Internet of Things and Patents: Towards the IoT Patent Wars?

Dr Guido NOTO LA DIEGA*

Abstract

Intellectual property is a key, albeit overlooked, issue when it comes to the Internet of Things (IoT). It is still unclear, for instance, to what extent trade secrets can be used to prevent the user from controlling their own device (the so-called right to hack) and to hinder interoperability. Likewise, it is still to be fully explored to what extent intellectual property (database rights) can be used to prevent data portability. This paper focuses on patent law and, namely, on computer-implemented inventions by giving account of the approaches followed in Europe, United States, and India. With the IoT patenting activity being over eight times larger than the general worldwide increase in patenting, research on this field appears critical. The occasion of this study is the adoption in 2016 of the final version of the Indian guidelines on the examination of computer-related inventions, which have been surprisingly overlooked in the legal literature. The main idea is that the Internet of Things will lead to a dramatic increase of applications for software patents and if examiners, courts, and legislators will not be careful, there is the concrete risk of a surreptitious generalised grant of patents for computer programs as such (in Europe) and for abstract ideas (in the United States). The clarity provided by the Indian guidelines, following a lively public debate, can constitute good practices that Europe, the United States, as well as the Republic of Turkey, should take into account. With the increase of IoT patents, it is foreseeable the shift from the smartphone wars to the IoT wars, as evidenced by some recent litigation between Fitbit and Jawbone. The (perhaps cold) war seems impending, due to a number of reasons, such as the complexity of the supply chain, the several domains in which the IoT is divided and the composite nature of the IoT devices.

Keywords: Internet of Things, IoT, software patents, computer-implemented inventions, computer-related inventions, software inventions, patenting, patent law, computer programs, patentable subject matter, patentability, exclusion

* Lecturer in Law, Northumbria University; President, 'Ital-IoT' Centre of Multidisciplinary Research On the Internet of Things; Fellow, Nexa Centre for Internet and Society; Convenor, NINSO Northumbria Internet & Society Research Interest Group. The author is grateful to the Ankara Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi for the invitation to the III. International Symposium on Intellectual Property Law. He is thankful to Dr Cahit Suluk and Mr Canan Öztürker for insight in the Turkish patent system. The responsibility for opinions and mistakes, however, rests with the author. Please, e-mail comments to guido.notoladiega@northumbria.ac.uk or tweet them to @guidonld. This paper builds on an article published on the *European Intellectual Property Review*.

1. Introduction

The Internet of Things (IoT) entails any physical entity capable of connectivity that directly interfaces the physical world, such as embedded devices, sensors and actuators (Noto La Diega and Walden 2016). It will be the largest device market in the world by 2019 and will result in $1.7 trillion in value added to the global economy (Greenough 2014). Such an opportunity could not be overlooked by innovators, as shown by the almost 22.000 IoT patents and patent applications published between 2004 and 2013 (Intellectual Property Office 2014). Moreover, between 2010 and 2013 the annual increase in the IoT patenting activity has been over eight times larger than the general worldwide increase in patenting (ibid.).

Even though it is recognised that "[l]egal and regulatory concerns of intellectual property issues […] are emerging challenges" (Rose, Eldridge, and Chapin 2015, 39) for the IoT, little research explored them (Noto La Diega 2017; Trappey et al. 2016; Horbal 2015). This paper deals with patent law, given that, according to the European Patent Office (EPO), the IoT is likely to increase patent density in relation to "all industrial sectors" (CEN and CELENEC 2016, 12). Moreover, IoT patents are seen as the key enabler for the Industry 4.0 and software patents are the second most granted patents after patents on controllers (Trappey et al. 2016). Besides, it has been observed that the so-called IoT patent thicket "has grown immensely over the last 10 years" (Ho 2016b), because the relevant players are getting patents at every level of the IoT ecosystem. The focus will be on one of the most relevant IoT-related patent law topics, that is computer-implemented inventions (CII, or computer-related invention, CRI).

A CII 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. CIIs are a critical topic in patent law, since a too relaxed approach in awarding grants for this kind of inventions may risk to allow a double protection for computer programs: copyright and patents. Thus, a too much broad monopoly would be legitimised, with a subsequent increased propertisation of intangibles. A similar problem can occur in the United States, notwithstanding the patentability of computer programs *per se*. There the risk

is the widespread eligibility for protection of mere abstract ideas. This would only partly offset by the difficulty to enforce IoT patents, mainly related to the issues of divided infringement and territoriality (Ho and Huang 2016).

Many countries continue to clearly exclude software patents, and this is the case of the Republic of the Republic of the Philippines. However, the trend seems to go in the opposite direction of recognising patents on CIIs and sometimes on computer programs *per se*.

This article sheds light on a much pressing issue by giving account of the approaches followed in Europe, United States, and India. The main idea is that the IoT will lead to a dramatic increase of applications for software patents (and of the relevant litigation). If examiners, courts, and legislators will not be careful, there is the concrete risk of a surreptitious generalised grant of patents for computer programs as such (in Europe) and for abstract ideas (in the United States). The clarity provided by the Indian guidelines, following a lively public debate, can constitute a good practice that Europe, the United States, and the Republic of Turkey should take into account.

2. Computer-implemented inventions in the case law of the European Patent Office

The protection of computer programs has always been a much debated topic. Whether to protect them, how to protect them: copyright, patents, or both.

There are three models. The first model, exemplified by the US, offers a double protection to computer programs, with an overlap of patent rights and copyright. The second, most common, model is the hybrid one. As in all the countries party to the European Patent Convention (EPC) and the Berne Convention, computer programs are protected as literary works by copyright (with a number of exclusions e.g. functionality, programming language and file formats), while their patentability is excluded, but only 'as such'. An example of this is the Turkish system. Under *Madde* 6 of the *551 sayılı Patent Haklarının Korunması Hakkında Kanun Hükmünde Kararname* (art. 6 of the Decree-Law No. 551 of June 24, 1995 on the Protection of Patent Rights), computer programs fall outside the scope of patent law, being *Patent Verilemeyecek Konular* (non-patentable subject matter), only as such. A computer-implemented invention shall be regarded as patentable within the meaning

of *Madde* 6 provided that the claimed invention defines technical features which solve a technical problem. The new Turkish Code of Industrial Property (22/12/2016 tarihli ve 6769 sayılı Sınai Mülkiyet Kanununa) entered into force on 10 January 2017 and it confirmed the adherence to the hybrid model. Finally, the third model is single binary, with copyright protection of computer programs, but absolute exclusion from patentability. This is the case with the Intellectual Property Code of the Philippines Act No. 8293 (s.172(1)(n) and (s.22(2)).

The EPC – effective in Turkey as of 1 November 2000 – excludes the patentability of computer programs claimed "as such" (art. 52(2)(c) and (3) EPC). Patents are not granted merely for program listings, which are protected by copyright. If a technical problem is solved in a novel and non-obvious manner, a CII patent may be granted.

For quite a long time, it was well established that the exclusion under Art. 52(2)(c) and (3) EPC applied to all computer programs, independently of their contents, independently of what the program could do or perform when loaded into an appropriate computer (e.g. *Röntgeneinrichtung* and *Editable document form*). This is no longer the case. The turning point has been *Computer program product/IBM*. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) played a critical role in the reasoning of the Boards of Appeal. Indeed, it was observed that under art. 27(1) TRIPS "patents shall be available for any inventions, whether products or processes, in all fields of technology". Therefore, allegedly, it would have been the clear intention of the TRIPS not to exclude from patentability any inventions, and, consequently, to include computer programs, provided that they have technical character. It is still not entirely clear what this technical character is, it would seem that it is everything that goes beyond the physical modifications of the hardware consisting in causing electrical currents, since this is common to all the computer programs. It is interesting that the latter are deemed to possess a technical character even if they do not produce a direct technical effect: the potential to produce a technical effect will do.

In my humble opinion, this interpretation collides with art. 10(1) TRIPS, whereby "[c]omputer programs, whether in source or object code, shall be protected as literary works under the Berne Convention". *Ubi lex dixit voluit, ubi noluit tacuit*.

The second turning point has been the opinion of the Enlarged Boards of Appeal in G 3/08. The President of the EPO referred the following point of law: “must a claimed feature cause a technical effect on a physical entity in the real world in order to contribute to the technical character of the claim?” The President noted that according to decisions *Colour television signal* and T 190/94, a technical effect on a physical entity in the real world was required. This was, however, not the case in *Gerätesteuerung/HENZE* and *Clipboard formats I/MICROSOFT*. In these decisions the technical effects were essentially confined to the respective computer programs. According to the Enlarged Boards, *Colour television signal* and T 190/94 merely accepted the effect on a physical entity “as something sufficient for avoiding exclusion from patentability; they did not state that it was necessary”. Since *Gerätesteuerung/HENZE* and *Clipboard formats I/MICROSOFT* considered that there were technical effects, “whether the boards concerned considered that these technical effects were on a physical entity in the real world was irrelevant”.

Nowadays, the CIIs do not receive a stricter assessment in comparison to other inventions. Indeed, in *DNS determination of telephone number/HEWLETT-PACKARD*, 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”.

‘Computer program/computer program product’ is one of the trickiest categories. The European Patent Office (EPO), indeed, stresses the (unclear) difference between the said category and the 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.” (European Patent Office, 2013).

The EPO distinguishes between two situations. On the one hand, inventions in which all the method steps can be carried out by generic data processing means. On the other hand, inventions in which at least one method step requires the use of specific data processing means or other technical devices as essential features (European Patent Office, 2016, 3.9).

Let us have a look at the first sub-category, which presents a higher risk of surreptitious software patenting. The EPO provides a non-exhaustive list which comprises examples of acceptable claim formulations (European Patent Office, 2016, 3.9.1). In particular, the model of acceptable set of claims is as follows: i. Method claim; ii. Apparatus/device/system claim; iii. Computer program (product) claim; iv. Computer-readable (storage) medium/data carrier claim.

If this pattern is followed, when assessing the novelty and inventive step of a set of claims, the examiner will start with the method claim. If the subject-matter of the method claim is considered novel and inventive, the subject-matter of the other claims will normally be novel and inventive as well. Conversely, claims that do not follow the pattern are assessed on a case-by-case basis in view of the requirements of clarity, novelty and inventive step. It is noteworthy that, as an example of the latter, the EPO provides the scenario "when the invention is realised in a distributed computing environment or involves interrelated products" (ibid.), that is, to some extent, the IoT. In this event, "it may be necessary to refer to the specific features of the different entities and to define how they interact to ensure the presence of all essential features" (ibid.), instead of making a mere reference to another claim as in the model set of claims.

It would seem that it could be harder to file an application for an IoT patent, in comparison with an average CII. This seems confirmed by the fact that the user interaction is increasingly important in a technological (and societal) development that claims to put the user at the centre. Indeed, if user interaction is required, an objection under Art. 84 EPC (clear and concise definition of the matter of the claim) may arise "if it is not possible to be determine from the claim which steps are carried out by the user" (European Patent Office, 2016, 3.9.1).

Final confirmation of the fact that IoT applications are less likely to be successful is the separate (and less favourable) regime afforded to inventions in which at least one method step requires the use of specific data processing means or other technical devices as essential features. The example provided is "If the invention involves an interaction between data processing steps and other technical means such as a sensor, an actuator etc." European Patent Office, 2016, 3.9.2). Devices with sensing and actuating capabilities, on the one hand, and data processing on the other hand are the main ingredients of the IoT. Now, sensors and actuators must be comprised in the independent claims if they are essential for carrying out

the invention. If the claims do not define which steps are carried out by the data processor or by the additional devices involved, as well as their interactions, objections of unclear and unconcise definition (art. 84 EPC) may arise.

The risk of software patents exists, but the EPO stresses that "it must be clear from the program that it is to be executed on the specific device" (European Patent Office, 2016, 3.9.2). Therefore, either a clear link between the software and the hardware is shown, or the patent would hardly be granted.

The guidelines on methods fully implemented by generic data processing means conclude in an obscure way. It refers to the guidance on claims comprising technical and non-technical features , "[f]or the assessment of inventive step for claims comprising features related to exclusions under Art. 52(2), as is often the case with CII". It is not clear what is often the case. On the one hand, it cannot mean that CIIs often comprise features related to computer programs or methods (and other excluded subject matter), because they always do. On the other hand, it does not seem to mean that CIIs usually fall under the excluded subject matter, because the reference is to the inventiveness test. It is important to keep patentability and inventiveness separate, because even the highest degree of inventiveness must not offset the lack of patentability of computer programs as such.

A common characteristic of CIIs is that non-technical features play a crucial role and they may prevail on the technical features (European Patent Office, 2016, 5.4). This has some effect on the assessment of the inventive step, which requires a non-obvious technical solution to a technical problem (*Two identities/COMVIK*; *Classification method/COMPTEL*). An example may be a method to reduce the network traffic of a game played on the cloud by reducing the maximum number of players. This cannot form the basis for the formulation of an objective technical problem. It is rather a direct consequence of changing the rules of the game, which is inherent in the non-technical scheme.

The EPO considers that some features may be non-technical *per se*, but, in the context of the invention, they could "contribute to producing a technical effect serving a technical purpose, thereby contributing to the technical character of the invention" (European Patent Office, 2016, 5.4). It remains unaffected that "features making no […] contribution [to the technical character of the invention] cannot support the presence of inventive step" (*Two identities/COMVIK*). An example may be a feature which contributes

only to the solution of a problem in a field excluded from patentability, such as computer programs.

This passage is critical because, even though the interrelation between software and hardware does not seem critical in the assessment of the patentability of CIIs (G 3/08), it becomes important in the assessment of the inventive step, because if the claimed CII resolves a problem which regards only the software, this problem will not be regarded as technical and the patent will not be granted for lack of inventiveness. Therefore, for instance, the programmer must have had technical considerations beyond "merely" finding a computer algorithm to carry out some procedure (G 3/08). Nonetheless, features of the computer program itself (*Computer program product/IBM*) as well as the presence of a device defined in the claim (*Clipboard formats I/MICROSOFT; Auction method/HITACHI*) may potentially lend technical character to the claimed subject-matter (European Patent Office, 2016, 3.6).

From an IoT perspective, it is worth mentioning the patentability of simulations, given the growing importance of virtual reality, holographic technologies, and augment reality. In *Checkpoint simulation/ACCENTURE*, the Boards of Appeal pointed out that the definition of technical processes seemed not to cover simulations, whose purpose is to replace physical entities with virtual ones. In T 208/84, the board had held that a technical process is different from a mathematical method in that the technical process is carried out on a physical entity and provides, as its result, a certain change in that entity. *Schaltkreissimulation I/Infineon Technologies* reversed it and held that the simulation of an adequately defined class of technical items could be a functional technical feature. In *Call center/IEX*, finally, the board left open the question whether it is a sufficient condition for a simulation to be patentable that the simulated items be technical. It observed that the simulated system was not technical; therefore, the condition did not hold.

The situation in Europe is still very much uncertain. In 2002, the European Commission drafted a Proposal for a Directive of the European Parliament and of the Council on the patentability of computer-implemented inventions (COM(2002) 92), which was ultimately rejected in 2005. The main reasons for the failure were the fear of extension of the patentable subject matter. It is what it is, but it is clear that harmonised and clear rules would benefit both businesses and consumers.

3. Brief notes on software patents and the Internet of Things.

The most analysed legal aspect of the IoT is privacy (Yeoh 2017; Beardwood and Bowman 2016; Weber 2015; Linkomies 2015), but scholars are starting to look into intellectual property (Lundqvist 2016; Zingales 2015) and patents seem to play the main role (Noto La Diega 2017; Trappey et al. 2016; Intellectual Property Magazine 2016; Ho and Huang 2016; Ho and Stein 2016; Ho 2016a; Ho and Johns 2016; Amundson 2016; Robinson 2015). As reported by Trappey et al. (2015), the top assignees (and therefore top IoT players) are Intel, IBM, Samsung, Huawei, ZTE, Qualcomm, Ericsson, Fujitsu, Siemens, and Nokia. In 2015, Samsung was the IoT leader in R&D expenditure. The top countries by assignees are the US, China, Japan, and Korea (with the WIPO, not technically a country, having more assignees than Korea). The IoT leaders the IoT leaders are bidding on sensors, wireless communication, as well as embedded systems. Finally, Trappey et al. (2016) found that, under the International Patent Classification the H04L class (transmission of digital information) dominates the industry, particularly in relation to multiplexing methods, baseband processing, and protocols. If one divides the IoT's layers in perception, transmission, computation, and application, the second one appears to be the most densely patented. Finally, as to the technologies, most patents refer to software, circuits, hardware, sensors, and encryption. These data enable the authors to conclude that "the IoT market will produce a wide array of new sensors, actuators, controllers, and circuits, as well as their transmission techniques in compliance with standards and forming IP ecosystems for adaptation and commercialization" (Trappey et al. 2016, 15).

Future research will need to address other fundamental intellectual property issues, for instance if and to what extent trade secrets can be used to prevent the user from controlling their own device (the so-called right to hack one's own device, for instance to repair it). Likewise, it is still to be fully explored to what extent intellectual property (database rights) can be used for datafication purposes, e.g. by preventing data portability, whose importance will increasingly grow with smart devices becoming commonplace and with the fading of the online/offline distinction. As noted by Lundqvist, "data, originating from users, from devices, sent through the 4G and 5G networks to the client servers and the Cloud are heavily boxed in by intellectual property rights" (2016, 10). Furthermore, for a copyright case, one could refer to the recent *Cisco Systems, Inc. v. Arista Networks, Inc.*,

The court found that Arista was not liable for using hundreds of command-line interfaces in its networking switches that Cisco Systems developed, due to the doctrine of *scénes á faire*. It was commented that many IoT players "were closely watching this case to see what parts of the IoT ecosystem could be protected by copyrights" (Mar and Liaw 2016). One could question, finally, whether the way devices interact (e.g. in a smart home environment) may be trademarked.

When it comes to patent law, which is the focus of this paper, CIIs are the only topic to be explored. Given technology convergence, industry fragmentation, and the need for interoperability, licensing is becoming as fundamental as complicated. It has been suggested that patent license packages for joint licensing and super packages (packages of patent licence packages) might constitute an answer (Ho 2016b). Reportedly, "[t]he patent licensing landscape for this market is on the verge of explosive growth" (Elvidge, Morrison, and Bijman 2016). If interoperability is key to the IoT, then standard essential patents and licences on FRAND terms will play a fundamental role (CEN and CENELEC 2016). Without full interoperability, we will have the Internet of Silos, as opposed to the IoT. Competition law and data protection may help opening up the silos, thus counterbalancing the abuse of proprietary systems. It has been noted that embedded software systems are often legacy, closed-box systems that prevent machines from communicating with each other over the IoT protocols (Lee 2006). Patents are, indeed, not the only hindrance to interoperability (let us think of trade secrets and copyright), therefore some authors call "for the EU to produce soft law encouraging best practices and addressing the tensions between standardization and intellectual property other than patents" (Zingales 2015, 5). A coordinated and holistic strategy is to be recommended.

More generally, given the growth of the IoT market, it is foreseeable that companies will use patents to secure their share in the relevant benefits. As recognised by Robinson (2015), IoT technology raises issues concerning patentability, joint infringement and patent quality. The first two issues are seen as surmountable. As to the latter, it is predicted that US Patent and Trademark Office's quality initiatives may lead to IoT patents of a reasonable scope.

Moving on to the focus of the paper, which also other authors see as the main patent law issue (Zingales 2015, 9), mischievous commentators may argue that the CIIs are a surreptitious way to obtain a double binary for software protection. This may become true

with the IoT. Indeed, with the gradual substitution of old products with smart devices, we will face an unprecedented growth of CIIs; therefore, asserting that computer programs are not patentable in Europe may sound hypocritical. In other terms, I foresee that most of the computer programs will be embedded in smart devices, with the consequential patentability of most computer programs under the label of CII.

The impact of the IoT on patents can be observed also from another point of view. I believe that the IoT provokes a redefinition of the inventive concept for purposes of assessing patentability, essentially because of two characteristics: (a) network structure: patentability may increasingly derive from the way smart devices interact; (b) composite nature of the said devices: novelty might stem from the way the components of a single device interact.

As to the first aspect, the customers are more and more interested to the novel interaction between their devices, rather than to the device in isolation (let us think a hub in a domotics context). Interoperability and open standards are the way forward, even though security plays often the role of excuse to build closed sub-systems, thus giving rise to the "Internet of Silos".

When it comes to the composite nature of devices, it means that usually devices incorporate several other devices. A smartphone contains a large number of sensors and a damage may occur because of a defect or inaccuracy of any of the said components of the device. It is not always clear if the liability should fall on the main actor responsible for the composite device or if its component's actors should be liable. Generally speaking, and unless a contrary evidence is provided, I am in favour of the first hypothesis, for at least two reasons.

Firstly, the final manufacturer has a duty to double-check the security and safety of the composite device both when placing it on the market and during the provision of the services. Secondly, it could prove impossible for the customer to track the supply chain and find the responsible for the single sub-thing. The conclusion may be different depending on the openness or closure of the system (e.g. Apple can control third-parties' apps through its store, whereas Android stores are open, thus not allowing the same control). Courts may also give some relevance to the number of sub-things present in the composite thing (an airplane is not the same as a light bulb) and the kind of activity for which the device is used (a

defibrillator can save a life and therefore higher standards of security and a stricter scrutiny are required) (Noto La Diega, 2016).

4. Some recent patent litigation in the US: *Alice* through the looking glass?

My prediction that CII cases will become more and more common has been confirmed, for instance, by the fact that Davis (2016) opens his list of top patent cases of 2016 with the "Alice reversals". As is common knowledge, *Alice Corp. v. CLS Bank International* held that a computer-implemented, electronic escrow service for facilitating financial transactions was not patentable, in that it covered only abstract ideas.

The petitioner argued that a computer "necessarily exist[s] in the physical, rather than purely conceptual, realm" (Brief for Petitioner 39). According to the US Supreme Court, however, the fact is beside the point. Indeed,

"*There is no dispute that a computer is a tangible system (in §101 terms, a "machine"), or that many computer-implemented claims are formally addressed to patent-eligible subject matter. But if that were the end of the §101 inquiry, an applicant could claim any principle of the physical or social sciences by reciting a computer system configured to implement the relevant concept*".

If that was the case, the determination of patent eligibility would "depend simply on the draftsman's art," (*Parker v Flook*, at 593), thus sterilizing the rule whereby "'[l]aws of nature, natural phenomena, and abstract ideas are not patentable." (*Association for Molecular Pathology v Myriad Genetics*). *Alice* at 2355 refers to *Mayo v Prometheus*. In *Mayo*, the Supreme Court set forth a two-step analytical framework to identify patents that, in essence, claim nothing more than abstract ideas. The court must first "determine whether the claims at issue are directed to a patent-ineligible concept." If so, the court must then "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." (*Mayo*, 132 S. Ct. at 1298, 1297). The Supreme Court described this as a "search for an 'inventive concept'—i.e., an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" (Id.).

As to pre-emption, finally, *Fitbit, Inc. v Aliphcom, et al* reaffirmed that the "concern that undergirds [the] § 101 jurisprudence" is pre-emption (*Alice* at 2358). If a claim is so abstract so as to "pre-empt use of [the claimed] approach in all fields, and would effectively grant a monopoly over an abstract idea" is not patent-eligible (*Bilski v. Kappos* at 612). Relatedly, "claims that are 'so result-focused, so functional, as to effectively cover any solution to an identified problem' are frequently held ineligible under section 101." (*Affinity Labs of Texas, LLC v. DIRECTV, LLC* at 1265). More importantly, they reiterated that "[w]hile preemption may signal patent ineligible subject matter, the absence of complete pre-emption does not demonstrate patent eligibility." (*Fairwarning IP* at 1098).

It has been observed that "subject matter eligibility might stand in the way of IoT patents because many IoT inventions are computer related" (Ho and Stein 2016), but it would seem that the wind is blowing in a new direction.

As reported by Sachs (2015), in October 2015 about 73 percent of motions arguing that patents were invalid under Alice have been granted by federal courts. Applicants had to focus patents on very narrow areas of protection in order to aspire to get an IoT (or, more generally, a CRI) patent. This could be done, for instance, by specifying the use of particular hardware or by providing specific operations, such as detailed algorithms (Ho and Johns 2016). The first root seems to be particularly suitable for the IoT, because if the applicant clearly links the operation of the software to a particular device, this would significantly strengthen the application. This said, after *Alice* and *Mayo,* it seemed that patenting software was a chimera. In recent times, however, there seems to be a change of policy and IoT patenting is likely to become easier.

The first example is provided by *ENFISH, LLC v. Microsoft Corp*., which reversed a district court's and conclude that all five claims on appeal were patent-eligible. The Court of Appeals observed at 1335 that

"some improvements in computer-related technology when appropriately claimed are undoubtedly not abstract, such as a chip architecture, an LED display, and the like. Nor do we think that claims directed to software, as opposed to hardware, are inherently abstract"

Applying the *Mayo* two step test, firstly, one has to assess if the claim is on a specific asserted improvement in computer capabilities or on a process that qualifies as an "abstract idea" for which computers are invoked merely as a tool. The second step asks if, nevertheless, there is some inventive concept in the application of the abstract idea. Therefore, according to *Enfish, Alice* should not be read as broadly holding that all improvements in computer-related technology are inherently abstract, thus having to be considered at step two. In *Enfish*, consequently, *Alice* has been interpreted narrowly, thus considering patentable “a specific improvement to the way computers operate, embodied in the self-referential table” (ibid at 1336).

Other evidence of the change of policy in the sense of a more liberal approach in recognising software patents comes from *Bascom Global Internet Services, Inc. v. AT&T Mobility LLC*. The US Court of Appeals for the Federal Circuit reversed a decision of the US District Court for the Northern District of Texas (No. 3:14-cv-03942-M, Judge Barbara M.G. Lynn) by holding that Bascom Global Internet Services’ patent on filtering internet content improved computer functioning and, therefore, was not an abstract idea. The broad approach builds on *DDR Holdings, LLC v. Hotels.com* (Judge Raymond Chen filed both the majority opinions), whereby what matters is that an invention “is not merely the routine or conventional use of the Internet” (ibid. at 1259). One has to notice that the *Enfish* claims, understood in light of their specific limitations, were unambiguously directed to an improvement in computer capabilities. Unlike *Enfish*, here the claims and their specific limitations “do not readily lend themselves to a step-one finding that they are directed to a nonabstract idea” (*Bascom* at 13). Therefore, the Court defer its consideration of the specific claim limitations’ narrowing effect for step two, which means assessing the inventive concept. Allegedly, the District Court has ignored that “[t]he inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art. As is the case here, an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces” (ibid. at 15). Finally, it is interesting that the concurring opinion tends towards an even more relaxed approach to software patents. Indeed, Judge Newman urges “a more flexible approach to the determination of patent eligibility, for the two-step protocol for ascertaining whether a patent is for an ‘abstract idea’ is not always necessary to resolve patent disputes”.

If the stream inaugurated with *DDR* and confirmed by *Enfish* and *Bascom* will lead the development of the future case law, there is the concrete risk that patents will be granted

for every software and method, with the sole exclusion of "longstanding, well-known method[s] of organizing human behavior" (*Bascom* at 12). If one analyses the aftermath, this does not provide evidence for a clear prediction. Indeed, on the one hand, *Fairwarning IP, LLC v. Iatric Sys, Inc.*, *Affinity Labs, LLC v. Amazon.Com Inc. et al.*, and *Intellectual Ventures I LLC v. Symantec Corp.* conclude with patent-ineligible subject matter.

On the other hand, leveraging the above analysed recent case law, *Micro, Inc. v. Bandai Namco Games Am., Inc.* concluded that "the ordered combination of claimed steps, using unconventional rules that relate sub-sequences of phonemes, timings, and morph weight sets, is not directed to an abstract idea is patent-eligible".

A similar trend was confirmed by in *Amdocs (Israel) Ltd v Openet Telecom Inc*, the Federal Circuit found that the claims at issue could be patentable in light of their written descriptions. Thus, it reversed the District Court's decision whereby the claims were directed to the abstract ideas of correlating two network accounting records to enhance the first record and using a database to compile and report on network usage information. In this case, the Court of Appeals held that even if they were to agree that the claims were directed to ineligible abstract ideas under step one of the *Mayo* test, nonetheless they would be eligible under step two because they allegedly contain a sufficient "inventive concept" (this does not mean, however, that they are valid). It is noteworthy that Circuit Judge Reyna dissented and criticised the majority for "avoid[ing] determining whether the asserted claims are directed to an abstract idea, or even identifying what the underlying abstract idea is". I join the dissenting opinion also, inasmuch as, even though it accepts that the written description discloses a patentable network monitoring system, it stressed that "the inquiry is not whether the specifications disclose a patent-eligible system, but whether the claims are directed to a patent ineligible concept". There would seem to be a contrast with the case law that clarifies that the "§ 101 inquiry must focus on the language of the Asserted Claims themselves […] complex details from the specification cannot save a claim directed to an abstract idea that recites generic computer parts" (*Synopsys v Mentor Graphics Corp* at 20–21, citing *Accenture Global Servs GmbH v Guidewire Software Inc* at 1345).

Likewise, a motion tracking system was found patentable in *Thales Visionix Inc. v. United States*. The Claims Court had found the claims ineligible, because they were directed to the abstract idea of using laws of nature governing motion to track two objects, and they provided no inventive concept beyond the abstract idea. The Federal Circuit reversed the

decision. Leaning on *Diamond v. Diehr,* the Court concluded that "the claims are directed to systems and methods that use inertial sensors in a non-conventional manner to reduce errors in measuring the relative position and orientation of a moving object on a moving reference frame." The court held that the invention applied laws of physics to solve this problem, and the mere presence of a mathematical equation in the solution "does not doom the claims to abstraction."

There is the risk of a gradual departure from *Alice* and *Mayo*, up to the point of patenting abstract ideas with no proper inventive concept. Soon, we might leave Wonderland and we would see *Alice* only through the looking glass. I join the concurring opinion of Judge Mayer in *Intellectual Ventures* (considered the "big event" of the case by Crouch, 2016), whereby claims directed to software implemented on a generic computer are categorically not eligible for patent. In particular,

"*the claims at issue in* BASCOM, Enfish, *and* DDR, *like those found patent ineligible in Alice, do 'no more than require a generic computer to perform generic computer functions'* Alice, *134 S. Ct. at 2539. Eliminating generally-implemented software patents would clear the patent thicket, ensuring that patent protection promotes, rather than impedes, 'the onward march of science' (*O'Reilly v Morse, *56 U.S. (15 How.) 62, 113 (1853), and allowing technological innovation to proceed apace*".

Roberts (2016) has commented that now, given this concurring opinion, "software patents are in peril". It is not causal that the other point of Judge Mayer's opinion was that "patents constricting the essential channels of online communication run afoul of the First Amendment". Indeed, a holistic approach to patents should take into account a number of trade-offs and endeavour to strike a balance between the conflicting interests, such as the right of the applicant to government-sanctioned monopolies, on the one hand, and, on the other hand, the "right to receive information and ideas [which] regardless of their social worth, is fundamental to our free society." (Stanley v. Georgia, 394 U.S. 557, 564 (1969). A similar approach, unprecedented in US law according to Crouch (2016), is already part of the European tradition, as one can see, for instance, in *GS Media BV v Sanoma Media Netherlands BV and others*, even though sometimes the result of the balance favours private interests, as pointed out by Nivarra (2011). Indeed, on 8 September 2016, the Court of Justice, in proposing a liberal approach to hyperlinking, has stressed that

"*the harmonisation effected by it is to maintain, in particular in the electronic environment, a fair balance between, on one hand, the interests of copyright holders and related rights in protecting their intellectual property rights, safeguarded by Article 17(2) of the Charter of Fundamental Rights of the European Union ('the Charter') and, on the other, the protection of the interests and fundamental rights of users of protected objects, in particular their freedom of expression and of information, safeguarded by Article 11 of the Charter, and of the general interest*" (*GS Media* at 31).

Finally, news from the world of quantified self and activity tracking confirm that CII litigation is increasing in relation to the growth of the IoT. In a forest of IoT patents (the so-called patent thicket), every step ahead may lead to an infringement.

An example is provided by the Aliphcom (Jawbone) / Fitbit lawsuits. The companies involved are giants in the market of quantified self and wearables. On 28 April 2016, two of the Jawbone' patents that were disputed at the U.S. International Trade Commission (ITC) were invalidated. Since Jawbone was trying to leverage those patents to prevent Fitbit's imports in the US, now this result appears hardly achievable. However, a Jawbone representative has pointed out that the patent ruling will be appealed and that "the two patents that are the subject of the ITC ruling represent only a portion of Jawbone's case against Fitbit and a small subset of Jawbone's overall patent portfolio" (Goode, 2016). Nonetheless, on 23 August 2016, Judge Dee Lord of the ITC struck-down Jawbone's request for an import ban against Fitbit products "the competitors' cross-filings for patent infringements had all been invalidated" (Trade Secrets Institute, 2016).

What is interesting from our perspective, is the official court filing states that the claims on the relevant patents "seek a monopoly on the abstract ideas of collecting and monitoring sleep and other health-related data." Consequently, they are not eligible for the grant of a patent, also because "no innovating concept is claimed in either patent. With particular regard to systems for organizing human activity, the courts have determined that a patent is not eligible when it claims the use of computer technology to accomplish tasks that were in the past performed by human beings." the filing states.

This ruling takes a strict approach to CIIs, which is commendable, since we foresee that an increasing number of applications for patents on IoT-software will be filed. The ruling has also an impact on the world of artificial intelligence and artificial enhancement.

These technologies are progressively substituting human beings in their everyday tasks. Inventors and developers shall be aware that, generally speaking, there will be a tendency not to award patents for inventions enabling machines to accomplish tasks once performed by human beings.

The road to a possible IoT patents war, that will overshadow the smartphone wars, is then evidenced by another lawsuit between the same parties, with Fitbit this time as a plaintiff (*Fitbit, Inc. v Aliphcom, et al.*). The court denied Jawbone's motion for judgement on the pleadings that three of Fitbit's patents on devices pairing methods are invalid for failure to claim patent-eligible subject matter. Given the importance of communications between devices for the growth (and for the existence itself) of the IoT and given the subsequent relevance of pairing technologies, this case may have an impact that goes well beyond the quantified-self domain. The court recognises that there are both reasons in favour and against the qualification as abstract idea (step one of the *Alice/Mayo* test), therefore they move on to step two, which courts must approach cautiously, "scrutiniz[ing] the claim elements more microscopically" than in step one (*Electric Power Group, LLC v Alstom S.A.* at 1354).

Fitbit claimed that the use of a server to identify eligible devices and the use of tapping, detected by a motion sensor, to validate a pairing were unconventional elements which supply an inventive concept. However, the Court agreed with Jawbone that none of the claim elements, assessed *individually*, provide an inventive concept. Indeed, "server," "client," and "portable monitoring device" are, in broad terms, generic, conventional components, none of which are inventive. The various steps of transmitting or receiving information and how they are accomplished are also generic—the claims recite these steps only functionally and require no inventive algorithm or data structure for performing them. Moreover, the Court also agreed with Jawbone that the claims' relation to wearable activity tracker technology, in and of itself, does not make them patent-eligible (*Alice* at 2358: limiting the use of an abstract idea "to a particular technological environment" is not enough for patent eligibility).

Nonetheless, the Court agreed with Fitbit that both the use of tapping and the use of a server, when considered along with the rest of the claims as an *ordered combination*, supplied an inventive concept that transformed the asserted claims into patent eligible subject matter under step two. Indeed, a difference between the smartphone and many IoT

devices is that the latter are smaller. Therefore, their design does not allow keyboards and/or buttons. This is a problem on many respects, including the pairing of the devices. Therefore, the Court saw the addition of tapping as the form of validation as an inventive concept. Moreover, Jawbone seemed to conflate inventive concept and novelty inasmuch as they argued that tapping could not supply an inventive concept since it was known in the art. Therefore, tapping transformed the asserted claims into something more than an abstract device pairing process: it "improve[d] an existing technological process" (*Alice* at 2358) by expanding the scope of devices that can be paired. Furthermore, the injection of a server to regulate and facilitate the pairing process was deemed to supply an inventive concept. Thus, the asserted claims shift the traditional paradigm so that all of the information needed for pairing does not have to be provided through the two devices.

It seems clear that these lawsuits "presage wider patent disputes over IoT technologies as they mature and more products become available to consumers" (Amundson 2016). The described trend, which seems quite favourable to the patent eligibility of IoT inventions, may contribute to increase the propertisation of IoT devices and the relevant shift from the IoT to the Internet of Silos. It is hoped that issues of divided infringement and territorial scope will somehow slow down the process, in consideration of the possible difficulties in enforcing IoT patents.

5. The Guidelines on the examination of computer-related inventions. Historical background, basic concepts and the (not always savvy) protests of the civil society.

It is not sufficiently known that India has a pioneering role in the development of new technologies and new approaches to the concept itself of innovation.

A notable example is Ministry of Electronics & Information Technology (2015), which builds on the 'Digital India Programme.' In issuing it, the Department of Electronics and Information Technology ('DeitY') pursued four goals. Firstly, to create an IoT industry in India of USD 15 billion by 2020 (with a share of 5-6% of 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. Lastly, to develop smart devices specific to Indian needs in all possible domains. The policy has been seen by

Aggarwal (2015) as the realisation of the "*Zero Defect Zero Effect*" slogan, which was coined by Prime Minister of India, Narendra Modi. Part of the Make in India strategy, it denotes manufacturing mechanisms whereby the possibility of error and the environmental impact are, or should be, eliminated. Malevolent commentators may judge it as a 'green washing' policy in order to convince transnational corporations to manufacture their products in India and to increase the exportations. In fact, in the Independence Day speech, Modi had said that the 'zero defect, zero effect' policy was critical so that "our exported goods are never returned to us." (Modi, 2014) However, the reasons for the policy will prove to be of secondary importance, as long as the implementation activities will be carried out with the bottom-up inclusive approach that we are seeing in the deployment of the Indian smart cities plan, as in Ministry of Urban Development (2015).

Future research shall focus on the risks of such a fast growth. For instance, in 2010, the Government of India (better said, the Unique Identification Authority of India, 'UIDAI') has 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 (Miglani & Kumar, 2016). On 25 March 2016, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 has received the assent of the President. The Act provides federal agencies with the right to access the said database in the interest of national security. There is the actual risk of using the largest biometric database in the world for surveillance purposes.

India, unlike the US, is following the double-binary European approach. Indeed, s.3(k) of the Patents Act 1970 states that a "computer programme *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 who knows that the Patents Act, notwithstanding its amendments, remains an old act, as shown inter alia by the several provisions on floppy disks.

The path towards the introduction of software patents had been gradual and Brownian. In 2002, the Patents (Amendments) Act, 2002 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 program 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 programs as such are not intended to be granted patent." (Comments and recommendations on the Guidelines, 2015). The first guidance explained 'ancillary' by referring to "things which are essential to give effect to the computer program."

The second step was the Patents (Amendment) Ordinance, 2004. At that time, an amendment to provide for the patentability of computer programs 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." (Chathurvedula, 2015).

A similar failed attempt was made by the Patents (Amendment) Bill, 2005 that sought to extend patentability to computer programs with "technical application to industry". The 'transnational corporations' exception was successfully raised again.

In 2011, then, the Controller General of Patents, Designs and Trade marks (hereinafter the 'Controller', the Indian homologous of the Intellectual Property Office) clarified that "claims directed at 'computer program products' are computer programs per se stored in a computer readable medium and as such are not allowable." (Office of Controller General of Patents, Designs & Trademarks 2011, 08.03.05.10.) Moreover, when a claim inter alia contains a subject matter that is not limited to a computer program, "it is examined whether such subject matter is sufficiently disclosed in the specification and forms an essential part of the invention." (ibid).

It is notable that the draft CRI guidelines published in 2013 were clear as to the exclusion of any computer program that may work on any general-purpose computer or "related device" (mainly smart devices) did not meet the requirements of law.

In August 2015, the Controller issued the first CRI guidance; it allowed the patenting of programs, which demonstrated technical advancement. Unsurprisingly, the guidance gave rise to protests of the civil society. Many organisations and citizens, indeed, complained about the contrast with s.3(k) of the Patents Act and because software patentability was seen as a break to innovation (Concerns over the "Guidelines, 2015). 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 programs were excluded "unconditionally" and that the one at issues 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 program, or - a *novel computer program 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 program, "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*." (Office of Controller General of Patents, Designs and Trademarks (2013), para 5.1).

The letter of the 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."

After the said protests, with order No. 70 of 2015, 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 19 February 2016, when the Controller published the new guidelines on the examination of CRIs (Office of the Controller General of Patents, Designs and Trade marks, 2016).

CRIs now 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 program or programs." Incidentally, one may note that 'other programmable apparatus' is a flexible concept indeed capable to encompass smart devices. 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 programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions." A very 'IoT' dictionary. 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."

The new guidelines reaffirm the exclusion of the software patents and introduces a three-step test to determine the applicability of s.3(k) of the Patents Act to CRIs. Indeed, "[e]xaminers 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 program, check whether it is claimed in conjunction with a novel hardware* and proceed to other steps to determine patentability with respect to the invention." (Guidelines 2016, s.5) Therefore, if the hardware is not novel (e.g. some innovative smart device), then no patent will be granted. It would seem, consequently, that computer programs running on traditional computers should be excluded by the subject matter of patents. This is particularly clear if one reads the previous version of the guidelines, which included the eligibility of "a novel computer programme 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".

Moreover, even though the phases of the examination procedure of CRIs are the same as the other inventions as to novelty, inventive step, 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." 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" ('what') and the specification has to explain the best method of operation. 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.

Even though the use of '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 require "greater skill"), the wording is adamant in linking the patentability of CRIs to inventions which constitute an inextricable mixture of software and (novel) hardware; that is to say, to smart devices. 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. Moreover, as a policy recommendation and in consideration of the foreseen growth of CIIs due to the IoT, the European Patent Office may want to be inspired by the Indian guidelines to update and deepen its out-of-date and insufficiently thorough guidance. A first commendable step has been the publication of the 8th edition of *Case Law of the Boards of Appeal of the European Patent Office* in July 2016, but some ad-hoc guidelines would be more appropriate.

6. Conclusions

With the advent of the IoT, applications for software patents disguised as CIIs will increase substantially in Europe. A similar phenomenon will take place in the United States, where there is the risk of a departure from *Alice*, with subsequent patentability of IoT inventions directed to an "abstract idea" and that do not add "significantly more" to that abstract idea. Besides these trends, it is not deniable that linking a claim to a specific device (as opposed to a generic computer) would make grant of a patent more likely (even though it may not be sufficient in itself). A larger number of IoT patents, currently increasing eight times faster than patents in other domains, will also lead to an increase in litigation. It is foreseeable a shift from the smartphone wars to the IoT wars (a taste of it coming from the Jawbone / Fitbit lawsuits). Indeed, the underlying forces of the smartphone wars were huge economic impact, multiple converging technologies, fragmented industry, competing

standards, as well as significant patent stockpiles. These apply all the more the IoT market, which makes a war likely. In particular, the complexity of the supply chain, the several domains in which the IoT is divided and the composite nature of the IoT devices are among the main reasons of the impending wars. These could also take the form of "a cold competition with grudging exchanges of cross-licenses and agreements not to sue" (Ho 2016a). This would seem the case with the Adidas / Under Armour settlement in May 2016, when the former granted the latter a license to some patents in exchange for a licensing fee paid by Under Armour and MapMyFitness.

The traditional view is that the United States Patent and Trademark Office undertakes less rigorous patent examination than the EPO (Nightingale, 2016). I do not know if the contrary has become true, like a recent study claims (Christie et al., 2016). However, in the field of CIIs it seems to me that both the systems are prone to recognizing a wide protection with subsequent increased propertisation of knowledge. It may be not useless to remember that intellectual property is about striking a balance between a number of (sometimes conflicting) private and public interests. A too strong patent regime for computer programs, in a moment when software is being embedded in most traditional devices, risks not to take into account the trade-off between remuneration of the investments and public good. Moreover, the prevalence of proprietary models can jeopardise interoperability, which is at the very heart of the IoT. Furthermore, there are issues of competition law. It has been noted that since IoT manufacturers will run to get patents "[n]ational regulators must […] apply utmost prudence to ensure that grants do not act as barriers to new entrants in existing and emerging markets" (Consumers International, 2016, 78). It is noteworthy, inter alia, that the "[t]op patent filer in the field hold[s] around 5% of the total patents" (LexInnova 2016). From a consumer law perspective, there is the "risk that intellectual property arguments and digital rights management will extend to products and services containing software, and risk superseding consumer protection law" (ibid., 5). But regimes such as product liability, unfair terms, unfair commercial practices, and data protection can prevail on contracts and licences, thus preventing intellectual property abuses.

There are some good practices to be followed. For instance, on 28 October 2016 a new exemption to the Digital Millennium Copyright Act has come into force allowing the circumvention of DRM and the reverse engineering of consumer devices for security purposes. Being eventually legal to hack one's own devices, it would seem that consumers

may be (relatively) back in control of their devices, notwithstanding the intellectual property protections (Greenberg, 2016).

Another approach that should be followed is the Indian one. After the civil society has (maybe too) harshly criticised the first version of the guidelines on the CRIs, the Government has revised them in order to make clear that in no way CRIs will be a surreptitious way of granting software patents.

With some exceptions, such as the Republic of Philippines, there is evidence that the world is going towards a wider patentability. One could mention, for instance, China. On 28 October 2016, indeed, the State Intellectual Property Office of the People's Republic of China (中华人民共和国国家知识产权局) has launched a public consultation on the revised Guidelines for Patent Examination. As to the examination criteria concerning computer programs, it is proposed to replace "computer programs" with "computer programs *per se*"[1].

It is not entirely clear if the United States and Europe are going towards the patentability of abstract ideas and computer programs *per se*, respectively. The above analysis has sent mixed signals. The legal systems seem to become more favourable to the IoT patenting and the characters themselves of the IoT market and of its devices may favour the patentability. However, on the one hand, there is evidence of an impending IoT war; on the other hand, even though once patented the enforceability could be difficult due to divided infringement and territorial scope issues.

It has been observed that "[m]ost of the innovation on the so-called Internet of Things is locked up in patents held by the companies that make the innards of sensors, routers, and other devices" (Wong 2016). If the justification of the monopolies stemming from patents is innovation, then something is going wrong. One should only wish that legislators and regulators were aware of the indeed negative consequences of software patents becoming commonplace in an IoT world.

Reference list

Aggarwal, V. (2015). India's first Internet of Things policy to focus on Zero Defect, Zero Effect. *The Economic Times India*. Retrieved from

[1] Part II, Chapter 9, Section 2 of the Guidelines. See Li (2016).

articles.economictimes.indiatimes.com/2015-04-10/news/61017670_1_iot-m-sips-draft-policy.

Amundson, S. (2016). United States: Patent Disputes Over Wearables May Herald BroaderPatent Litigation Regarding The Internet Of Things. *Mondaq Business Briefing* (4 April)

Beardwood, J., and Bowman, M. (2016). The internet of things and privacy: when do privacy laws apply*? Comps. & Law*, *26*(Jun/Jul), 37-40.

CEN and CENELEC (2016). *Standard Essential Patents and Fair, Reasonable and Non-Discriminatory (FRAND) Commitments* (CEN-CENELEC)

Chathurvedula, S. (2015). Revised guidelines for software patents put on hold. *Live Mint*. Retrieved at www.livemint.com/Industry/XGBbgNllmvuEUhJWs2cWgK/Revised-guidelines-for-software-patents-put-on-hold.html.

Christie, A.F., Dent, C. & Liddicoat, J. (2016). The Examination Effect: A Comparison of the Outcome of Patent Examination in the US, Europe and Australia, *J. Marshall Rev. Intell. Prop. L.*, *16*, 21.

Comments and recommendations on the Guidelines for Examination of Computer-Related Inventions (CRIs) (2015). Retrieved at www.knowledgecommons.in/wp-content/uploads/2015/11/Comments-Recommendations-on-CRI-Guidelines-2015.pdf.

Concerns over the "Guidelines for Examination of Computer Related Inventions (CRIs)" (2015). Retrieved at sflc.in/wp-content/uploads/2015/09/Letter_CRIGuidelines2015-Prime-Minister.pdf.

Consumers International (2016). Connection and Protection in the Digital Age. The Internet of Things and challenges for consumer protection. April 2016. Retrieved at http://www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

Crouch, D. (2016). First Amendment Finally Reaches Patent Law. Retrieved at http://patentlyo.com/patent/2016/10/amendment-finally-reaches.html.

Davis, R. (2016). The Top Patent Cases of 2016: Midyear Report. Retrieved at http://www.law360.com/articles/812729/the-top-patent-cases-of-2016-midyear-report.

Elvidge, J., Morrison,J., and Bijman, M. (2016). The IoT : A Look at the IP Landscape of Fitness Wearables. *IP Watchdog* (24 August).

European Patent Office. (2016). Guidelines for Examination in the European Patent Office, November 2016. Retrieved from http://www.epo.org/law-practice/legal-texts/html/guidelines/e/index.htm

European Patent Office. (2013). *Patents for software? European law and practice*. Retrieved from documents.epo.org/projects/babylon/eponet.nsf/0/a0be115260b5ff71c125746d004c51a5/$FILE/patents_for_software_en.pdf.

Goode, L. (2016). Fitbit wins big in trade ruling vs. Jawbone. *The Verge*. Retrieved at http://www.theverge.com/2016/4/29/11538454/fitbit-wins-trade-patent-ruling-vs-jawbone-ineligible

Greenberg, A. (2016). It's Finally Legal to Hack Your Own Devices (Even Your Car). *The Wired*. Retrieved at https://www.wired.com/2016/10/hacking-car-pacemaker-toaster-just-became-legal/?mbid=nl_11116_p3&CNDID=32599349

Greenough, J. (2014). The 'Internet of Things' will be the world's most massive device market and save companies billions of dollars. *Business Insider UK* (18 November).

Ho, K. (2016a). United States: Internet Of Things: Another Industry Patent War? *Mondaq Business Briefing* (5 January)

Ho, K. (2016b). United States: 4 Things You Need To Know About The ImpendingInternet-Of-Things Patent Wars. *Corporate Counsel* (16 May)

Ho, K. and Huang, H.-Y. (C.) (2016). Internet Of Things Patents: Tough To Enforce? *IoT Central* (7 November)

Ho, K., and Johns, C.C. (2016). Patent the Internet Of Things, or Not? *TechBeacon* (18 January)

Ho, K., and Stein, J.D. (2016). 3 Challenges for Internet-Of-Things Patents. *Law360* (10 June)

Horbal, P. (2015). Patents and the Internet of Things. *Mondaq Business Briefing* (29 July)

Intellectual Property Magazine, Things just got interesting, *I.P.M.*, Feb, 7-8.

Intellectual Property Office (2014). *Eight great technologies: The internet of things* (UK Intellectual Property Office)

Lee, E.A. (2006). Cyber-physical systems – Are computing foundations adequate? *Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*

LexInnova (2016). Internet of Things. Patent Landscape Analysis (WIPO).

Li, Y. (2016). Chinese Patent Office proposed revisions to its Examination Guidelines, 16 November 2016. Retrieved at http://trustinip.com/chinese-patent-office-proposed-revisions-to-its-examination-guidelines/.

Linkomies, L. (2015). Internet of Things market develops fast but there are privacy concerns. *P.L. & B.U.K.N.*, *79*(May), 1,5-7.

Lundqvist, B. (2016). Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World. Faculty of Law, *University of Stockholm Research Paper No. 1*

Mar, E.Y., and Liaw, W. (2016). IP Law December Developments: What to Expect in the Future. *FBM* (28 December).

Miglani S., & Kumar, M. (2016). India's billion-member biometric database raises privacy fears. Retrieved at www.reuters.com/article/us-india-biometrics-idUSKCN0WI14E.

Ministry of Electronics & Information Technology (2015). Draft Policy on Internet of Things. Retrieved at https://mygov.in/sites/default/files/master_image/Revised-Draft-IoT-Policy-2.pdf

Ministry of Urban Development (2015), Smart cities. Statement and Guidelines.

Modi, N., Prime Minister Narendra Modi's speech on 68th Independence Day. Retrieved at http://indianexpress.com/article/india/india-news-india/pm-narendra-modis-speech-on-independence-day-2016-here-is-the-full-text/

Mohan, V. (2014). Ecologists cheer Modi's 'zero defect, zero effect' slogan. *The Times of India*. Retrieved at timesofindia.indiatimes.com/home/environment/developmental-issues/Ecologists-cheer-Modis-zero-defect-zero-effect-slogan/articleshow/40312809.cms.

Nightingale, A. (2016). More Rigorous Patent Examination in US Than Europe and Australia? *Intellectual Property Watch*, 2 November 2016.

Nivarra, L. (2011). La proprietà europea tra controriforma e "rivoluzione passiva". *Europa e diritto privato*, *13*(3), 575-624.

Noto La Diega, G. (2017). Software patents and the Internet of Things in Europe, the United States, and India. *European Intellectual Property Review*, *39*(3), 173-184.

Noto La Diega, G. (2016). 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 & Economic Regulation*, *9*(1), 69-93

Noto La Diega, G., and Walden, I. (2016). Contracting for the 'Internet of Things': Looking into the Nest. *European Journal of Law & Technology*, II, 1-38.

Office of the Controller General of Patents, Designs and Trade marks (2016). Guidelines for Examination of Computer Related Inventions (CRIs).

Office of Controller General of Patents, Designs and Trademarks (2013). Draft Guidelines for Examination of Computer Related Inventions, June 2013

Office of Controller General of Patents, Designs & Trademarks (2011). Manual of Patent Office Practice and Procedure, v. 1.11.

Roberts, J.J. (2016). Here's Why Software Patents Are in Peril After the Intellectual Ventures Ruling. Retrieved at http://fortune.com/2016/10/03/software-patents/.

Robinson, W.K. (2015). Patent Law Challenges for the Internet of Things. *Wake Forest J. Bus. & Intell. Prop. L.*, *15*(4) 655

Rose, K., Eldridge, S., Chapin, L. (2015). *An Overview Understanding the Issues and Challenges of a More Connected World* (Internet Society)

Sachs, R.R. (2015). Alice Haunted Federal Courts and USPTO in October. Retrieved at http://www.law360.com/articles/724855.

Trade Secrets Institute (2016). In the Matter of Certain Activity Tracking Devices, 337-963, U.S. International Trade Commission (Washington). Retrieved at http://tsi.brooklaw.edu/cases/matter-certain-activity-tracking-devices-337-963-us-international-trade-commission-washington.

Trappey, A.J.C., Trappey, C.V., Govindarajan, U.H., Chuang, A.C., Sun, J.J. (2016). A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0. *Advanced Engineering Informatics*

Weber, R.H. (2015). Internet of Things: privacy issues revisited. *C.L.S. Rev., 31*(5), 618-627.

Wong, J.I. (2016). One company has a big edge in the fight to dominate the Internet of Things. *QZ* (23 May).

Yeoh, P. (2017). The fourth industrial revolution: technological impact and privacy and data security issues. *Bus. L.R., 38*(1), 9-13.

Zingales, N. (2015). Of Coffee Pods, Videogames, and Missed Interoperability: Reflections for EU Governance of the Internet of Things. *TILEC Discussion Paper No. 2015-026.*

Cases law

Europe

Judgment of the Court (Second Chamber) of 8 September 2016. *GS Media BV v Sanoma Media Netherlands BV and Others*, C-160/15. EU:C:2016:644

EPO Boards of Appeal, T 1784/06 *Classification method/COMPTEL* of 21 September 2012, EP:BA:2012:T178406.20120921

EPO Boards of Appeal T 0531/09 *Checkpoint simulation/ACCENTURE* of 3 May 2012, EP:BA:2012:T053109.20120503

EPO Boards of Appeal, T 1265/09 *Call center/IEX* of 24 January 2012, EP:BA:2012:T126509.20120124

EPO Enlarged Boards of Appeal, G 3/08 Programs for computer of 12 May 2010, EP:BA:2010:G000308.20100512

EPO Boards of Appeal, T 1606/06 *DNS determination of telephone number/HEWLETT-PACKARD* of 17 July 2007, EP:BA:2007:T160606.20070717

EPO Boards of Appeal, T 1227/05 *Schaltkreissimulation I/Infineon Technologies* of 13 December 2006, EP:BA:2006:T122705.20061213

EPO Boards of Appeal, T 0424/03 *Clipboard formats I/MICROSOFT* of 23 February 2006, EP:BA:2006:T042403.20060223

EPO Boards of Appeal, T 0258/03 *Auction method/HITACHI* of 21 April 2004, EP:BA:2004:T025803.20040421

EPO Boards of Appeal, T 0125/01 *Gerätesteuerung/HENZE* of 11 December 2002, EP:BA:2002:T012501.20021211

EPO Boards of Appeal, T 0641/00 *Two identities/COMVIK* of 26 September 2002, EP:BA:2002:T064100.20020926

EPO Boards of Appeal, T 1173/97 *Computer program product/IBM* of 1 July 1998, EP:BA:1998:T117397.19980701

EPO Boards of Appeal, T 0190/94 of 26 October 1995, EP:BA:1995:T019094.19951026

EPO Boards of Appeal, T 0110/90 *Editable document form* of 15 April 1993, EP:BA:1993:T011090.19930415

EPO Boards of Appeal,T 0208/84 *Computer-related invention* of 15 July 1986, EP:BA:1986:T020884.19860715

EPO Boards of Appeal, T 0163/85 *Colour television signal* of 14 March 1989, EP:BA:1989:T016385.19890314

EPO Boards of Appeal, T 0026/86 *Röntgeneinrichtung* of 21 May 1987, EP:BA:1987:T002686.19870521

United States

Thales Visionix, Inc. v. United States, No. 2015-5150 (Fed. Circ. 2017)

Fitbit, Inc. v Aliphcom, et al., No. 15-cv-04073-EJD (N.D. Cal. 2017)

Amdocs (Israel) Ltd v Openet Telecom Inc, No. 2015-1180 (Fed. Circ. 2016).

Cisco Systems, Inc. v. Arista Networks, Inc., No. 5:14-cv-05344-BLF (NC) (N.D. Cal. 2016)

Fairwarning IP, LLC v. Iatric Sys, Inc., No. 15-1985 (Fed. Cir. 2016)

Synopsys v Mentor Graphics Corp, No. 2015-1599 (Fed. Cir. 2016)

Affinity Labs, LLC v. Amazon.Com Inc. et al, No. 6:2015cv00029 - Document 75 (W.D. Tex. 2016)

Intellectual Ventures I LLC v. Symantec Corp., No. 15-1769 (Fed. Cir. 2016)

Micro, Inc. v. Bandai Namco Games Am., Inc., No. 15-1080 (Fed. Cir. 2016)

Bascom Global Internet Services, Inc. v. AT&T Mobility LLC, No. 15-1763 (Fed. Cir. June 27, 2016)

ENFISH, LLC v. Microsoft Corp., 822 F. 3d 1327 - Court of Appeals, Federal Circuit 2016

Jawbone v Fitbit (2016) unpublished

Electric Power Group, LLC v. Alstom S.A., 830 F.3d 1350 (Fed. Cir. 2016)

Affinity Labs of Texas, LLC v. DIRECTV, LLC, 838 F.3d 1253 (Fed. Cir. 2016)

DDR Holdings, LLC v. Hotels.com, L.P., 773 F.3d 1245 (Fed. Cir. 2014)

Alice Corp. v. CLS Bank International, 573 U.S. __, 134 S. Ct. 2347 (2014)

Association for Molecular Pathology v Myriad Genetics, No. 12-398 (569 U.S. ___ June 13, 2013)

Accenture Global Servs. GmbH v Guidewire Software Inc 728 F.3d 1336 (Fed. Cir. 2013)

Mayo v Prometheus, 132 S. Ct. 1289 (2012)

Bilski v. Kappos, 561 U.S. 593 (2010)

Diamond v. Diehr, 450 U.S. 175 (1981)

Parker v Flook, 437 U. S. 584 (1978)

O'Reilly v Morse, 56 U.S. (15 How.) (1853)