The Internet of Citizens: A Lawyer's view on some Technological Developments in the United Kingdom and India*

Guido Noto La Diega†

> "*The social power, i.e., the multiplied productive force, which arises through the co-operation of different individuals as it is determined by the division of labour, appears to these individuals, since their co-operation is not voluntary but has come about naturally, not as their own united power, but as an alien force existing outside them, of the origin and goal of which they are ignorant, which they thus cannot control, which on the contrary passes through a peculiar series of phases and stages independent of the will and the action of man, nay even being the prime governor of these.*"
>
> —Karl Marx and Friedrich Engels,
> *The German Ideology* (1846)

I. Introduction

This article aspires to constitute a useful tool for both Asian and European readers as regards some of the state-of-the-art technologies revolving around the Internet of Things ('IoT') and their intersection with cloud computing (the Clouds of Things, 'CoT') in both the continents. The main legal issues

* This work is dedicated to the memory of Giulio Regeni and Valeria Solesin.

† 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). I am profoundly grateful to Ms. Ipshita Bhuwania, who skilfully assisted me during the research necessary for this work. This would not have been possible without the research previously undertaken at the Microsoft Cloud Computing Research Centre. The responsibility for this article and the errors therein are, however, solely mine. Any kind of feedback is welcome and can be emailed to noto.la.diega@gmail.com or tweeted to @guidonld.

emerging the refrom will be presented, with a focus on intellectual property, consumer protection, and privacy. The cases chosen are from India and the United Kingdom, two countries that are conspicuously active on this front.

The IoT is an expanding and heterogeneous universe encompassing all Things[1] which are capable of connectivity and are equipped with sensing and actuating capabilities. One can find Things in very diverse sectors, from agriculture to manufacturing, retail, healthcare, leisure, domotics, urban development, etc. Therefore, not only is providing an exhaustive and static definition of the IoT nearly impossible (or at least pointless), but also the endeavour of providing a complete picture of the phenomenon would be a cumbersome path towards failure. Consequently, I will give an account only of (what I consider to be) the highlights of the IoT in India and the United Kingdom.[2]

With respect to India, the selected speculative prism is composed of net neutrality, smart cities, manufacturing, computer-related inventions, and a recent bill on the surveillance aspects of the world's largest biometric database. In turn, I will look at the British context by analysing some (quasi) regulatory acts with a focus on privacy and consumer protection.

One last caveat; when it comes to new technologies, one tends to be either 'apocalyptic' or 'integrated'.[3] Either the technology will save us all by leveraging a revolution leading to a disruptive innovation,[4] or it will destroy our lives and the world will go to the dogs. I take a middle position and believe that through education, collective awareness, and soft law, one will be able to keep the human being at the centre, to unite people rather than divide them, to empower them and alleviate discrimination and poverty. What is important is neither should one delegate to technology nor to rely entirely on

---

1 I suggest using 'Thing' instead of 'smart device', 'smart home', etc., for at least two reasons. Firstly, most new products are designed with 'smart' capabilities, thus if everything is smart, nothing is. Secondly, 'smartness' and 'intelligence' are human attributes and one does not want to commit the epistemological crime named 'anthropocentricism'.

2 I will necessarily leave out some important aspects. For instance, reportedly, on March 2, 2016, the Andhra Pradesh Cabinet adopted an IoT (Internet of Things) policy to set up ten IoT hubs with the active participation of the private sector and create fifty thousand jobs. However, the news reported in the media is currently not substantiated by the text of the proposal. It is not clear how this policy will interact with the central one and with the guidelines on smart cities.

3 I refer to Umberto Eco, Apocalittici e integrati. *Comunicazioni di massa e teorie della cultura di massa* (1964), which analysed mass culture and mass media (for the American version, *see* Umberto Eco and Robert Lumley, Apocalypse postponed (Flamingo, 1994)).

4 For a critique, *see also* Guido Noto La Diega, *Clouds of Things. Data protection and consumer law at the intersection of cloud computing and the Internet of Things in the United Kingdom*, Journal of Law and Economic Regulation (forthcoming).

government: if the IoT is to actually become a revolution, it will do so due to the commitment of each and every one of us who will contribute to create the Internet of Citizens.[5]

II. Internet of Things: risks and regulatory options

The problem of access to the Internet becomes even more pressing given the most recent technological developments that go under the names of IoT, smart cities, Industrial Internet, web 3.0, etc. In simple terms, the Things talk to people and to other 'Things', affecting the physical world (unlike the traditional problems related to "pure" cloud computing).

The presence of Things in our everyday life gives rise to many problems. Let me name just what I consider the three main issues: surveillance, commercial exploitation of big data, and security.

This is not the place to go deep into (Government) surveillance, but to sell the idea of the importance of the phenomenon (and the connected hypocrisies),[6] it is sufficient to remember that the European Court of Justice has invalidated the Safe Harbour scheme,[7] an international agreement between the EU and the US which had been the legal basis for the transnational flow of personal data for fifteen years. The real, albeit partly not declared, reason for the ruling is the fear that the American agencies spy on European citizens (and governments). Surveillance will be the subject of a separate paragraph, since India has recently made headlines by passing a bill which enables the sharing of biometric data for security and public interest reasons.

Things are inside of us (pills and more generally 'ingestibles'), on us (wearables, implantables, etc.) and around us (domotics, robotics, etc.). We are growing so used to these Things, that we do not even notice them and are getting dependent on them. A good example is provided by the prevalence of mobile phone overuse among British adolescents aged 11–14 which was

---

[5] There are several projects that pursue this goal. One of them is http://hubofallthings.com/what-is-the-hat/. All the URLs of this work have last been accessed on March 21, 2016.

[6] I use the strong term 'hypocrisy' because the European governments have reacted to the Snowden case and kindred scandals as if they would not carry out surveillance activities on citizens and foreign governments themselves.

[7] Judgment of the Court (Grand Chamber) of October 6, 2015, C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner*, ECLI:EU:C:2015:650; *cf.* Mantelero, Alessandro: *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per i cittadini ed imprese?*, in *Contratto e impresa / Europa*, 2015, 719.

reportedly 10% in 2014,[8] whilst in 2012, 39-44% of the homologous group in India appeared to be addicted to mobile phones.[9]

Consequently, governments can enter hitherto inaccessible spaces, that is, private homes and the body itself. This is an unprecedented opportunity for law enforcement agencies (LEAs)[10] and it is not the case that surveillance laws are proliferating everywhere.[11]

The second risk is the use of this data for commercial purposes. Predictive analytics enabled by cloud computing, machine learning, and other "artificial intelligence" (AI) technologies, applied to big data, constitute an unprecedented opportunity for companies willing to trade the users' personal data and use it for profiling, targeted advertising and the like.

Thanks to IoT, companies can combine raw data flowing through various Things and infer personal or even sensitive data. One would think immediately about cookies, which are a traditional threat and whose misuse is being dealt with, in somewhat contrasting manners, by legislators[12] and the

---

[8] O Lopez-Fernandez *et al*, *Prevalence of problematic mobile phone use in British adolescents*, 17(2) Cyberpsychology Behaviour and Social Network, 91–98 (2014) *available at* doi:10.1089/cyber.2012.0260.

[9] Pedrero Pérez EJ *et al*, *Mobile phone abuse or addiction: A review of the literature*, 24 Adicciones 139–152 (2012).

[10] According to the U.S. Director of National Intelligence, James Clapper, Things in homes are new opportunities for spying. *See* Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee (February 6, 2016) (statement of James Clapper), *available at* http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

[11] *See* the Investigatory Powers Bill, where the word 'bulk' appears 402 times, but the UK Government alleges that it is not about mass surveillance; *see also* the widespread use of automatic number plate recognition (ANPR) systems by UK police forces, which "*[c]ould be one of the world's largest non-military surveillance systems (…) But who ever gave their consent to this, where is the legislation and where was the debate in parliament? So, I argue that some forms of surveillance have no legislative framework whatsoever*" (T. Porter, Humanity vs Surveillance, Commissioner's speech to Stirling University (November 23, 2015)), *available at* https://www.gov.uk/government/speeches/humanity-vs-surveillance-commissioners-speech-to-stirling-university). More generally, *see* FRA, *Surveillance by intelligence services. fundamental rights safeguards and remedies in the EU* (November 2015), available at http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services. In India, the Centre for Development of Telematics's Central Monitoring System is reportedly among the worst in the world. According to Reporters Without Borders, *Enemies of the Internet*, Report (2014), *available at* http://en.rsf.org/enemies-of-the-internet-2014-11-03-2014,45985.html. The Central Monitoring System allows the government direct, unlimited and real-time access to a wide variety of electronic communications without relying on internet service providers and gives the authorities a free hand to mount major surveillance operations against users of the web and other telecommunication technology.

[12] Under art. 5(3) of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('e-Privacy directive'), "the use of electronic

courts.[13] A good step in this direction would be to curb, the adoption of the new rules proposed by the Federal Communications Commission (FCC), which concerns the ability of businesses to share data about users' activities with advertisers without the users' consent.[14] Furthermore, a new non-rhetorical discussion on consent should be started, but this is not the place for that.[15]

Cookies, web beacons, device fingerprinting and kindred phenomena are interesting,[16] but it is submitted that cross-device tracking[17] is what is more directly relevant to the IoT and, maybe more dangerous since people are not aware of it.

---

communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller.". *Cf.* Article 29 Working Party, Opinion 4/2012 on Cookie Consent Exemption (June 7, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf, and Article 29 Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies (October 2, 2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf. The Article 29 Working Party can be broadly considered as the European regulator of data protection.

13 *Cf.*, *e.g.*, *Vidal-Hall* v. *Google Inc.*, 2014 *EWHC* 13 (QB), about the distress suffered by users of Apple Things from learning that their personal characteristics formed the basis for Google's targeted advertisements and from having learnt that such matters might have come to the knowledge of third parties who had used or seen their Things. The claimants used Apple's Safari browser, which was set to block Third Party Cookies that would enable the tracking and collation of browser activity. They pleaded that a Safari workaround operated by Google allowed it to obtain and record information about their Internet use and use it for the purposes of its AdSense advertising service. The High Court, Queen's Bench Division held, among other things, that 'damage' under the Data Protection Act 1998 need not necessarily have an economic aspect.

14 FCC, *Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice, Transparency & Security with Respect to Their Data* (March 10, 2016), *available at* https://www.fcc.gov/document/broadband-consumer-privacy-proposal-fact-sheet.

15 First of all, do the users have the actual possibility of dissenting? Do they understand what they are consenting to? Are there not other justifications for the processing of personal data? Should we not be more realistic? The answers to these questions should be the basis of future research.

16 *See*, *e.g.*, Article 29 Working Party, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting (November 25, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf.

17 On the use of high-frequency sounds to covertly track across a range of devices, *see* Chris Calabrese *et al*, *Comments for November 2015 Workshop on Cross-Device Tracking*, Letter from the Center for Democracy & Technology to the Federal Trade Commission (October 16, 2015), *available at* https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf.

It may be true that "*automatically sharing web activity information between devices has the potential to improve the usability of the mobile web*",[18] but the use of high-frequency sounds to covertly track across a range of devices is an activity that can hardly be regarded as fair, let alone legal, and it is not the case that this issue has attracted the interest of the Federal Trade Commission ('FTC').[19] Consequently, by combining the information produced or flowing through a user's Things, companies can have a complete picture of the user's profile and preferences.

This situation is made even worse by the oligopolistic structure of the IoT market. The biggest transnational corporations are very active in mergers and acquisitions, which are, *inter alia,* ways to have access to the data owned by the acquired company. Therefore, for instance, if I have a Nest smart thermostat, smoke detector or camera, I am aware that I am sharing my personal data with Nest, but may not be aware that Nest is sharing my data with its parent Google (now part of the holding Alphabet). Likewise, one should not be surprised if, once they have added someone's number on WhatsApp, Facebook will suggest this person's 'friendship'. One may argue that the fact that I am "friends" with someone does not identify me, therefore it is not a personal datum. However, as a user of many social network platforms, I have often inferred a lot of personal information merely from observing someone's list of "friends". For instance, their political opinions, religious beliefs, social class and sexuality are easy to glean from their social media profiles. If I can do it myself, let us not even imagine what big data analytics tools can do.

Let us have a look, for instance, at the privacy policy of the instant messaging mobile app.[20] The company states that, whereas the Status Submissions[21] are openly accessible, "*[t]he contents of messages that have been delivered by the WhatsApp Service are not copied, kept or archived by WhatsApp in the normal course of business.*" It is not clear what happens in moments or activities falling outside 'the normal course of business'. Indeed, elsewhere in the same policy, one reads that "*WhatsApp may retain date and time stamp information associated with successfully delivered messages and the mobile phone numbers involved in the messages, as well as any other information*

---

[18] Shaun K. Kane, *et al.*, *Exploring cross-device web use on PCs and mobile devices,* Human-Computer Interaction–INTERACT 2009 722-735 (Springer Berlin Heidelberg, 2009); *Cf.*, more recently, Jokela, *et al*, *A diary study on combining multiple information devices in everyday activities and tasks*, Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM (2015).

[19] On the workshop on cross-device tracking, *see* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.

[20] Privacy notice (July 7, 2012), *available at* https://www.whatsapp.com/legal/.

[21] Text, profile photos and other communications submitted by the user.

which WhatsApp is legally compelled to collect." Is the stamp retained only if the company is legally compelled? By the by, when would the company be legally compelled? Then, on further reading, it is found that "*[f]iles that are sent through the WhatsApp Service will reside on our servers after delivery for a short period of time*". How long does this "short period" last? Apropos the servers, it is important to remember that, even though the Privacy Shield that will substitute the Safe Harbour is not effective yet,[22] "*you are transferring your personal information to the United States and you expressly consent to that transfer and consent to be governed by California law for these purposes*." This transnational flow is happening without a legal basis.

WhatsApp collects user-provided information, cookies information, and log file information. Even though, professedly, they will require the user's consent to use personal data for marketing purposes, they will nevertheless use this data to "*track (…), and analyz(e) user preferences and trends*." Moreover, and most importantly, your personal data is shared with third parties for commercial purposes even without your consent, if this sharing is "*part of a specific program or feature for which you will have the ability to opt-in or opt-out*." The fact that one does not opt out should not be considered as equivalent to consent. Besides, personal information will be shared not only for law enforcement purposes,[23] but also for contractual enforcement ones. Indeed, the company "*reserves the right to disclose Personally Identifiable Information*[24] *(…) that WhatsApp believes, in good faith, is appropriate or necessary to enforce our Terms of Service, take precautions against liability, to investigate and defend itself against any third-party claims or allegations (…), and to protect the rights, property, or personal safety of WhatsApp, our users or others*." A quite broad provision, one may

---

[22] On February 2, 2016, the EU and the US agreed on a new framework for transatlantic data flows: the EU-US Privacy Shield. The College of Commissioners has mandated Vice-President Ansip and Commissioner Jourová to prepare a draft adequacy decision, which should be adopted by the College after obtaining the advice of the Article 29 Working Party and after consulting a committee composed of representatives of the Member States. In the meantime, the U.S. side will make the necessary preparations to put in place the new framework, monitoring mechanisms and the new Ombudsman. The draft adequacy decision (*available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf) and the text of the Privacy Shield (*available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf) have been presented on February 29, 2016.

[23] Reportedly, in March 2016, the US Department of Justice had been discussing how to proceed in a criminal investigation in which a federal judge had approved a wiretap, but investigators were stymied by WhatsApp's encryption. *See* M. Apuzzo, *WhatsApp Encryption Said to Stymie Wiretap Order*, The New York Times (March 12, 2016), *available at* http://www.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html?smid=pl-share.

[24] 'Personally identifiable information' is the American equivalent of the European 'personal data.'

argue. The most peculiar section, though, regards "Your choices": what can the user do to protect his data? Firstly, if they do not agree with the terms imposed by the company, they must uninstall the app. Fair enough, but there is also the possibility of using the app without providing personal information. True, but if you do so, "*WhatsApp may not be able to provide certain services to you.*"

This is *inter alia* a reminder that even when we are not paying for a service, we are actually paying for it with our data: we are all digital labourers.

I have not found the contractual basis of the sharing of data between WhatsApp and Facebook. Is it where the former says "*We may share your Personally Identifiable Information with third party service providers to the extent that it is reasonably necessary to perform, improve or maintain the WhatsApp Service*"? Is Facebook an actual third party? Is this sharing *necessary* to improve the instant messaging services? It is for posterity to judge.

Given the network effect of most IoT markets, new entrants find it particularly hard to stay in the market. My suggestion is to use privacy-friendliness as a competitive advantage, building on it a strong marketing strategy.

Lastly, but not less importantly, the IoT can jeopardise people's lives insofar as a security breach can lead to a hacker controlling your car, an oil station, a surgeon robot, etc.

With "pure" cloud computing deployments, one risks a breach of data or the unauthorised use of one's personal data by third parties. Even though one should not undermine the importance of such threats, it is non-debatable that diverting the course of a car, leading it against a group of children, playing with the valves of an oil station, or remotely controlling a robot during a surgery operation can be riskier.

III. Internet of Things: risks and regulatory options

Unlike the Cloud,[25] there is neither commonly accepted definition nor taxonomy of the IoT.[26] However, the latter has been recently defined by the ISO

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

[26] In March 2015, I made a survey of the existing definitions of the IoT and collected 64 definitional attempts, none of which is entirely convincing. I would not be surprised if this number were doubled now. NIST (National Institute of Standards and Technology) is

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*."[27] Whereas the ISO/IEC formula can be roughly accepted as a starting point (with the caveat of the introduction), the Microsoft Cloud Computing Research Centre prefers to look at the Thing,[28] understood as any physical entity capable of connectivity that has a direct interface with the physical world (i.e. a sensing and/or actuating capability).[29] From another perspective (especially product liability), Things can be understood as an inextricable mixture of hardware, software, and services.[30]

Things may be attached (e.g. wearables) or embedded (e.g. pacemakers).[31] They are usually composite- smartphones and connected cars being the simplest examples.[32] Virtual entities are not Things, notwithstanding the ITU's

---

working on some definitions. It is notable that the *Draft Framework for Cyber-Physical Systems* of September 2015 refers 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.

[27] 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 (*available at* http://www.iso.org/iso/internet_of_things_report-jtc1.pdf); its Special Working Group 5 (SWG 5 'Internet of Things') established, among other things, 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.

[28] I will refer to 'Thing' to distinguish it from ordinary 'things'.

[29] W. Kuan et al., *Twenty Legal Considerations for Clouds of Things*, Queen Mary School of Law Legal Studies Research Paper No. 216/2016 (January 4, 2016), *available at* SSRN:http://ssrn.com/abstract=2716966, 4.

[30] *See* more broadly G. Noto La Diega & I. Walden, *Contracting for the 'Internet of Things': Looking into the Nest*, Queen Mary School of Law Legal Studies Research Paper No. 219/2016, *available at* SSRN:http://ssrn.com/abstract=2725913.

[31] Things may also not have any physical contact with human beings. Let us think about 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, 5, I, 41-68 (1936), *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, "*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.* "

[32] A smartphone contains a large number of sensors and 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-thing's actors should be liable. Generally speaking and unless 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

definition, whereby a Thing is "*an object of the physical world (physical thing) or the information world (virtual thing), which is capable of being identified and integrated into communication networks*."[33] Human beings and animals are not Things. Not yet, at least. It is likely that evolutions in artificial enhancement techniques (AE) and in implants technologies will be at some point so developed 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!), the moment will not be clear when we cease to be human, having become androids and thus Things. When that day will come, we will not dispute what 'Thing' means, but what 'human' does.[34]

Given the complexity of the relevant ecosystem(s), one solution to simplify is to break it down by adopting a sectoral taxonomy, whereby one ought to consider separately, health (e.g. robot surgery), city planning (e.g. "smart" cities), manufacturing (e.g. 3D printing), distribution (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 could constitute the basis for criticising my proposal for a holistic regulation of the IoT. The objection would not necessarily fall short. However, there is a significant overlap between most of the sectors (one need only think of drones and BYOD, which can potentially fall under any category). This is *inter alia* demonstrated by the fact that regulators complain that they encounter lack of competence when trying and regulating the IoT, mainly because of these overlap. Their counterpart is the

---

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 one 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 scrutiny are required).

[33] 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.

[34] At the same time, Things will become more and more autonomous, thanks to the developments in 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 human intelligence.

overlapping of competences between different regulators (e.g. communications and data protection).[35]

Moreover, and maybe most importantly, one critical characteristic of IoT systems is repurposing. 'Repurposing' can be understood 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 the system to perform actions and produce information which the single Thing was incapable of; ii. under certain conditions (e.g. emergency) the system may reconfigure either in an automated fashion or a user-initiated one.[36]

Consequently, what is the best regulatory option for the IoT? Recent studies have shown that self-regulation is not a satisfactory option.[37] Traditional regulation, however, would lack the necessary flexibility required by the constantly changing technological landscape. Therefore, co-regulation seems to be the appropriate option,[38] providing a clear general framework of rules, whose implementation is left to private stakeholders. That said, how do we strike a balance between a one-size-fits-all regulation of the IoT and a fragmented one? The relevant best practice is provided by Italy, which has recently established a permanent committee on machine-to-machine

---

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

[36] 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.

[37] According to D. McCarthy & P. Morling, *Using Regulation as a Last Resort: Assessing the Performance of Voluntary Approaches*, Royal Society for the Protection of Birds: Sandy, Bedfordshire 10 (2015), most self-regulatory schemes (82%) perform poorly (*Contra*, FTC () 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."

[38] 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.

(M2M) communication,[39] where regulators and ministers can coordinate their initiatives.[40]

The UK Government Chief Scientific Adviser (GCSA)[41] has specified that "*[l]egislation should be kept to the minimum required to facilitate the uptake of the Internet of Things*",[42] 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.*"[43] I do not entirely agree with a legislative instrument, let alone anticipatory regulation.

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.*"[44]

---

[39] Machine-to-Machine communications, also known as Machine Type Communication (MTC), is "a rapidly growing area with the potential to significantly affect mobile telecommunication 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*, June 15, 2012, *available at* http://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-IOT-2012-M2M-PDF-E.pdf) There is no agreement on whether M2M ought to be considered a precursor to 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}*, September 11, 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), 14 2014, 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."

[40] On November 25, 2015, the *Comitato permanente per i servizi di comunicazione Machine to Machine* (permanent committee for M2M communication services) was 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* (transport 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.

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

[42] GCSA, *The Internet of Things: making the most of the Second Digital Revolution,* 9 (December 18, 2014) (also known as the Blackett Review).

[43] *Id*, at 9.

[44] *Id*.

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 the highest level, based on fundamental normative principles rather than on detailed prescriptions for behaviour.[45] However, we know how slow the formation of an international consensus can be and we have to act immediately, otherwise we risk closing the stable door after the horse has bolted.

IV. Cloud of Things

If the IoT is an understudied phenomenon, its intersection with cloud computing has also been mostly overlooked. The CoT[46] can be understood as "*ecosystems in which there are communications between things and clouds, including M2M communications mediated by cloud*."[47] Even though only part of the IoT is currently based on cloud technologies, these are becoming more and more common and are raising noteworthy issues.

The relation between the IoT and cloud computing has heretofore been fuzzy.[48] 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*",[49] against those who affirm that the cloud is what has made the IoT possible.[50] A position in the middle of the opposing views should be taken.

---

[45] C. Reed & D. Stafanatou, *Legal and Regulatory update – embedding accountability in the international legal framework* (forthcoming). Thanks to the Authors for sending the manuscript.

[46] 'Clouds of Things' has been the object of the 2nd annual Symposium of the Microsoft Cloud Computing Research Centre, held in Windsor from October 26-27, 2015. *See 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 (*available at* 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.

[47] Hon et al., *supra* note 29, at 7.

[48] 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), 23 (Barcelona, August 27-29, 2014), 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.

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

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

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 as the mediator and coordinator between Things. One needs to then think of big data,[51] analytics[52] and the constrained on-board (processing, storing, and battery) capacity of Things that make fundamental 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[53] and its co-essential open sharing.[54] Furthermore, cloud accessibility addresses the fact that many Things are worn (or anyhow part of our everyday life), hence it is crucial for the user(s)[55] to be able to access the services and applications regardless of their temporary geographical location.[56] Finally, new cloud technologies decrease the footprint of a virtual machine by approximately two orders of magnitude, allowing clouds to run on very small Things.[57] Other recent computing paradigms allow us

---

[51] *Cf.* M. Aazam et al, *Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved*, (Proceedings of the 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) 414 (Islamabad, Pakistan, January 14-18, 2014)), 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 IoTs 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 IoTs and develop smart applications for the users.'

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

[53] *Cf.* L. Atzori et al., *The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization*, 56 Computer Networks 3594 (2012) 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) (Bangalore, India, January 6-10, 2015), IEEE Proceedings, 2015. For the basic concepts of the social Internet of Things, *see* http://www.social-iot.org/.

[54] 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 163 (November 6-8, 2012)).

[55] 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 & K. Jeffery, 12 (2012), *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.

[56] The work of Y. Benazzouz et al., *Sharing User IoT devices in the Cloud*, IEEE World Forum on Internet of Things (WF-IoT) 373 (2014), is interesting, 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.

[57] *Cf.* http://unikernel.org/.

to foresee a growth of the CoT, namely cloudlets,[58] fog computing,[59] and personal clouds.[60]

Evidence of the theoretical importance of CoT is provided, for instance, by the conferences on the topic[61] and also by ClouT,[62] a joint European-Japanese project, aimed 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 infrastructure can be cheap, easy to maintain, open-source based, compatible and interoperable with different platforms and services.[63]

---

[58] 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) 268-269 (April 8-11, 2014), 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*, 8 IEEE Pervasive Computing 14-23 (2009). Recent studies focus on the use of cloudlets (or edge computing) for the IoT (*see*, for instance, M. Satyanarayanan *et al*, *Edge Analytics in the Internet of Things*, 14(2) IEEE Pervasive Computing 24-31 (April-June 2015), 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).

[59] The term was coined in 2012 by researchers of Cisco; especially F. Bonomi *et al Fog Computing and Its Role in the Internet of Things*, *available at* 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 et al., *Assessment of the Suitability of Fog Computing in the Context of Internet of Things*, in PP(99) *IEEE Transactions on Cloud Computing* 1 (October 1, 2015). 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 technologies.

[60] 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 et al., *Supporting the personal cloud*, in 2012 IEEE Asia Pacific Cloud Computing Congress (APCloudCC) 25-30 (November 14-17, 2012)).

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

[62] 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 face emerging challenges such as efficient energy management, economic growth and development (*see also* https://vimeo.com/112706883).

[63] 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, April 3-5, 2014).

We are on the verge of a shift from ubiquitous computing, to ubiquitous sensing and ubiquitous actuating. Obviously enough, new challenges arise, for instance, the emergence of 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*."[64] At the same time, not every cloud-related legal issue exists or has the same meaning in an IoT context. One need only consider that security is important in both cases, but whereas hacking a cloud can merely affect data[65] (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 lives.[66] The cloud can play a critical role, also to strengthen the security of a system, especially thanks to its role as a mediator and coordinator. In fact, if data has 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 to the system, thus ensuring data integrity.[67]

V. The complexity of the Cloud of Things ecosystem

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

The second factor can be well depicted as the Internet of Silos problem. The infancy state of certifications and the lack of common standards and protocols render interoperability hard.[68] Interoperability is a critical aspect

---

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

[65] By 'cloud' here we mean the use of cloud computing in itself, and 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 act on – 'hacking the cloud' can cause real-world security issues.

[66] GCSA (42) refers to two examples: a cyber-attack that allowed one to control steering and braking of a car and a hacker shouting at a sleeping child using a baby monitor. There are, however, many other examples: *see*, *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*, December 1, 2015, *available at* https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices.

[67] J. Singh, et al., *Twenty Security Considerations for Cloud-Supported Internet of Things*, PP (99) IEEE Internet of Things Journal 1, pp. 1–15 (2015).

[68] *See*, for instance, K. Kreuzer, *Eclipse Technologies for the Internet of Things and the Smart Home* (May 12, 2013), *available at* 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." (though his tripartition of the IoT into M2M, cloudy things and Intranet

of the 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 a single Thing. The 'system' dimension can be hindered by the fact that, unlike the cloud,[69] currently,[70] 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,[71] 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 without any particular obstacle.

Thirdly, there is the technical complexity.[72] At a higher 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) mean. Education is needed to raise awareness and therefore trust in CoT. Technical complexity also means that computer scientists and engineers are still struggling with some technical aspects, for instance, those related to 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 the researcher have studied a domotics scenario through an empirical research on the 'legals'[73] of Nest Inc., a CoT company providing thermostats, smoke

---

of Things is disputable). *Cf. also* B. Di Martino et al., *Advances in Applications Portability and Services Interoperability among Multiple Clouds*, in IEEE Cloud Computing 22 (March/April 2015), who, among other things, suggest the use of some ready-to-go solutions for portability and interoperability (namely, Docker, ElasticBox and Cloudify).

[69] 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.

[70] 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.

[71] *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.

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

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

alarms and cams. The results of that research will be made use of.[74] This 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, thus, 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 are binding, generally lack both the encompassing and coherent structure of the holistic approach and the granularity and concrete articulation of the sectoral approach;[75] too many, too vague.

---

[74] Noto La Diega & Walden, *supra* note 30.

[75] *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 (April 10, 2014) (*see* opinions ECOSOC (September 14, 2014), CoR (December 4, 2014)); EDPS, opinion 1/2015 on Mobile Health (May 21, 2015); Comm. Staff WD on the existing EU legal framework applicable to lifestyle and wellbeing apps (April 10, 2014); Council EU, Conclusions on Safe and efficient healthcare through eHealth, (December 1, 2009); 29WP, Health data in apps and devices, Annex to the letter to the Commission on February 5, 2015; 29WP, Opinion 3/2012 on developments in biometric technologies (April 27, 2012); 29WP, Working document on biometrics (August 1, 2003); 29WP, Opinion 6/2000 on the Genome Issue (July 13, 2000); Commun. *e-Health Action Plan 2012-2020 - Innovative healthcare for the 21st century* (December 6, 2012) (*see* Comm. Staff WD (December 6, 2012), opinions EDPS (March 27, 2013), ECOSOC (May 22, 2013) and CoR (July 3, 2013)); Commun. on telemedicine for the benefit of patients, healthcare systems and society (November 4, 2008) (*see* opinion ECOSOC (July 15, 2009)); Commun. *e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area* (April 30, 2004) (*see* opinion CoR (November 17, 2004)); Commission White Paper *Together for Health: A Strategic Approach for the EU 2008-2013* (October 23, 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 (December 22, 2011); Commission Recommendation on cross-border interoperability of electronic health record systems (July 2, 2008); Council conclusions on a safe and efficient healthcare through e-Health (December 1, 2009); Council conclusions on early detection and treatment of communication disorders in children, including the use of e-Health tools and innovative solutions (December 2, 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* (May 4, 2012); eHealth Network, Guidelines on ePrescriptions dataset for electronic exchange (November 18, 2014); eHealth Network, Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange (November 19, 2013); European Commission Decision C (2015)6776, Horizon 2020 Work Programme 2016 – 2017. 8. Health, demographic change and well-being (October 13, 2015).

The last but not least important factor behind complexity pertains to the actors of the CoT: who are they and which kind of relationships binds them? There are 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. The domotics scenario illustrated above will be used to shed light on the CoT supply chain.

One of the main flaws of literature on the IoT and CoT is that one gets the impression that everything is about the Thing, forgetting that human beings are and must be at the centre of technologies aspiring to be sustainable and empowering. Therefore, it is advisable to 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-users. This is mainly due to two factors: first, multi-tenancy, which is an important characteristic of both cloud computing and IoT. In fact, with respect to the person[76] who 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 can as well be a tenant. The difference may have also practical consequences. In terms of UK contract law, the statute implies a term into the contract that the purchasers of a good (not the tenant) will "enjoy quiet possession",[77] which would potentially be breached if the Thing were disconnected or some of its functionalities were taken away.[78]

If the end-users generally have no substantive power in the supply chain, the situation changes when it comes to the manufacturer of the Things;

---

[76] A separate issue is that of the use of Things to contract. On Things that sell Things and Things that sell themselves, *see* Hon et al., *supra* note 29, at 12-13. An aspect which seems to preoccupy lawyers when it comes to artificial intelligence is their substitution with machines (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 the arrest of robots would be probably seen as insane, 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).

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

[78] *See Rubicon Computer Systems Ltd.* v. *United Paints Ltd.*, (2000) 2 TCLR 453; Noto La Diega & Walden, *supra* note 30, at 6, call 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 everything is connected and private Things produce data flows and actions that necessarily interfere with public Things' flows and actions. In such a scenario, can the citizens claim a right to be disconnected, notwithstanding the scale effect of decisions of the kind?.

better said, again, the manufacturers. 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 start-ups 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 for small businesses. At any rate, one can see how IT transnational corporations are dominating the CoT. This has at least two effects on the relevant 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 has then become part of the multinational conglomerate Alphabet Inc., which also controls Calico, Google Capital, Google Fiber, Google Life Sciences, Google Ventures, and 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 one finds 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.[79] 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 service 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[80] and with energy providers as to Rush Hour Rewards and Seasonal Savings.[81]

---

[79] In Noto La Diega & Walden, *supra* note 30, at 11, we claim that the Thing is an inseparable mixture of hardware, software and service.

[80] 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.

[81] 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", *available at* https://nest.com/support/article/What-is-Auto-Tune). The liability issues arising out of AI and machine learning are out of the scope of this research.

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 operators.

–

The CoT, however, is not only about a single Thing. It is about the system, the network of Things, and the communications 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 healthcare. In fact, to the number obtained by the above descripted operations, one has to add doctors (not just physicians, surgeons, 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 Exchanges (HIEs), Regional Health Information Organizations (RHIOs), other care delivery organizations, and providers of medical devices, drugs, etc. Even this extensive list probably excludes 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. This discussion will now move on to Indian and British cases.

VI. Net neutrality and Facebook's 'Free Basics' app in India

India has recently surprised the West by shutting the door in Mark Zuckerberg's face. The CEO of Facebook had offered a Free Basics internet service app; it would have enabled free access to a limited number of websites, thus giving rise to a two-tier Internet, according to one's capacity of

paying for the services. 'Free Basics' is the main output of 'Internet.org', a partnership between the social networking platform and Samsung, Ericsson, MediaTek, Opera Software, Nokia and Qualcomm. There is legitimate suspicion about the reasons that caused these Western giants in the direction towards bringing access to selected Internet services to less developed countries. A conflict of interest being apparent, one fears that the digital divide will not be solved by offering connectivity in a discriminatory way, therefore one should welcome the ruling of the Telecom Regulatory Authority of India ('TRAI'),[82] which reaffirms the principle of net neutrality.

Net neutrality is a hot topic. It is the principle whereby, moving from the assumption that everybody has a fundamental right to access the Internet, this access and the relevant use must be granted in a non-discriminatory way.

The United States has led the way by introducing the *Open Internet rules* in February 2015,[83] followed, nine months later, by the European Union's regulation.[84] Both provide no blocking and no throttling rules. Under the first rule, broadband providers may not block access to legal content, applications, services, or non-harmful devices. Under the second one, broadband providers may not impair or degrade lawful Internet traffic based on content, applications, services, or non-harmful devices. However, the American rules are the only ones providing for the 'no paid prioritization'-that broadband providers shall not favour some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind. This rule prevents Internet Service Providers ('ISPs') from prioritizing the content and services of their affiliates. On the contrary, the European regulation allows 'zero rating', a commercial practice of some ISPs not to measure the data volume of particular applications or services when calculating their customers' data usage. Thus, those applications and services have an advantage when dealing with users with strict data caps, that is to say, with most users of Things, characterised by restrained connectivity, storage, and computing capabilities.

---

[82] TRAI, regulations n. 2/2016 of February 8, 2016, *Prohibition of discriminatory tariffs for data services regulations* (2016) *available at* http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf.

[83] Federal Communications Commission ('FCC'), Open Internet rules of February 26, 2015.

[84] In Europe, the first net neutrality rules have been introduced by the Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November, 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. Most of this regulation has become effective on November 29, 2015, and the rest of it will be in effect from April 30, 2016.

India, with the regulations analysed herein, is positioning itself along the same lines as the FCC. They build on the results of the Consultation Paper (CP) on Differential Pricing for Data Services,[85] and the Open House Discussion of January 21, 2016.[86] As one learns from the annexed Explanatory Memorandum, while the tariff regime has generally been left to forbearance, regulatory oversight is required so that the tariff framework follows the broad regulatory principles of non-discrimination, transparency, non-predationary practices, unambiguity, competitiveness and being non-misleading in nature. The terms of the licences for providing telecommunication services also require access to be provided to subscribers to all lawful content available on the internet without restriction.

The TRAI has taken into consideration two options, that is, imposing an *ex ante* bar on differential tariffs or barring such tariffs on a case-by-case basis. Following the indications of American scholars,[87] they choose the *ex ante* approach for reasons of certainty, high costs of individual investigations and justice towards the weak actors of the IoT chain (end users, low-cost innovators, start-ups, non-profit organisations, etc.).

As to the content, under the 'Prohibition of discriminatory tariffs for data services regulations', "*[n]o service provider shall offer or charge discriminatory tariffs for data services on the basis of content*" (r.3(1)) and "*[n]o service provider shall enter into any arrangement, agreement or contract, by whatever name called, with any person, natural or legal, that has the effect of discriminatory tariffs for data services being offered or charged to the consumer on the basis of content*." (r.3(2)) There is only one exception, whereby a service provider may reduce tariff for accessing or providing emergency services, or at times of grave public emergency (r.4). In other terms, the prohibition of discriminatory tariff for data services appears necessary to ensure that service providers continue to fulfil their obligations in keeping the Internet open and non-discriminatory.

At any rate, there are no grounds for complacency, since the CEO of Facebook has promised that they will continue their "*efforts to eliminate*

---

[85] The consultation opened on December 9, 2015 and closed on January 7, 2016. The paper is available at https://mygov.in/sites/default/files/mygov_1449738907190667.pdf and the 1062 submissions can be found at https://mygov.in/group-issue/seeking-comments-trai%E2%80%99s-consultation-paper-differential-pricing-data-services/.

[86] *See* here https://blog.mygov.in/open-house-discussion-on-differential-prices-for-data-services/. Following the open discussion, further comments have been received.

[87] B. Van Schewick, *Network Neutrality and Quality of Service: What a Non Discrimination Rule Should Look Like*, Stanford Law Review (2015), *available at* http://www.stanfordlawreview.org/sites/default/files/67_Stan_L_Rev_1_van_Schewick.pdf.

barriers and give the unconnected an easier path to the internet and the opportunities it brings."[88]

VII. The bottom-up creation of a new concept of city

Even though poverty is still a plague, India is living a golden moment with regard to urban development. In June 2015, the Ministry of Urban Development published 'Smart cities: Statement and Guidelines' (hereinafter "the Guidelines") and observed that, given that urban areas are expected to house 40% of India's population and contribute 75% of India's GDP by 2030, the government has to invest in a comprehensive development of physical, institutional, social and economic infrastructure. This is seen as critical "*in improving the quality of life and attracting people and investments to the City, setting in motion a virtuous cycle of growth and development*." The mission is financed with INR 70.6 billion (more than €940 million) and will cover one hundred cities and last for five years (2015-16 to 2019-20). The states nominated the cities by July 2015 and in January 2016, twenty cities were named winners. A group of twenty-three cities entered a fast-track phase to upgrade their proposals and compete again for funding. The selected cities are setting up the Special Purpose Vehicle (SPV)[89] and starting implementation of their Smart City Plan (SCP), preparing Detailed Project Reports (DPRs), tenders, etc. The remaining cities will have the chance to compete in the next competition cycle.[90]

Now, as it has been correctly observed, "*[w]hile smart cities in the West rely on the mining and analysis of big data to create urban networks, Indian smart cities aim to provide basic urban services: water, sanitation, electricity, housing and so on*."[91] The strategy is centred on four pillars: city

---

[88] Zuckerberg's words have been reported by all the main newspapers; *see*, for instance, A. Soni, *India deals blow to Facebook in people-powered 'net neutrality' row*, The Guardian, February 8, 2016, *available at* http://www.theguardian.com/technology/2016/feb/08/india-facebook-free-basics-net-neutrality-row.

[89] The implementation of the Mission at the City level will be done by a Special Purpose Vehicle (SPV), a limited liability company created for the purpose. The SPV will plan, appraise, approve, release funds, implement, manage, operate, monitor and evaluate the Smart City development projects. Each Smart City will have a SPV which will be headed by a full-time CEO and have nominees of Central Government, State Government and urban local bodies (ULB) on its Board.

[90] For the timeline and other details, *see* http://www.smartcitieschallenge.in/ and http://smartcities.gov.in/.

[91] A. Datta, *Will India's experiment with smart cities tackle poverty – or make it worse?*, The Conversation January 27, 2016, *available at* http://theconversation.com/will-indias-experiment-with-smart-cities-tackle-poverty-or-make-it-worse-53678.

improvement (retrofitting), city renewal (redevelopment),[92] city extension (greenfield development), and a Pan-city initiative in which Smart Solutions are applied, covering larger parts of the city.

From an 'Internet of Citizens' perspective, it is important to point out that the deployment of the plan will be accompanied by consultations with residents, with an emphasis on their visions. One may rebut this by saying that the rate of illiteracy is still over 35% of the population (nearly 45% if we look at the female cluster),[93] but one should be confident that the growth in the education sector may help overcome this situation. Moreover, even though the cities will have a certain degree of discretion in the implementation of the plan, their strategies should mandatorily encompass affordable housing, eGovernance and citizen participation, sustainable environment, and the safety and security of citizens and education. For instance, eGovernance solutions will encompass public information and grievance redressal.[94]

The gradual approach is another commendable aspect. Thus, for instance, an area consisting of more than 500 acres will be identified by the city in consultation with citizens; only after the completion of the retrofitting, the strategy may be completed through the replication in another part of the city. Whereas the largest area is set to serve the planning within the existing built-up area (retrofitting), in a 50 acres area the replacement of the existing built-up environment will be carried out by enabling the co-creation of a new layout with enhanced infrastructure using mixed land use and increased density (redevelopment). It is noteworthy that the greenfield development, which will introduce most of the smart solutions in a previously vacant area (more than 250 acres), will include "*affordable housing, especially for the poor.*" Pan-city development envisages the application of selected 'smart' solutions to the existing city-wide infrastructure (e.g. traffic management systems, waste water recycling, and new generation metering).

As a policy recommendation, the government should do everything in its power to ensure inclusiveness in the new city model and citizens should stay vigilant. Therefore, it is commendable that, even though it is not compulsory for the shortlisted cities to realize all the first three pillars, the fourth (the city-wide one) is mandatory, on the assumption that "*it is necessary that*

---

[92] Two examples of the redevelopment model are the Saifee Burhani Upliftment Project in Mumbai (also called the Bhendi Bazaar Project) and the redevelopment of East Kidwai Nagar in New Delhi being undertaken by the National Building Construction Corporation.

[93] The main data of the Indian Census of 2011 is publicly available at http://www.censusindia.gov.in/2011-prov-results/indiaatglance.html.

[94] *See also* http://www.smartcitieschallenge.in/recentnews/cities-for-citizens-incorporating-citizen-feedback-in-smart-cities.

all the city residents feel there is something in it for them also." (emphasis supplied)

A problem of top-down regulation is the one-size-fits-all approach. This is acceptable and even sensible for the discipline of non-contextual events such as homicide. If I commit homicide, I am a killer, no matter where I live, what my personal conditions are, what my gender is, etc.[95] On the contrary, the discipline of technology is ontologically contextual, which is a strong argument for a bottom-up approach. Again, one should praise the Indian government, because they are "*not prescribing any particular model to be adopted by the Smart Cities*", on the contrary, "*each city has to formulate its own concept, vision, mission and plan (proposal) for a Smart City that is appropriate to its local context, resources and levels of ambition*."

If a critique to the Guidelines had to be moved, it is that the shortlisted cities are required to draft their plans with external agencies. The main Western (US, UK, France, Germany) and Eastern (Japan) powers have offered to play this role. However, it is submitted that India could have found (and will find, for the cities that have not completed the process) the resources within its territory, in order to avoid any kind of possible cultural colonisation. At the end, Athens was a democracy because they did not imitate the laws of neighbouring states.

VIII. Zero defect, zero effect. Manufacturing between green washing and innovation

In 2015, the Department of Electronics and Information Technology ('DeitY', Ministry of Communciations and Information Technology) drafted an IoT Policy[96] which has four main goals: firstly, to create an IoT industry in India of USD 15 billion by 2020 (with a share of 5-6% of the global IoT industry); secondly, to undertake capacity development for IoT specific skill-sets for domestic and international markets; thirdly, to undertake R&D for all the assisting technologies; and lastly, to develop Things specific to Indian needs in all possible domains. Even though the final version is not available yet, it is worthwhile to briefly analyse this ambitious and pioneering document.

---

[95] Obviously, some contextual elements may matter (for instance, in the case of self-defence).

[96] The original draft is from October 17, 2014 and can be found at http://deity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf. The revised draft is available at https://mygov.in/sites/default/files/master_image/Revised-Draft-IoT-Policy-2.pdf. The latter was delivered on April 8, 2015, but the final version has not been published yet.

As to the implementation, it should follow a multi-pillar approach. There are five vertical pillars (Demonstration Centres, Capacity Building & Incubation, R&D and Innovation, Incentives and Engagements, and Human Resource Development) and two horizontal supports (Standards & Governance structure).[97]

This policy builds on the 'Digital India Programme'[98] whose objectives are Broadband Highways, Universal Access to Mobile Connectivity, Public Internet Access Programme, eGovernance, electronic delivery of services, Information for All, Electronics Manufacturing, IT for Jobs, and Early Harvest Programmes. It is noteworthy that the Digital India Program aims at "*transforming India into digital empowered society and knowledge economy*", thus providing the necessary input for the development of the IoT industry ecosystem in the country.

Another interesting, related precedent, albeit limited to R&D, is the Indo-Dutch Joint Research Programme for ICT.[99] The Netherlands Organisation for Scientific Research and DeitY have identified the following research topics "*where major technology trends will start to scale and shape business models, innovation and affect everyday life: Big Data, Internet of Things, Serious Gaming.*"

The policy has been seen as the realisation of the 'Zero Defect, Zero Effect' slogan, which was coined by the Prime Minister of India, Narendra Modi.[100] As part of the Make in India[101] strategy, it denotes manufacturing mechanisms whereby the possibility of error and the environmental impact are, or should be, eliminated.[102] Malevolent commentators may judge it as

---

[97] *See* http://deity.gov.in/content/internet-things.

[98] The Digital India Programme is available at http://deity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf.

[99] The budget of the programme was EUR 2 million; the deadline was October 14, 2014 and the call is temporarily closed. *See* more at http://www.nwo.nl/en/funding/our-funding-instruments/ew/indo-dutch-joint-research-programme-for-ict/indo-dutch-joint-research-programme-for-ict.html and http://deity.gov.in/sites/upload_files/dit/files/guidelines_final_vers3%20(1).pdf.

[100] *See* V. Mohan, *Ecologists cheer Modi's 'zero defect, zero effect' slogan*, The Times of India, August 16, 2014, *available at* http://timesofindia.indiatimes.com/home/environment/developmental-issues/Ecologists-cheer-Modis-zero-defect-zero-effect-slogan/articleshow/40312809.cms.

[101] 'Make in India' is a programme launched by Prime Minister Modi in September 2014 and is aimed to transform India into a global design and manufacturing hub. Alongside the technological aspects, it constitutes the realisation of the neoliberal motto 'Minimum Government, Maximum Governance'. *See* more at http://www.makeinindia.com/.

[102] 'Zero Defect, Zero Effect' is the highlight of the IoT policy according to V. Aggarwal, *India's first Internet of Things policy to focus on Zero Defect, Zero Effect*, The Economic Times India, April 10, 2015, *available at* http://articles.economictimes.indiatimes.com/2015-04-10/news/61017670_1_iot-m-sips-draft-policy.

a 'green washing' policy in order to convince transnational corporations to manufacture their products in India and to increase exportations. In fact, in his Independence Day speech, Modi had said that the 'Zero Defect, Zero Effect' policy was critical so that "*our [India's] exported goods are never returned to us*."[103]

Nonetheless, it is true that 'green manufacturing' is an important element of the IoT policy, even though there is no mention of the said slogan. Indeed, the first pillar 'Demonstration of domain specific applications' has a very 'green' attitude (one will have to monitor, however, the implementation process). The strategies of this pillar are mainly focused on smart water, smart environment, smart waste management, smart supply chain and logistics, and smart manufacturing/industrial IoT. For instance, the government wants to set up projects for alarm and control of CO_2 emissions of factories and pollution caused due to toxic gases emitted by cars. When dealing with 'green manufacturing', one must also mention the strategies to i. setup a project for enabling universal "ambulance service" at any place using Things; ii. enable a logistics chain managed by the government for essential food items to ensure need-based re-filling and reduction in the wastage of food; and iii. set up projects- here the proper *ex ante* 'zero defect' tool – using IoT for planning "*preventive and in-time maintenance for equipment in various manufacturing verticals*"; iv. set up projects for process-improvement in manufacturing, leading to optimal utilization of resources; and v. set up projects for monitoring operations and creating warnings/alerts for deviation/damages (here the *ex post* 'zero defect tool').

We do not know if and when this policy is to become effective; however, the Government has launched new initiatives aimed at implementing the 'Zero Defect, Zero Effect' principle. Namely, they are the 'ZED'[104] and 'Startup India'[105] programmes, with the former targeting micro, small and medium enterprises (MSMEs) and the latter, startups.[106]

---

[103] The full text of Modi's speech for the 68th Independence Day is available at http://indianexpress.com/article/india/india-others/full-text-prime-minister-narendra-modis-speech-on-68th-independence-day/. *Cf.* V. Venugopal, *Manufacturing to move into 'zero defect, zero effect' category*, The Economic Times India, January 21, 2016, *available at* http://articles.economictimes.indiatimes.com/2016-01-21/news/69960938_1_qci-msme-secretary-quality-council.

[104] The programme, foreseen in the 68th Independence Day speech and announced in January 2016, was set to be launched in March 2016. *See* more at http://zed.org.in/brief-history.php.

[105] The scheme has been launched on January 16, 2016. *See* more at http://startupindia.gov.in/actionplan.html.

[106] *See* more in Venugopal, *supra* note 103.

IX. The intellectual property of computer-related inventions: An IoT-friendly soft law

An impetus to the development of IoT and CoT in India may come from the new guidelines on computer-related inventions. A computer-related invention ('CRI' or computer-implemented invention, 'CII', in the European formulation) is one which involves the use of a computer, computer network or other programmable apparatus, where one or more features are realised wholly or partly by means of a computer program.

The protection of computer programmes has always been a much debated topic. Whether to protect them, how to protect them: copyright, patents, both? The European Patent Convention (EPC or Munich Convention) has opted for a ban on patentability of computer programmes claimed "as such" (arts. 52(2)(c) and (3) EPC).[107] Patents are not granted merely for program listings. Program listings as such are protected by copyright. For a patent to be granted for a CII, a technical problem has to be solved in a novel and non-obvious manner.[108] A particularly tricky category is 'computer program/computer program product'. The European Patent Office ('EPO'), stresses the (unclear) difference between the said category and computer programs as a list of instructions: the subject matter is patentable "*if the computer program resulting from implementation of the corresponding method is capable of bringing about, when running on a computer or loaded into a computer, a 'further technical effect' going beyond the 'normal' physical interactions between the computer program and the computer hardware on which it is run*."[109]

---

[107] In an attempt to address whether case-law concerning excluded matter is settled, and derive uniformity of application of European patent law, the President of the EPO referred four questions on the patentability of computer programs to the Enlarged Board of Appeal in October 2008 (G3/08, opinion on May 12, 2010, *available at* http://www.epo.org/law-practice/case-law-appeals/pdf/g080003ex1.pdf). However, the Board concluded that the referral was inadmissible because the decisions referred to were not considered to be "divergent", and declined to answer the questions beyond determining their admissibility. This led to the Court of Appeal reaffirming its view that practice was not yet settled in *HTC Europe Co. Ltd.* v. *Apple Inc.*, 2013 EWCA Civ 451 at 44.

[108] The CIIs do not receive a stricter assessment in comparison to other inventions. Indeed, in EPO Board of Appeal, T 1606/06 (DNS determination of telephone number/HEWLETT-PACKARD) of July 17, 2007, EP:BA:2007:T160606.20070717, the appellant argued that, since the patent concerned a CII, the triviality test should have been stricter. According to the Board, there is no basis for doing so and "[t]he only 'special' treatment for computer-implemented inventions relates to aspects or features of a non-technical nature; in fact, this treatment is only special in the sense that the presence of non-technical features is a problem which does not arise in many fields".

[109] European Patent Office (EPO), *Patents for software? European law and practice* (2013), *available at* http://documents.epo.org/projects/babylon/eponet.nsf/0/a0be115260b5ff-71c125746d004c51a5/$FILE/patents_for_software_en.pdf. For a landmark case of the

Mischievous commentators may argue that the CIIs are a surreptitious way to obtain a double binary for software protection. This may become true with IoT. Indeed, with the gradual substitution of old products with Things, we will face an unprecedented growth of CIIs. Therefore, asserting that computer programmes are not patentable in Europe may sound hypocritical. In other terms, the researcher foresees that most computer programs will be implemented in Things, with the consequential patentability of most computer programmes under the label of CII.

The impact of the IoT on patents can be observed also from another point of view. The researcher believes that the IoT provokes a redefinition of the concepts of novelty and originality for purposes of assessing patentability, essentially because of two characteristics: (a) network structure: patentability may derive from the way Things interact; (b) composite nature of Things: novelty might stem from the way the components of a single Thing interact. These profiles shall be the subject of further research.

India, unlike the US, follows the double-binary European approach. Indeed, s. 3(k) of the Patents Act[110] states that a '"computer program *per se*' is not patentable, but until recently, it was not clear whether CRIs were excluded from the subject matter or not. The silence kept on CRIs will not surprise those who know that the Patents Act, notwithstanding its amendments, remains an old act, as shown *inter alia* by the several provisions on floppy disks.

The Controller General of Patents, Designs and Trade marks (hereinafter the 'Controller', the Indian homologue of the Intellectual Property Office)

Board of Appeal, *see* T 1227/05 (Circuit simulation I/Infineon Technologies) of December 13, 2006, EP:BA:2006:T122705.20061213, *available at* https://www.epo.org/law-practice/case-law-appeals/pdf/t051227ep1.pdf, whereby "technical and inventive Specific technical applications of computer-implemented simulation methods, even if involving mathematical formulae, are to be regarded as "inventions" in the sense of Article 52(1) EPC. Circuit simulations possess the required technical character because they form an essential part of the circuit fabrication process." The most recent EPO case regarding computer programmes is T 1722/11 of December 18, 2015 on an Apple Inc. application for a "Method and system for message delivery management in broadcast networks." It is available at https://www.epo.org/law-practice/case-law-appeals/pdf/t111722eu1.pdf. As Fox LJ stated in Merrill Lynch's Application, 1989 RPC 561, 569, "it cannot be permissible to patent an item excluded by section 1(2) [of the Copyright, Designs, and Patents Act (1988)] under the guise of an article which contains that item - that is to say, in the case of a computer program, the patenting of a conventional computer containing that program. Something further is necessary."

[110] The Patents Act (1970), as amended on March 11, 2015, *available at* http://www.ipindia.nic.in/IPActs_Rules/updated_Version/sections-index.html.

has issued its guidelines on the examination of CRIs,[111] which comprise "*inventions which involve the use of computers, computer networks or other programmable apparatus and include such inventions having one or more features of which are realized wholly or partially by means of a computer programme or programmes*." Incidentally, one may note that 'other programmable apparatus' is a flexible concept capable of encompassing Things. The pendant of this notion is the 'computer system', which, under the Information Technology Act, 2000 is "a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions"; a very 'Thingy' dictionary.[112]

In August 2015, the Controller issued the first CRI guidance; it allowed the patenting of programmes which demonstrated technical advancement. Unsurprisingly, the guidance gave rise to protests from civil society. Many organisations and citizens complained about the contrast with s. 3(k) of the Patents Act and because software patentability was seen as a break to innovation.[113] To be precise, the guidance reaffirmed that computer programs *per se* were excluded from patentability and, therefore, "*[c]laims which are directed towards computer programs per se are excluded from patentability*"; consequently, the citizens' claims that computer programmes were excluded 'unconditionally' and that the one at issue was a 'blanket exclusion' were not entirely correct. Moreover, for being considered patentable, the subject matter should involve either "- *a novel hardware, or - a novel hardware with a novel computer programme, or - a novel computer pro-*

---

[111] Office of the Controller General of Patents, Designs and Trade marks, *Guidelines for Examination of Computer Related Inventions (CRIs)*, February 19, 2016, *available at* http://www.ipindia.nic.in/iponew/GuidelinesExamination_CRI_19February2016.pdf.

The first version was issued on August 21, 2015 and is still available at http://www.ipindia.nic.in/iponew/CRI_Guidelines_21August2015.pdf.

[112] Even before that, the definition of 'computer' is sufficiently flexible to accommodate the IoT specific characteristics. The term 'computer' is defined in The Information Technology Act, 2000 as "any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network."

[113] *Concerns over the "Guidelines for Examination of Computer Related Inventions (CRIs)" issued on August 21, 2015* (September 15, 2015), *available at* http://sflc.in/wp-content/uploads/2015/09/Letter_CRIGuidelines2015-Prime-Minister.pdf. I will not analyse the latter claim, also because it appears rhetoric and unsubstantiated and will open a Pandora's box of potential harm to the Indian industry. Such a step will invariably stifle innovation.

gramme with a known hardware which goes beyond the normal interaction with such hardware and affects a change in the functionality and/or performance of the existing hardware." The 'physical' element looked critical, but the third category presented some ambiguity. In addition, the attached clarification was not helpful (also, it was not clear if it was a clarification or a fourth category): a computer programme, "*when running on or loaded into a computer, going beyond the 'normal' physical interactions between the software and the hardware on which it is run, and is capable of bringing further technical effect may not be considered as exclusion under these provisions*."[114] (emphasis supplied)

The path towards the introduction of software patents had been gradual and Brownian. In 2002, the Patents (Amendment) Act introduced the words '*per se*' in s. 3(k) of the Patents Act. This was explained by the Joint Parliamentary Committee by saying that "*sometimes the computer programme may include certain other things, ancillary thereto or developed thereon. The intention here is not to reject them for grant of patent if they are inventions. However, the computer programmes as such are not intended to be granted patent.*"[115] The first guidance explained 'ancillary' by referring to "*things which are essential to give effect to the computer program*."

The second step was tried in 2004.[116] At that time, an amendment to provide for the patentability of computer programmes insofar as they enhanced technology was rejected by the Lok Sabha and the Rajya Sabha (the houses of the Parliament of India), "*as they feared that this would be beneficial only to multinational companies*."[117]

A similar failed attempt was made by the Patents (Amendment) Bill, 2005 that sought to extend patentability to computer programmes with "*technical*

---

[114] Para. 5.1, italics mine. The letter from civil society complained that the patentability of software was maintained dependent on the industrial applicability. This is not precise. Whereas the cited patentability as a result of technical effect could be tricky, the guidance limited itself to state that "[t]he examination procedure of patent applications relating to CRIs is the same as that for other inventions to the extent of consideration of novelty, inventive step, industrial applicability, sufficiency of disclosure and other requirements under the Patents Act and the rules made thereunder."

[115] *See Comments and recommendations on the Guidelines for Examination of Computer-Related Inventions (CRIs)* (2015), *available at* http://www.knowledgecommons.in/wp-content/uploads/2015/11/Comments-Recommendations-on-CRI-Guidelines-2015.pdf.

[116] Patents (Amendment) Ordinance (2004).

[117] S. Chathurvedula, *Revised guidelines for software patents put on hold*, Live Mint December 16, 2015, *available at* http://www.livemint.com/Industry/XGBbgNllmvuEUhJWs2cWgK/Revised-guidelines-for-software-patents-put-on-hold.html.

application to industry". The 'transnational corporations' exception was successfully raised again.

In 2011, the Controller clarified that "*claims directed at 'computer programme products' are computer programmes per se stored in a computer readable medium and as such are not allowable*."[118] Moreover, when a claim contains, *inter alia,* subject matter which is not limited to a computer programme, "*it is examined whether such subject matter is sufficiently disclosed in the specification and forms an essential part of the invention*."

It is notable that the draft CRI guidelines published in 2013[119] were clear as to the exclusion of any computer programme that may work on any general-purpose computer or 'related device' (that is to say, Thing) and that it did not meet the requirements of law.

After the said protests, with order n. 70 of 2015,[120] the Controller announced that the criticised guidance was to be "*kept in abeyance till discussions with stakeholders are completed and contentious issues are resolved*." The discussions have been completed and the contentious issues resolved on February 19, 2016, when the Controller published the new guidance.[121]

The guidance reaffirms the exclusion of software patents and introduces a three-step test to determine the applicability of s. 3(k) of the Patents Act to CRIs:

> "*Examiners may rely on the following three stage test in examining CRI applications: (1) properly construe the claim and identify the actual contribution; (2) if the contribution lies only in mathematical method, business method or algorithm, deny the claim; (3) if the contribution lies in the field of computer programme, check whether it is claimed in conjunction with a novel hardware and proceed to other steps to determine patentability with respect to the invention*."

---

[118] Office of Controller General of Patents, Designs & Trademarks, *Manual of Patent Office Practice and Procedure,* v. 1(11) (March 22, 2011), 08.03.05.10, *available at* http://ipindia.gov.in/ipr/patent/manual/HTML%20AND%20PDF/Manual%20of%20Patent%20Office%20Practice%20and%20Procedure%20-%20pdf/Manual%20of%20Patent%20Office%20Practice%20and%20Procedure.pdf.

[119] On June 28, 2013, the Controller published the draft guidance, *available at* http://ipindia.nic.in/iponew/draft_Guidelines_CRIs_28June2013.pdf.

[120] Office of Controller General of Patents, Designs & Trademarks, order n. 70 of 2015 (December 14, 2015), *available at* http://ipindia.nic.in/officeCircular/officeOrder_14December2015.pdf.

[121] Alongside the above-cited text, *see* Office of Controller General of Patents, Designs & Trademarks, order n. 11 of 2016 (February 19, 2016), *available at* http://www.ipindia.nic.in/iponew/OfficeOrder_CRI_19February2016.pdf.

Moreover, even though the phases of the examination procedure of CRIs are the same as other inventions as to the requirements of novelty, inventiveness, industrial applicability and sufficiency of disclosure, "*[t]he determination that the subject matter relates to one of the excluded categories requires greater skill on the part of the examiner.*"[122] While explaining that these concepts apply equally to ordinary inventions and to CRIs, the Controller specifies that the "*determination of industrial applicability in case of CRIs is very crucial since applications relating to CRIs may contain only abstract theories, lacking in industrial application.*" Furthermore, it explains how the sufficiency of disclosure applies to CRIs. The said requirement means that the invention has to be described "fully and particularly"[123] and the specification has to explain the best method of operation.[124]

Even though the use of the word 'may' might suggest a certain scope for the examiners' discretion and one would have expected that the excluded subject matter should have to be interpreted in a stricter way (as opposed to requiring "greater skill"), the wording is adamant in binding CRI patentability to inventions which constitute an inextricable mixture of software and hardware, i.e., to Things. From this point of view, the new CRI guidance may be a formidable input to the developments of IoT inventions, now supported by legal clarity and certainty.

---

[122] *See* more at http://cis-india.org/.

[123] It can be useful to report the wording of this subparagraph: "1. If the patent application relates to apparatus/system/device i.e. hardware based inventions, each and every feature of the invention shall be described with suitable illustrative drawings. If these system/device/apparatus claims are worded in such a way that they merely and only comprise of a memory which stores instructions to execute the previously claimed method and a processor to execute these instructions, then this set of claims claiming a system/device/apparatus may be deemed as conventional and may not fulfil the eligibility criteria of patentability. If, however, the invention relates to 'method', the necessary sequence of steps should clearly be described so as to distinguish the invention from the prior art with the help of the flowcharts and other information required to perform the invention together with their modes/means of implementation. 2. The working relationship of different components together with connectivity shall be described. 3. The desired result/output or the outcome of the invention as envisaged in the specification and of any intermediate applicable components/steps shall be clearly described." (para. 4.4.1).

[124] Under para. 4.4.2 of the new guidance, "*[t]he best mode of operation and/or use of the invention shall be described with suitable illustrations. The specification should not limit the description of the invention only to its functionality rather it should specifically and clearly describe the implementation of the invention.*"

X. Surveillance in disguise and the world largest biometric database. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016

The Indian Parliament has recently passed a bill on surveillance on the world's largest biometric database and I believe that this is relevant for a study on the IoT. Firstly, I have clarified how surveillance is critical in an IoT environment; secondly, biometric data is becoming more and more important in multi-factor authentication, which is a fundamental brick in the erection of the IoT.[125]

Even though biometric authentication can prove to be very secure, it has its downside. Indeed-with Things everywhere and with many of them equipped with webcams and other sensors-LEAs, terrorist groups and everyone else may be able to copy, say, the face scan. Unlike the password-based system, the biometric one is rigid inasmuch as one can always modify their password, whilst one cannot change their face (unless one undertakes face surgery).

In 2010,[126] the Government of India (better said, the Unique Identification Authority of India or UIDAI) started collecting biometric data (mainly fingerprints and iris signatures) as a condition to issue the so-called Aadhaar number and card. Without the number, one cannot apply for subsidies. The UIDAI has already collected the biometric data of nearly a billion people.[127]

In March 2016, the Parliament of India passed The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill,

---

[125] The bifactorial authentication will be increasingly insufficient. For instance, a malware hitting Android phones can intercept incoming SMS text messages, thus allowing one 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* (December 1, 2015), *available at* http://www.abs.org.sg/pdfs/Newsroom/PressReleases/2015/MediaRelease_20151201.pdf. *Cf.* Kennedy et al., *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 (April 30, 2015), *available at* SSRN: http://ssrn.com/abstract=2600795.

[126] The National Identification Authority of India Bill, 2010 had been passed to provide legislative backing to the UIDAI, but it had been withdrawn when the here-analysed bill was introduced.

[127] The data can be found in S. Miglani & M. Kumar, *India's billion-member biometric database raises privacy fears*, March 16, 2016, *available at* http://www.reuters.com/article/us-india-biometrics-idUSKCN0WI14E. They report *inter alia* that the bill "has been showcased as a tool exclusively meant for disbursement of subsidies and we do not realize that it can also be used for mass surveillance," (Tathagata Satpathy, a lawmaker from the eastern state of Odisha).

2016,[128] which provides federal agencies with the right to access the said database in the interest of national security.

The fact that this unprecedented[129] collection of biometric (thus personal) data has been disguised under the appearance of a law on subsidies is susceptible to criticism. Now, the decision to qualify the bill as a 'money bill', thus depriving the Rajya Sabha (the upper House) of the power to reject it, seems rather unfair. On such topics, the larger and deeper the discussion and the more transparent the process, the better is the output.

This system has been defended in Parliament by the Government by leveraging the asserted financial savings (150 billion rupees or $2.2 billion would have been saved in 2014-2015). However, since the right to privacy is at issue,[130] the balance should not be in favour of merely economic interests. A closer look at the bill,[131] going beyond the exaggerations that abound in the press, is warranted.

The Statement of Objects and Reasons of the Bill states that the identification of targeted beneficiaries for delivery of various government subsidies and services has become a challenge for the government. The said delivery is dependent on the residents' consent to provide their biometric data. More precisely, everyone is requested to submit their (i) biometric data (photograph, finger print, iris scan) and (ii) demographic data (name, date of birth, address). Given that the said information is already substantially personal, one does not see why one should leave the UIDAI with the blanket power to specify other biometric and demographic information to be collected. The limits of this regulation should be subjected to democratic debate in Parliament.

---

[128] Introduced by the Minister of Finance, Mr. Arun Jaitley, in the Lok Sabha on March 3, 2016, the bill was passed on March 11, 2016 in the Lok Sabha and on March 16, 2016 in the Rajya Sabha. The President's assent is currently pending.

[129] If the collection is unprecedented, the passing of legislation on surveillance in India is not. *See*, for instance, the Indian Telegraph Act (1885), which allows national security agencies and tax authorities to eavesdrop on conversations of individuals for public safety reasons.

[130] On the right to privacy in India *see*, for instance, CRID University of Namur, *First Analysis of the Personal Data protection Law in India. Final Report*, *available at* http://ec.europa.eu/justice/data-protection/document/studies/files/final_report_india_en.pdf.

[131] The reference text (as passed) can be found at http://www.prsindia.org/uploads/media/AADHAAR/Aadhaar%20bill%20as%20passed%20by%20LS.pdf. The original bill is available at http://www.prsindia.org/administrator/uploads/media/AADHAAR/Aadhaar%20Bill,%202016.pdf; a summary at http://www.prsindia.org/uploads/media/AADHAAR/Bill%20Summary-%20Aadhaar%20Bill.pdf; the issues for consideration at http://www.prsindia.org/uploads/media/AADHAAR/Aadhaar%20Bill%20Issues%20for%20Consideration%20%2008.03.16.pdf; and the comparison between the 2010 bill and the 2016 one at http://www.prsindia.org/uploads/media/AADHAAR/Comparison%20of%202010%20and%202016%20Aadhaar%20Bills.pdf.

At the moment of enrolment, then, the individual will be informed *inter alia* of the manner in which the information will be used and of the nature of recipients with whom the information will be shared. It is not clear what 'manner' (why not 'purpose'?) means and why the bill does not restrict *ex ante* the nature of recipients. The two main points are restrictions on sharing information and the circumstances under which the personal data can be revealed.

As to the first point, the authority is provided by Clauses 29 (1), (4), and Clause 8 (4).

Biometric information such as an individual's fingerprints, iris scan and other biological attributes as specified by the UIDAI regulations will be used only for Aadhaar enrolment and authentication, and for no other purpose. There is a commitment not to share such information with anyone else. The biometric and demographic data will be stored in electronic form in accordance with the safeguards of the Information Technology Act, 2000.

When authenticating an individual's identity, the UIDAI cannot reveal information related to iris scan and fingerprints, to the entity requesting for authentication. The agency requesting authentication of an individual's identity may use the disclosed information only for purposes for which the individual has given consent.

Then, even though the Aadhaar number and information related to an Aadhaar number holder's fingerprints and iris scan shall not be published or displayed publicly, the UIDAI is free to introduce exceptions.

As to the circumstances under which an individual's information may be revealed, Clause 33 (1), (2) provides a clear exception when it comes to national security and judicial orders.

Indeed, in the interest of national security, an officer not below the rank of Joint Secretary to the Government, specially authorised by an order of the Government, may issue a direction for revealing (i) an individual's Aadhaar number, (ii) biometrics (iris scan, finger print and other biological attributes specified by regulations), (iii) demographic information and (iv) photograph. Such a decision will be valid for 6 months and has to be reviewed by an Oversight Committee before it takes effect.

Secondly, a court not inferior to the District Judge has the power to order the revelation of (i) an individual's Aadhaar number, (ii) photograph and (iii) demographic information. This provision goes with the proviso that no order by the court shall be made without giving an opportunity of hearing.

Now, one may say that most of the above provisions were already part of the 2010 Bill; many provisions introduce new guarantees for the citizens, such as the *ex ante* control of the Oversight Committee. However, a mischievous commentator may interpret them as a game of smoke and mirrors. What is more alarming is the unclear scope of the UIDAI's discretion in regulating the information to be collected and the exceptions to its sharing. Moreover, it is hard to understand why the judges' orders could regard photographs and demographic data, whereas the administration (*in primis* the LEAs), which usually acts secretly, has a blanket power to access also the biometric data.

As to the aftermath, the Supreme Court[132] is examining a petition claiming that Aadhaar is in violation of the right to privacy, therefore it would be worthwhile to keep track of the next developments.

XI. IoT deployment and Regulation in the United Kingdom

The 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[133] 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.[134] 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 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

---

[132] *K.S. Puttaswamy* v. *Union of India*, (2014) 6 SCC 433, (2015) 8 SCC 735, (2015) 10 SCC 92.

[133] Aegis Systems Ltd-Machina Research, *M2M application characteristics and their implications for spectrum. Final report*, 2606/OM2M/FR/V2 (May 13, 2014), *available at* http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/M2M_FinalReportApril2014.pdf. The report has been commissioned by Ofcom.

[134] *See* Department of Energy and Climate Change, *Smart meters: a guide* (January 22, 2013) (last updated October 8, 2013), *available 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* (January 22, 2013), *available at* https://www.gov.uk/guidance/smart-meters-information-for-industry-and-other-stakeholders.

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 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 substantial public investment. Indeed, on July 8, 2015, the UK 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.[135] Ultimately, there is 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 sector) has announced a £62.8 million investment to deliver a smarter energy network for consumers.[136]

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 informed the review *The Internet of Things: making the most of the Second Digital Revolution* (also known as the *Blackett Review*),[137] published on December 18, 2014. It covers five sectors (transport, energy, healthcare, agriculture, buildings) and has three main goals. The first is to explain what the 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, commissioning spectrum and networks, standards, skills and research, data, regulation and legislation, trust, and coordination.

---

[135] 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/.

[136] The announcement has been made on November 30, 2015 (*see* https://www.ofgem.gov.uk/publications-and-updates/ofgem-announces-62-8-million-deliver-smarter-energy-network-consumers).

[137] GCSA, *supra* note 42.

In the meantime, on July 23, 2014, the Office of Communications (Ofcom, the UK communications regulator) published a call for inputs on "*Promoting investment and innovation in the Internet of Things*", aimed to identify potential barriers to investment and innovation in the IoT (and on the role of the regulator).[138] The "*Summary of responses and next steps*"[139] has been delivered on January 27, 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 give merely a short account of the other aspects.

Understandably enough, network addressing is not of great importance, as telephone numbers are "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*";[140] closed on November 12, 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 properties different from 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 unsurprising that network security and resilience have become critical. Ofcom reports a growing demand in terms of both 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,[141] the European Commission is about to initiate the establishment of a Public-Private Partnership on cyber security in the area of technology

---

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

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

[140] 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.

[141] European Commission communication *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, issued on May 6, 2015.

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 on 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 the ICO on RFID[142] and the Smart Energy Code[143]- 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, it will be taken into account in the following analysis.

XII. Data protection and privacy:The repurposing issue

When it comes to the CoT, there is an undisputable interest in the data protection and privacy aspects (surprisingly, not so much for the security ones). This is due mainly to four factors. I have partly referred to them in the introduction, since some of them constitute the main reasons why people should be concerned about the IoT as a whole. Here I am looking at them from a data protection point of view.

Firstly, the data processed is potentially almost always personal data because the Things are in/on the human body and abound in private spaces (e.g. domotics), thus being capable of gathering information hitherto unavailable to the public (and to 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. cross-device identification and the adoption of IPv6) exist.[144] Lastly, surveillance has

[142] ICO, *Data Protection Technical Guidance Radio Frequency Identification* (August 9, 2006), *available at* https://ico.org.uk/media/for-organisations/documents/1590/radio_frequency_indentification_tech_guidance.pdf.

[143] The Smart Energy Code (SEC) came into force on September 23, 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 an ongoing consultation 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.

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

increasingly become a problem. As an example, in addition to the previously named ones, one may think to the proposal for a EU directive on the use of Passenger Name Record (PNR).[145] The increase of surveillance is assertedly connected to counter-terrorism. In fact, between 2001 and 2013, 239 specific EU laws and policy documents have been adopted in the name of counter-terrorism. Of those, 88 are legally binding.[146]

Europe is aware of these problems. For instance, on December 15, 2015, the European Parliament, the Council and the Commission reached an agreement on the draft General Data Protection Regulation (GDPR). Under recital 24,

> "*Individuals 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 individuals and identify them*".

---

[145] 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 December 2, 2015, a provisional agreement had been met; the vote of the European Parliament is (was) set for early 2016. 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 to 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*, EuObserver, December 9, 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* (September 24, 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). According to the last document available in the register of the Council, the Member States have officially declared that they will make full use of the possibility offered by Article 1a of the PNR Directive, which allows them to apply it to intra-EU flights, upon notice to the Commission to that end (Note no. 15271/15 from the General Secretariat of the Council to the Delegations (December 15, 2015), *available at* http://data.consilium.europa.eu/doc/document/ST-15271-2015-INIT/en/pdf). The document 'Passenger Name Record Data Exchange Pilot (PNRDEP) for Passenger Information Units- Proposal for the 5th IMS action list' of March 10, 2016, is not publicly available.

[146] B. Hayes & C. Jones, *Report on how the EU assesses the impact, legitimacy and effectiveness of its counterterrorism laws*, Statewatch SECILE report 28 (December 2013), *available at* http://www.statewatch.org/news/2013/dec/secile-how-does-the-EU-assess-its-counter-terrorism-law.pdf; they 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 is encrypted both in transmission and storage. In fact, one may think that given the power constraints of Things, encryption should be avoided since it is energy consuming. On the contrary, researchers have shown, for instance, that the Advanced Encryption Standard (AES) Algorithm, instead of consuming power, can save it.[147]

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.[148] 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, is 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 to easily and transparently 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[149] has in fact shown that apps can seek 235 different kinds of permission from smartphone users. Consumers are concerned with these 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 be used.

Even though the ICO has not issued an ad-hoc guidance, its response to the Ofcom's consultation of October 1, 2014 contains many useful indications.

---

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

[148] *See supra* note 125.

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

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. It should be added that given that multi-tenancy is a characteristic of both the cloud and the IoT, one can not always know who is actually using the Thing. It is nonetheless true that inferential data grows in importance and as a consequence, 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 and whoever 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 the 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 the researcher has referred to above as repurposing; therefore, a TV can be designed not to process personal data, but it can end up processing very personal (even sensitive, e.g. health-related) data.

Anyway, in the event the DPA does not apply, the 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.[150]

An aspect which the ICO commendably stresses on is that Things may not have a physical interface at all with which an individual can interact. Consequently, acquiring valid informed consent can be difficult. Though this is true, sometimes technology solves the problems it creates. One example is provided by holographic computers: a hologram could easily substitute a traditional interface.[151]

---

[150] The draft of this industry code has been presented by the editor Hans Graux of time.lex on December 7, 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.

[151] *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) 162-166 IEEE (Thiruvananthapuram, December 13-15, 2013). Thanks to the new definition of trade marks provided by the

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, 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 the case, due to the herein analysed repurposing. Thirdly, deep learning and AI technologies are being widely adopted, with the consequence, as to the point at issue, that the Things can reprogram themselves, thus expelling the privacy settings.

If, on the one hand, the users risk not being 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 the actual responsible actor.

Owners of old models of smartphones and tablets would be well aware of another problem. Software lifecycles are by far shorter than hardware ones and software projects soon become unsupported. If security updates are no longer provided, there is an increasing security risk, let alone the fact that old Things stop functioning because of this discrepancy. One solution

---

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.

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 recall 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 fight between Apple and the FBI, where the company refused the request of the federal agency to unlock 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."[152]

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 issued a code of practice focused on the need to actively provide privacy notices.[153] 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 takes 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 will all have to provide privacy notices. It is notable that there is a proposal to supplement the individual privacy 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.

---

[152] T. Cook, *A Message to Our Customers* (February 16, 2016), *available at* http://www.apple.com/customer-letter/.

[153] The code has been issued on February 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' closed on March 23, 2016. The text is available here https://ico.org.uk/media/about-the-ico/privacy-notices-transparency-and-control-0-0.pdf.

Privacy and data protection are also at the core of the mentioned *Blackett Review*. The GCSA is not particularly enlightening on the point, since it limits itself to underlining 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).[154] As a policy recommendation, one could not disagree with the invitation to keep legislation to the minimum required to facilitate uptake.

XIII. Consumer protection and property

In ordinary language, data protection and privacy can be viewed as a part of consumer 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 B2C relationships.[155]

The Consumer Rights Directive ('CRD')[156] looks rather influenced by CoT developments. Indeed, digital content supplied in a tangible medium (in other terms, in Things) is now defined as a 'good' (art. 2(3)). Moreover, 'digital content' means data which is 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 can still 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

---

[154] *See supra* note 66.

[155] 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).

[156] Directive 2011/83/EU of the European Parliament and of the Council of October 25, 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.

latter, in turn, is defined as "the standard hardware and software environment with which the digital content is compatible" (*ibid*). Even 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 (arts. 5(1)g) and 6(1)r)), given that not only do they exacerbate the imbalance of power in B2C relationships, but they risk to contribute to the fragmentation of the CoT, thus leading to the Internet of Silos.[157]

The main critique that the researcher feels obliged to move towards the CRD regards the fact that consumers do not enjoy the right of withdrawal with respect to to some contracts, as set out in arts. 9 to 15. 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)), and secondly, and maybe more importantly, the contract 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 would 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 the Consumer Rights Act, 2015, as amended ('CRA').[158] 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 in 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, most CoT contracts, although American in origin, tend to make safe consumer protection law; therefore, inconsistent contractual sections should be unenforceable.

---

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

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

The weakest link of the CRA illuminates a peculiar relationship between ownership and data protection. The CRA applies only to sales contracts, contracts for the hire of goods, hire-purchase agreements, and contracts for the 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 under the CRD.

XIV. Conclusion

This paper shows that the technological development epitomised by the IoT and CoT leads to rethink some traditional concepts in matters 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 prominent characteristics, 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 which 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 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).[159] A holistic assessment of the

[159] A pioneering thought on autonomous machines was made by N. Wiener, *The Machine Age*, vers. 3, 8 MIT (1949): "[*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*

impact of AI on the concept(s) of predictability (proper of many fields of law) would be an important contribution to the advancement of the relevant scholarship.

Future research shall focus on the application of the herein analysed principles to eHealth. CoT-health is an unexplored sector of eHealth and it promises to create a new era for healthcare which will be decentralised, patient-centric, and dynamic. The use of health big data and the flows generated by 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 the CoT an empowering, inclusive, and safe ecosystem through increasing awareness and trust in society. If it is true that "the most profound technologies are those that disappear",[160] we will have to be very alert.

Another thing lacking in the current literature is the imbalance between the focus on privacy and the studies on other legal issues. If AI is stimulating a new scientific stream as to the liability aspects, much is still to be said on the intellectual property aspects. Alongside the development of some things I have suggested here (such as the 'network structure'), it appears clear that the Standard Essential Patents (SEP) and the FRAND regime will play a critical role in the said context. Moreover, one ought to assess the potential impact of the European reforms of trademarks[161] and copyright[162] on the IoT and CoT.

---

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.

[160] 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.

[161] Directive (EU) 2015/2436 of the European Parliament and of the Council of December 16, 2015 to approximate the laws of the Member States relating to trade marks (in effect from January 15, 2016; it needs to be implemented by January 14, 2019) and Regulation (EU) 2015/2424 of the European Parliament and of the Council of December 16, 2015 amending Council Regulation (EC) No 207/2009 on the Community trade mark and Commission Regulation (EC) No 2868/95 implementing Council Regulation (EC) No 40/94 on the Community trade mark, and repealing Commission Regulation (EC) No 2869/95 on the fees payable to the Office for Harmonization in the Internal Market (effective from March 23, 2016).

[162] The reference is to the Digital Single Market Strategy (COM/2015/0192 final of May 6, 2015), which is carrying out a modernisation of the EU copyright framework. One of the main problems is geo-blocking, tackled by the proposal for a regulation on ensuring the cross-border portability of online content services in the internal market (COM(2015) 627 final of December 9, 2015). Other critical issues are dealt with by the draft directive on certain aspects concerning contracts for the supply of digital content (COM(2015) 634

Lastly, further investigations shall assess the application of the existing Indian legislation to the IoT and CoT scenario. The analysis shall move from the Information Technology Act, 2000, whose existence may surprise all the western scholars who have always ridiculed the possibility of an Internet Law or a Cyberlaw, frowned upon as the 'Law of the Horse.'[163]

Moreover, the Indian attitude towards privacy appears relatively relaxed;[164] therefore, an empirical survey on this aspect might be of interest, given that "India controls 44% of the global outsourcing market of software and back-office services"[165] and European and American businesses are major clients of the business process outsourcing industry. If an updated survey found that Indian citizens are still unaware of the role of privacy, this could be a further argument to criticise the Aadhaar bill.

Poverty is still a palpable reality in India, with an estimated 17.6% of the Indian population, or about 276 million people, living below $1.25 per

---

final of December 9, 2015). For the other measures, see the communication 'Towards a modern, more European copyright framework' (COM(2015) 626 final). *See also* Directive 2014/26/EU of the European Parliament and of the Council of February 26, 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market.

[163] In F.J. Easterbrook, *Cyberspace and the Law of the Horse*, U Chi Legal F 207 (1996) (*available at* https://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf), the judge spoke out against the construction of specialised fields of law (namely concerning the cyberspace), pointing out the risk of losing a systematic view. This is not entirely false, but one cannot deny that there are some aspects that cannot be accommodated by traditional principles and that IT law has a lot to teach also to other scientific fields (*see* L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, Harv. L. Rev. 501 (1999)). Moreover, whereas the Internet of Things is a part of everyday life (that is why it has been called by the term '*everyware*'), unfortunately only a minority has got horses: not everyone, for instance, know what the fetlock is, whilst there is nearly no one who does not *WhatsApp* pictures to share them with friends and family. Obviously enough, such a law should be an essential, open and agile tool, in order to avoid the risk of the Locomotive Act (1865) (so-called Red Flag Law), which required, among other things, a man carrying a red flag to walk in front of cars as a security measure against the revolution of cars.

[164] According to B. Crutchfield George & D. Roach Gaut, *Offshore Outsourcing to India by U.S. and E.U. Companies. Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing*, 6 U.C. Davis Bus. L.J. 13 (2006), the delay in enacting a data protection legislation is mainly due to four factors: 1) there are no major privacy breaches in Indian history; 2) there is not serious resentment in India toward the central government; 3) given the population density, privacy is not a great concern; and 4) hitherto, identity theft has not been a problem in India.

[165] J. Hils Shea, *Attitudes Toward Privacy: A Comparison of India and the United States* (February 2007), *available at* http://www.frostbrowntodd.com/resources-214.html. There already exist some notable studies, such as P. Kumaraguru & N. Sachdeva, *Privacy in India: Attitudes and Awareness* V 2.0 (November 22, 2012), *available at* http://precog.iiitd.edu.in/research/privacyindia/PI_2012_Complete_Report.pdf; however, given the rise of surveillance and the development of new technologies, an updated research would be needed.

day.[166] However, one should not think that investing in a new concept of city, in a non-discriminatory Internet and in a new way to manufacture goods is something unrelated to the fight against poverty. Not only because the new services and Things may create a considerable number of new jobs, but above all, because the Indian IoT seems to be built by the Indian citizens and for the Indian citizens. Nonetheless, it is important for everyone to stay vigilant, in order to prevent the IoT from becoming just a matter of smoke and mirrors.

The researcher believes in needs-based law and empowering technologies. Therefore, it is critical, in order to give rise to the Internet of Citizens, to ensure their constant, conscientious involvement. To this aim, collective awareness platforms should be launched, as well as informal consultations in the local communities, not to leave behind the illiterate citizens. Education is the key for the actual empowerment of citizens and law and new technologies should never be used to conceal the needs of the citizens, nor the needs be used to extort personal data, as a mischievous interpretation of the Aadhaar bill suggests.

In conclusion, the researcher believes that as more and more Things will be connected and produce valuable information, one will not have to fight for the right to access the Internet, but for the right to be disconnected. India, with its refusal of Facebook's offer, is leading the way, but the new surveillance bill may cast a shadow on its future.

---

[166] M. Ravallion (World Bank), *World Bank's $1.25/day poverty measure- countering the latest criticisms* (January 2010), *available at* http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTRESEARCH/0,contentMDK:22510787~pagePK:64165401~piPK:64165026~theSitePK:469382,00.html.