Silos.[99]

The main critique that I feel obliged to move the CRD regards the fact that consumers do not enjoy the right of withdrawal as set out in art.s 9 to 15 as to some contracts. Two of them are particularly relevant in a CoT context. Firstly, the 'service contracts' "after the service has been fully performed if the performance has begun with the consumer's prior express consent, and with the acknowledgement that he will lose his right of withdrawal once the contract has been fully performed by the trader" (art. 16(a)). Secondly, and maybe most importantly, the contracts for the supply of digital content "which is not supplied on a tangible medium if the performance has begun with the consumer's prior express consent and his acknowledgment that he thereby loses his right of withdrawal." Thus, consumers have a right to withdraw from purchases of digital content, such as music or video downloads, but only up until the actual downloading process begins. Users of Things know that one is hardly aware of the moment when the download begins. This is the weakest link in the chain.

The CRD has been implemented in the UK by Consumer Rights Act 2015 as amended ('CRA').[100] It is important, since it is the legal basis for the right to repair or replacement when digital content (e.g. online films, games, e-books) is faulty. The services should match up to what has been agreed, otherwise there is a duty to bring the service into line with the contract, unless this is not practical, in which case the consumer has the right to be reimbursed.

The remedial array of the CRA well accomodates CoT, since beforehand one could not do much in case of faults in the software and service components of Things. Moreover, must CoT contract, although American in the origin, they tend to make safe consumer protection laws, therefore inconsistent contractual sections should be unenforceable.

The weakest link of the CRA illuminates a peculiar relationship between ownership and data protection. Indeed, the CRA applies only to sales contracts, contracts for the hire of goods, hire-purchase agreements, and contracts for transfer of goods. A sales contract is not generally defined by the act, but under the CRD it is "any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price thereof, *including any contract having as its object both goods and services*" (art. 2(5), italics mine).

However, the CRA applies only if "being supplied, the goods will be owned by the consumer" (s.5(2)b)) and ownership is "the general property in goods, not merely a special property." (s.4(1)). Now, even when the consumer has property on the hardware (often they are merely tenants), they are not owners of software and service. Consequently, one could hardly claim the existence of a general property on the Thing and therefore the consumer could not seek remedy un-

[99] See more at http://europa.eu/rapid/press-release_MEMO-11-450_en.htm?locale=en.

[100] The last amendments have been introduced by The Consumer Rights Act 2015 (Commencement No. 3) (Wales) Order 2015.

der the CRD.

Ⅷ. (Not So) Final Remarks

This paper shows that the technological development epitomised by CoT leads to rethink some traditional concepts in matter of liability (especially for defective products), data protection, and consumer protection. This is the consequence of the nature of CoT, analysed through the prism of one of its specific characteristics, such as the 'repurposing'.

Repurposing suggests, among other things, that it is not useful to attempt sectorial taxonomies of the IoT/CoT, as a peculiar characteristic of those ecosystems is that a Thing is manufactured and/or provided for a purpose and then acts or produces information in an unforeseen way. Consequently, ideally regulators should intervene jointly in a gradual and soft way, like the good practice of the Italy Permanent Committee on Machine-to-Machine Communications shows.

This paper is the output of an ongoing research and future works should focus on the interaction between Things, cloud computing and AI technologies. In fact, when Things will (re)program themselves and take properly autonomous decisions (they are already doing so, to some extent), the effects of repurposing and recombination will be utterly unimaginable (let alone the consequences in terms of responsibility).[101]

CoT does not affect only legal principles, but also that vast realm that goes under the name of eHealth. CoT-health is an unexplored sector of eHealth and it promises to create a new era for healthcare, which will be decentralised, patient-centred, and dynamic. The use of health big data and of the flows generated by the Things can be extremely valuable, but legal scholars, healthcare professionals and computer scientists have to collaborate in order to overcome the Internet of Silos and make of CoT an empowering, inclusive, and safe ecosystem through increasing awareness and trust in society. If it true that "the most profound technologies are those that disappear",[102] we will have to be very alert.

As more and more Things will be connected and will produce valuable information, one will not have to fight for the right to access the Internet, but for the right to be disconnected, which I do not see on the horizon of this perennial-surveillance world.

〈References〉

Aazam, M. et al., *Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved*, Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th – 18th January, 2014, 414.

[101] A pioneering thought on autonomous machines was made by N. Wiener, *The Machine Age*, vers. 3, MIT, 1949, 8: "[i]f we move in the direction of making machines which learn and whose behaviour is modified by experience, we must face the fact that every degree of independence we give the machine is a degree of possible defiance of our wishes. The genii in the bottle will not willingly go back in the bottle, nor have we any reason to expect them to be well disposed to us (…) We can be humble and live a good life with the aid of the machine, or we can be arrogant and die." The full text is available at http://monoskop.org/images/3/31/Wiener_Norbert_The_Machine_Age_v3_1949.pdf.

[102] M. Weiser, *The Computer for the 21st Century*, Scientific American Ubicomp Paper after Sci Am editing, 1991, available at https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf.

Aegis Systems Ltd. and Machina Research, *M2M Application Characteristics and Their Implications for Spectrum. Final Report*, 2606/OM2M/FR/V2, 13.5.2014.

Amyx, S., *Why the Internet of Things Will Disrupt Everything*, July 2014, http://www.wired.com/insights/2014/07/internet-things-will-disrupt-everything/.

Atzori, L. et al., *The Social Internet of Things (SIoT) – When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization*, in *Computer Networks* 56 (2012) 3594.

Benjamin, W., *Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit*, in *Zeitschrift für Sozialforschung*, 1936, 5, I, 41.

Botta, A. et al., *On the Integration of Cloud Computing and Internet of Things*, 2014 International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, 27-29.8.2014.

Calabrese, C. et al., *Comments for November 2015 Workshop on Cross-Device Tracking*, Letter of the Center for Democracy & Technology to the Federal Trade Commission, 16.10.2015.

Christensen, C.M., *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, 1997.

Cook, T., *A Message to Our Customers*, 16.2.2016, at http://www.apple.com/customer-letter/.

Department of Energy and Climate Change, *Smart Meters: a Guide*, 22.1.2013.

Divya, P.S. and Sheeja, M.K., *Security with Holographic Barcodes Using Computer Generated Holograms*, in *2013 International Conference on Control Communication and Computing (ICCC)*, 13-15.12.2013, IEEE, Thiruvananthapuram, 162-166.

ENISA, *Security and Resilience of Smart Home Environments*, 1.12.2015.

FTC Staff Report, *Internet of Things. Privacy & Security in a Connected World,* January 2015.

GCSA, *The Internet of Things: Making the Most of the Second Digital Revolution,* 18.12.2014.

Hayes, B. and Jones, C., *Report on How the EU Assesses the Impact, Legitimacy and Effectiveness of its Counterterrorism Laws*, Statewatch SECILE report, December 2013.

Höller, J. et al., *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*, Oxford (MA), 2014.

Hon. Kuan, W. and Millard, C., and Singh, J., Twenty Legal Considerations for Clouds of Things (January 4, 2016). Queen Mary School of Law Legal Studies Research Paper No. 216/2016. Available at SSRN: http://ssrn.com/abstract=2716966.

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1, *Internet of Things (IoT): Preliminary Report 2014*, Geneva, 2015.

ITU (International Telecommunication Union), *The Internet of Things*, ITU Internet Reports 2005, November 2005.

International Telecommunication Union Standardization Sector (ITU-T), *Overview on the Internet of Things*, Y.2060, 06/2012.

Kennedy, E.J. and Millard, C., *Data Security and Multi-Factor Authentication: Analysis of Requirements Under EU Law and in Selected EU Member States*, Queen Mary School of Law Legal Studies Research Paper No. 194/2015, 30.4.2015, available at http://ssrn.com/abstract=2600795.

King, A.A. and Baatartogtokh, B., *How Useful Is the Theory of Disruptive Innovation?*, in *MIT Sloan Management Review*, Fall 2015.

McCarthy, D. and Morling, P., Using *Regulation as a Last Resort: Assessing the Performance of Voluntary Approaches*. Royal Society for the Protection of Birds: Sandy, Bedfordshire, 2015.

Mell, P. and Grance, T., *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-145, 2011.

Ministry of Science, ICT, and Future Planning (Republic of Korea), *Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution*, 8.5.2014.

Noto La Diega, G., *British Perspectives on the Internet of Things: The Clouds of Things-Health Use Case*, in *Internet of Things: Legal Issues and Challenges towards a Hyperconnected World*, Proceedings of the International Conference of the Center for Law & Public Utilities, Seoul National University, Honolulu (US), 27.11.2015, 45-150.

Noto La Diega, G. and Walden, I., Contracting for the 'Internet of Things': Looking into the Nest (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016. Available at SSRN:http://ssrn.com/abstract=2725913.

OECD, *Science, Technology and Industry Scoreboard 2015*, 19.10.2015.

Reed, C. and Stafanatou, D., *Legal and Regulatory Update - Embedding Accountability in the International Legal Framework*, forthcoming.

Sarkar, S., Chatterjee, S. and Misra, S., *Assessment of the Suitability of Fog Computing in the Context of Internet of Things*, in *IEEE Transactions on Cloud Computing*, Volume: PP, Issue: 99, 1.10.2015, 1.

Satyanarayanan, M. et al., *Edge Analytics in the Internet of Things*, in IEEE Pervasive Computing, Volume:14, Issue: 2, Apr.-June 2015, 24-31.

Advances in Clouds. Research in Future Cloud Computing, Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit, edited by L. Schubert and K. Jeffery, 2012.

Scroxton, A., *Half of UK Businesses Looking for Internet of Things Lead Roles*, in *ComputerWeekly.com*, 17-2-2016.

Singh, J., Pasquier, T., Bacon, J., Ko, H., and Eyers, D., *Twenty Security Considerations for Cloud-Supported Internet of Things*, in *Internet of Things Journal, IEEE*, 2015, 99, 1.

SRI Consulting Business Intelligence, *Disruptive Technologies Global Trends 2025*, Appendix F: The Internet of Things, available at http://www.internet-of-things.eu/resources/documents/appendix-f.pdf.

Technology Strategy Board, *Internet of Things (IoT) and Machine to Machine Communications (M2M) Challenges and Opportunities: Final paper*, May 2013.

Weber, R.H., and Weber, R., *Internet of Things. Legal Perspectives*, Springer, Heidelberg-Dordrecht-London-New York, 2010.

Weiser, M., *The Computer for the 21st Century*, Scientific American Ubicomp Paper after Sci Am editing, 1991.

Wright, P. and Manieri, A., *Internet of Things in the Cloud. Theory and Practice*, CLOSER 2014, 4th International Conference on Cloud Computing and Services Science, Barcelona, 3-5.4.2014.