IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 12 | Issue 1 | 2016

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY

BANGALORE

Subscription: INR (INR for students)

The mode of citation for this issue of The Indian Journal of Law and Technology 2016 is as follows:

– – – – – – – – – – – – – – –

Published by:

Student Bar Association
National Law School of India University
Nagarbhavi, Bangalore – 560072
Website: Email:

Distributed exclusively by:

Eastern Book Company
34, Lalbagh, Lucknow - 226 001
U.P., India
Website: www.ebc.co.in Email: sales@ebc-india.com

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

WWW.IJLT.IN

Volume 12 | Issue 1 | 2016

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 12 | Issue 1 | 2016

Contents

ARTICLES

Picket Patents: Non-Working as an IP Abuse
Dr. Feroz Ali 1

Technology Innovations in Securities Trading: Can SEBI's Bicycle Catch the High-Frequency Trading Ferrari
Armaan Patkar 24

The Internet of Citizens: A Lawyer's view on some Technological Developments in the United Kingdom and India
Guido Noto La Diega 53

BOOK REVIEW

The Politics of Pirates: Jonas Andersson Schwarz's "Online File Sharing"
Gautam Bhatia 105

Picket Patents: Non-Working as an IP Abuse

Dr. Feroz Ali[†]

Abstract: *Patents picket when the patent holder practices the patent in certain jurisdictions but refuses to work the patent in others. The concept of patent picketing developed as a result of a shift from the representation of the working of an invention physically to the merely describing, effectively, the inventions in patent applications. Patent holders picket with their patents and demand a higher price, thereby not only preventing others from using their invention but also ensuring that the product is not made available in all markets. Such behaviour can be regarded as an intellectual property (IP) abuse when the non-working of a patent leads to deprivation of another patent locally. The issuance of a market-initiated compulsory licence may solve the problems linked with IP abuse arising out of patent picketing.*

I. Introduction

The history of patent law notes the metamorphosis of the discipline that supported, though the ages, the nation's quest for self-development. In the early times, the chief aim of the patent system was to encourage industrialization. Patents were granted by nations to develop their natural resources and increase their technical and manufacturing capabilities.[1] In the medieval era, English patent law, the predecessor to the United States', granted privileges with the sole objective of "instructing the English in a new industry."[2] Immigrant weavers, clockmakers, miners, and manufacturers of silk and salt were encouraged to move to England and benefit from the Crown's power to grant privileges for public goods. However, early grant of privileges, in the form of monopoly licences, came with some restrictions. For

---

[†] MHRD IPR Chair Professor at the Indian Institute of Technology Madras, and Advocate, Madras High Court.

[1] Edith Tilton Penrose, The Economics of the International Patent System 137 (1951).

[2] E. Wyndham Hulme, *History of the Patent System Under the Prerogative and at Common Law*, 12 L. Q. Rev. 141, 142 (1896).

instance, a licence to manufacture white soap not only required the wares to be inspected by the municipal authorities to see if they were as good as those made in Spain, but was also accompanied by a threat of the privilege being rendered void on proof of defective manufacture.[3] In medieval England, there was great emphasis on working the privilege locally and affordably, as is evident from the licence granted to immigrant makers of ovens and furnaces that stipulated that the grant would be void if the patentees failed to practice the grant within two months or proved to be extortionate in their charges.[4] During these years, the grant of patent-like privileges was focused on rewarding creative labour embodied in the subject matter of the manufactured good.[5] Patent specification—the art of technically 'embodying' the invention in writing—was yet to appear on the scene.[6]

Things were, however, set to change soon. In the modern era, attention shifted away from the creative labour embodied in the manufactured product or process—the material embodiment—to concentrate more on the description of the creative labour in writing—the textual embodiment. Thus, as a consequence of the implementation of a registration system for patents, mental labour that produced the artifact was sidelined and prominence was given to paper inscriptions that the system produced.[7] By making the patent specification an end in itself, "registration radically changed the nature of the way the law dealt with intellectual property."[8]

Though the new registration system provided a stable reference point to ascertain the identity of the intangible, it also allowed patentees to secure exclusive rights by the mere demonstration of the invention in writing. This created a practice that focused exclusively on the ways in which documents were drafted, registered and interpreted.[9] Patentees enjoyed exclusivity by

---

3 *Id*. at 145.

4 Hulme, *supra* note 2, at 146. In 1565, a special mining licence granted to German miners by the Queen of England was challenged by the Earl of Northumberland on the ground that work was within the Royalties granted to his family in the earlier reign. The Earl lost the case on the ground of neglect of the Earl's family to work the minerals for seventy years. *Id*. at 147.

5 Hulme, *supra* note 2, at 145 (describing an early grant for the manufacture of saltpeter that required the "secrets of manufacture" to be reduced in writing before payment of the promised reward of £300).

6 Richard Miller et al., Terrell on the Law of Patents 9 (17th edn., 2011) (ascribing the emergence of modern specification in England to the Patent Law Amendment Act of 1852).

7 Brad Sherman & Lionel Bently, The Making of Modern Intellectual Property Law: The British Experience, 1760-1911, 181–82 (1999).

8 *Id*. at 182 (noting that the reduction of intellectual property to a paper inscription helped to overcome the difficulties of space and distance, i.e., those created by the size of buildings occupied by the Registry and those generated by the centralization of the Registers).

9 *Id*. at 186.

creating documents that complied with the administrative requirements set by the patent office. The harmonization of patent laws of different countries also consolidated the central role of specification.[10] The issue of manufacturing the artifact as it existed earlier and that of working the invention were gradually removed from the newly emerging confines of modern patent law.

The focus on patent specification led to some interesting consequences in the behaviour of patentees. In some cases, patentees could file specifications without any ability or intention to manufacture the product. By doing so, these non-practicing entities (NPEs) used patents as instruments to stop others from doing something which they never did or would do. Though the NPEs restricted others from working the invention, they did not pose an unsolvable problem. They filed infringement suits with the chief objective of seeking higher royalties.[11] The consequence of not working the invention was manageable as these suits were filed against entities that were practicing the artifact covered by the NPE's patent. Non-working of inventions, however, posed a greater problem when patents crossed borders.

Harmonization of patents laws, though modest in its impact, gave an impression that modern universal patent laws did not require patents to be worked locally. The patentees who benefited from harmonization could now secure exclusive rights through which they were free to practice in the countries of their choice. This allowed patentees to use their patents in protest. The practicing entity in one country, for instance the United States, could be a non-practicing entity in another country, thus allowing the patent holder to extract a higher rate of compensation in the country where the patent holder did not practice its patent by refusing to supply or allow others to produce, or by extracting licence terms that benefited its purposes, such as licences allowing production for domestic use and not for export. Patent holders could now picket with their patents, seeking a higher price: a conduct by which they could not only stop others from using their invention, but also, in contrast with the NPE situation, ensure that the invention was not at all available in a given market. The problem of patents that picket emerged as a new situation, where entities that practised their inventions in some jurisdictions refused to practice them in others.

---

[10] Harold C. Wegner, Patent Harmonization 23–24 (Sweet & Maxwell, 1993) (describing the creation of a worldwide procedural treaty, the Patent Cooperation Treaty of 1970 as an important tool for patent applicants as it allowed simultaneous filing of applications in multiple locations).

[11] *But cf.* Mark A. Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 Tex. L. Rev. 1991 (2006–2007) (reporting that existing patent remedies systematically result in excessive royalties).

Patent picketing is a problem that arises when patents are voluntarily not worked in some jurisdictions (mostly developing countries) while they are worked in others (mostly developed countries). Though picketing by patents is most commonly used in the pharmaceutical industry, there could be instances of picketing in other industries as well. The author shall limit the scope of this paper to only the pharmaceutical industry.

The impact of picketing, in the pharmaceutical industry, was felt when Bayer's patented drug, Nexavar, was not worked locally and consequently became the subject matter of a compulsory licence in 2012. Though the scholarship that emerged highlighted the significance and controversies involved in the issue of the compulsory licence,[12] it failed to note that the resulting response was as unique as the problem that evoked it.

When patents picket, countries have an option of issuing a market-initiated compulsory licence, as was done by India in issuing such a licence on Nexavar. Market-initiated compulsory licences are a distinct class of compulsory licences which can be issued at the request of a private party in the absence of a health emergency. Compulsory licences on patents have been regarded as a response to the abuse of a patent right, which amounts to an Intellectual Property (IP) abuse. Though the absence of local working (or non-working) of patents is historically treated as an abuse, it may be difficult to justify the local working in a global economy built on free trade, especially when the final word on international patent law, the TRIPS Agreement, is silent about it. Taking a cue from antitrust law, in part I of this article, I offer a rule-of-reason-like justification for treating the absence of local working as an abuse: not all patents are required to be worked locally but only those, the non-working of which leads to an abuse, i.e., where it leads to the deprivation of benefit locally. Part II of the article looks into the manner in which patent picketing leads to contempt of the patentee's obligation to work his invention, thereby resulting in a shift in focus from the material embodiment of the invention in the product to the textual embodiment of the invention in the specification. This part further discusses in detail the way in which the concept of local working has developed in different countries and the relevance of local working of a patented invention. Part III draws parallels to antitrust law to redefine picketing as an abuse of the patent system and advocating the issuance of compulsory licences by the affected country. The paper finally concludes with an analysis of the benefits of market-initiated compulsory licences as a means to end the abuse of patents due to picketing.

---

[12] *See, e.g.*, Betsy Vinolina Rajasingh, *India's First Compulsory Licence over Bayer's Patent*, JIPLP Blog (May 10, 2012), http://jiplp.blogspot.com/2012/05/indias-first-compulsory-licence-over.html?m=1.

II. Picket Patents: They Won't Work, They Won't Let Others Work

Like other Intellectual Property (IP) rights, patents attempt to balance its power of exclusive rights to stimulate the creation of inventions on the one hand and its tendency to curtail widespread public enjoyment of the inventions on the other.[13] This balancing act has affected the way in which a patent is perceived. Is it an absolute right that mysteriously ceases at the end of its term? Or is it a contingent right awaiting a challenge to its validity? Are there any accompanying obligations? Some of these pondering debates pertain to the rights and obligations conferred by a patent. Patents confer a bundle of rights which allow the patentee to exclude others from using, and to permit others to use by way of licence, its invention.[14] They also cast certain obligations on the patentee such as the obligation to make an enabling disclosure.

A. Patent as a Right

During the Elizabethan era, English patent law regarded the exclusive right of sale as the right subsequent to and derived from the sole right to manufacture.[15] The emphasis on manufacturing can be noticed from the inclusion of 'working clauses' in the grants, which required the patentee to practice the grant on the threat of revocation of the privilege.[16] Most of the early grants of privilege were in the form of manufacturing privileges, though there were few instances of privileges given for facilitating importation as well. The evolution of patent law in England shows that the exclusive right to use or stop others from using emerged from and was dependent on the exclusive right to manufacture. This understanding is, however, at variance with the contemporary exclusivity-centric understanding of patents.

Contemporary legal literature regards patent as a negative exclusionary right, a right that does not require the patentee to do anything but can nevertheless be effectively used to restrain others from doing things covered

---

[13] William Fisher, *Theories of Intellectual Property*, *in* New essays in the legal and political theory of property 168, 169 (Stephen R. Munzer ed., Cambridge University Press, 2001).

[14] Thomas C. Grey, *The Disintegration of Property*, *in* Property: Nomos XXII 69 (John W. Chapman & J. Roland Pennock eds., New York University Press, 1980) (describing patents as a bundle of rights).

[15] Hulme, *supra* note 2, at 153.

[16] Hulme, *supra* note 2, at 153 ("Apart from the frequent insertion of clauses regulating the period within which the new industry was to be introduced, it is obvious that prior to the rise of the patent specification a privilege became void owing to non-working within the reasonable period on the ground of want of consideration.").

by the patent.[17] By this characterization, a patentee is not required to work the patent at all: a patentee can, in fact, receive a patent for the prospect of working the invention in the future.[18] Whether or not the patentee works the invention commercially, manufactures or utilizes the technology covered by the patent is not a concern of patent law.[19] In short, there is no expectation that the invention be worked or practised, though there is a stress on the fact that the invention works.[20]

Patents confer the right to exclude others from making, using, offering for sale or selling the invention throughout the country, or importing the invention into the country.[21] They were considered as property rights due to the characterization of the patent as a right to exclude.[22] The right in a patent mimicked the right in real property in certain ways.[23] There were some benefits in this characterization; it immediately relieved the patentee from the responsibility of working the invention, a boon for technologies which have a long gestation period and for technologies like pharmaceuticals that require regulatory approval before marketing their products. However, there was some harm too. Entities could now patent technologies without any desire to practice or produce them and hold the real manufacturers for a ransom, a conduct that has earned these entities the title of 'non-practicing

---

[17] Robert P. Merges & John F. Duffy, Patent Law and Policy: Cases and Materials 48–49 (5th edn., 2011) ("Unlike other forms of property, however, a patent includes only the right to exclude and nothing else. Patents rights are wholly negative rights — rights to stop other from using — not positive rights to use the invention.").

[18] *But cf.* Edmund W. Kitch, *The Nature and Function Of The Patent System*, 20 J.L. & Econ. 265, 266–67 (1977) (propounding the "prospect theory", that patent system performs a hitherto unknown function of awarding exclusive and publicly recorded ownership of a prospect shortly after the discovery, and noticing the grant of many technologically important patents in America long before their commercial exploitation became possible).

[19] But the right to use an invention could become the concern of other laws. *See, e.g.*, *Whistler Corpn.* v. *Autotronics Inc.*, 1988 US Dist. LEXIS 17302, at 4 (observing that incongruity of asking a court of law through an infringement suit to protect a device (a radar detector) used to circumvent the law (of the states that banned the use of such devices).

[20] The 'working' of an invention refers to the fact that the invention is put to practice or made available to the public. This is different from the fact that the invention works. No patent would be granted for an invention that does not work. The requirement of enablement in patent law is one technique that requires the inventor to describe her invention clearly for a person skilled in the art to make and use it. *See* 35 U.S.C. § 112(1).

[21] *See, e.g.*, 35 U.S.C. § 154(a)(1).

[22] *But cf. Kaiser Aetna* v. *United States*, 62 L Ed 2d 332: 444 US 164, 176 (1979) (describing the right to exclude as "one of the most essential sticks in the bundle of rights that are commonly characterized as property").

[23] *But cf.* Gilbert H. Montague, *Proposed Patent Law Revision*, 26 Harv. L. Rev. 128, 133 (1912-1913) ("Owners of unimproved land cannot be compelled to improve their property, nor — except by eminent domain — to allow others to improve it. Similarly, the patent owner cannot be compelled to use his invention, nor — except by eminent domain — to allow others to use it.").

entities'.[24] The negative characterization also allowed entities to refuse to licence their technology to parties who needed it, as there was no obligation to permit that which came with the right to exclude.[25]

When characterized as an exclusive right to use, the patent exhibits two co-existing characteristics: it confers on the patentee not only the right to exclude but also the right to include others. The right to exclude gives the patentee the right to stop others from using its invention. The right to include allows the patentee to licence its invention to others who, by virtue of such permission, are protected from an infringement action. These two aspects of a patent right are not mutually exclusive as a patentee who grants an exclusive licence can still sue others for infringement.[26]

Sometimes the right or the privilege to use is characterized as a negative obligation. In general, the owner of an IP right does not have an obligation to use the right.[27] In the case of patents, this principle was established by the Supreme Court of United States when it referred to the right to exclude conferred by a patent as "the very essence of the right conferred by the patent, as it is the privilege of any owner of property to use or not to use it, without question of motive."[28] Concomitant with the absence of an obligation to use is the right to refuse to use or licence the patent.[29] The patentee's right to refuse to use implies its right to refuse licence to others. However, it need

---

[24] *See, e.g.*, Patent Quality Improvement: Hearings Before the Subcomm. on Courts, the Internet and Intellectual Property of the House Comm. on the Judiciary, 198th Cong. 21 (2003) (testimony of David Simon, Chief Patent Counsel, Intel Corporation) (coining the term 'patent trolls' for non-practicing entities and describing their practices).

[25] *See, e.g.*, In re, Independent Service Organizations Antitrust Litigation, 203 F 3d 1322, 1328 (Fed Cir 2000) (holding that a refusal to licence would not amount to exclusionary conduct in the absence of "any indication of illegal tying, fraud in the Patent and Trademark Office, or sham litigation, the patent holder may enforce the statutory right to exclude others from making, using, or selling the claimed invention free from liability under the antitrust laws.").

[26] *But cf.* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv. L. Rev. 1089, 1092 (1971–1972) ("An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agree upon by the seller.").

[27] Herbert Hovenkamp et al., *Unilateral Refusals to Licence*, 2 J. Competition L. & Econ.1, 2–3 (2006).

[28] *Continental Paper Bag Co.* v. *Eastern Paper Bag Co.*, 52 L Ed 1122: 210 US 405, 429 (1908). Eastern owned a patent for a machine for making self-opening square paper bags which it never used or licensed to others. Eastern sued Continental for patent infringement. Continental raised a plea that it would be inequitable to enforce a patent as Easter was not using the patented machine and was using the patent to suppress competition. The district court found that Continental infringed the patent, the Court of Appeals, First Circuit and the Supreme Court affirmed the decision.

[29] 35 U.S.C. § 271(d)(4) (stating that a patent owner cannot be deemed guilty of misuse by virtue of its refusal to licence or use any rights to the patent). Though this provision refers

not necessarily imply that the patentee's right to enforce is independent of its right to use.[30] Despite the stress on the characterization of the patent as a *right*, modern patent statutes cast some requirements on the patentee that view the patent as an *obligation*.

One such obligation is the duty to disclose information to the patent office, which if the applicant violates through bad faith or intentional misconduct, can jeopardize the grant of a patent on the application.[31] Courts regard the obligation to disclose information, which in some cases is imposed judicially, as one of the conditions for enforcing the issued patent.[32] The right to exclude, which materializes upon the grant of a patent is, thus, dependent on the obligation to disclose.[33]

B. Patent as an Obligation

Patent law has historically imposed an obligation on the patent holder to practice the patent. Patents evolved as rights with a strong component on working, a positive act that the patentee did to put his invention to practice within a specified time.[34] In the early days, patent-like privileges were tied to manufacture and were focused on bringing foreign technology to local markets.[35] Patentees were required to compulsorily work the invention as such privileges would become void if not worked within the stipulated time, on the ground of want of consideration.[36] Since most countries held the view that patents were granted in order to promote technical progress and as an indemnity to the inventor for making the invention public, they perceived

---

to patent misuse and not directly to antitrust violations, the policy it expresses remains relevant in antitrust law. *See* Hovenkamp et al., *supra* note 27, at 3.

30 In some cases the right of the patentee to injunctive relief is dependent on the use of the invention. *See, e.g.*, *Foster* v. *American Machine & Foundry Co.*, 492 F 2d 1317 (2nd Cir 1974) (where the court refused to grant permanent injunctive relief to the patentee which did not practice the invention either directly or through licensees).

31 37 C.F.R. § 1.56(a) & (b); Patents depart from other forms of intellectual property in its disclosure obligations. While copyright (protection of unpublished works) and trade secret laws condone non-use and non-disclosure of the rights, patent laws confines its scope of protection to nonuse alone. *See* Hovenkamp et al., *supra* note 27, at 3.

32 Merges & Duffy, *supra* note 17, at 1111.

33 *J.E.M. Ag Supply Inc.* v. *Pioneer Hi-Bred International Inc.*, 51 L Ed 2d 508: 534 US 124, 142 (2001) ("The disclosure required by the Patent Act is the *quid pro quo* of the right to exclude.").

34 Penrose, *supra* note 1, at 2–3 (noting the practices in 15th and 16th century Europe that made working the invention an important consideration for the grant of a special privilege).

35 *See, e.g.*, Statute of Monopolies, 1623, 21 Jac.1, c.3, § 6 (Eng.). The Statute of Monopolies is regarded as the 'direct ancestor' of the United States patent law. Penrose, *supra* note 1, at 43.

36 Hulme, *supra* note 2, at 154.

that this aim would not be achieved if the patentee was allowed to prevent others from exploiting the invention without being, simultaneously, put under an obligation to make the invention available to the public through his own efforts.[37] Until the early 20th century, countries were almost unanimous in requiring patents to be compulsorily worked within a specified time.[38] One of the early commentators of the Paris Convention emphasized the importance of local working by holding the view that the member states were free to define what they understood by 'failure to work'.[39]

This unanimity diminished gradually as countries scaled the ladder of development. Opposition to the compulsory working requirement came in the latter part of the 19th century, when countries like Belgium, Great Britain, Russia, Turkey, Italy and the United States insisted that working in one country, the country of origin, should suffice as working in all the others.[40] Developed countries, the ones where patents were more likely to be filed and practiced, relaxed the compulsory working requirement as most of the patents were aimed at the markets in those countries. Moreover, by making similar arrangements among other developed countries, the requirement for working diminished as, given the purchasing power of the consumers in these countries, the invention would be practiced anyway to be commercially viable. In keeping with the times, scholars soon developed a dislike for local working and regarded the requirement of local working as redundant and discriminatory.[41] Non-working, thus, was not a problem which the developed countries perceived. This was because they were the markets for the new inventions and there was very little possibility of the inventions not being worked or practised in those countries.[42]

---

[37] Jan Vojáček, A Survey of the Principal National Patent Systems 59 (Prentice-Hall 1936).

[38] Penrose, *supra* note 1, at 137.

[39] G.H.C. Bodenhausen, Guide to the Application of the Paris Convention for the Protection of Industrial Property, as Revised at Stockholm in 1967, 71 (World Intellectual Property Organization 1968).

[40] Penrose, *supra* note 1, at 79–81.

[41] The discussions on non-working, though relevant in history, did not have a place in modern times. The early works on international patent law devoted a few pages of commentary on non-working or the absence of local working. *See, e.g.*, Vojáček, *supra* note 37, at 59–63. As times changed, the newer works did not have any discussion on non-working of patents. Scholars proclaimed that there is no place for compulsory licensing or working in a conservative understanding of intellectual property laws. *See, e.g.*, Hovenkamp et al., *supra* note 27, at 4.

[42] *But cf.* Ashish Arora et al., Markets for Technology : The Economics of Innovation and Corporate Strategy 200 (MIT Press 2001) (countering the prevailing thought that integration of countries increase growth as the fixed cost of producing ideas spread over a larger market and observing that integration, though beneficial to the follower countries, does not increase the number of Specialized Engineering Firms (SEFs) in the First World, as most of the SEFs which arose to serve the First World market remain

This change is also attributed to the manner in which patent law developed. History witnessed a shift from the material embodiment of the invention in the product—the fact that the invention worked when practiced—to the textual embodiment of the invention in the specification—the fact that the invention worked as disclosed. Thus, around the 18th century, the obligation to work the invention was replaced by the obligation to disclose the invention, as both had in common the object of "making the new art known and training others in the practice of it."[43] Spectacularly, the obligation to disclose relieved the burden of putting the invention to practice from the patentee as he was only required to disclose the invention in a manner that enabled a skilled person to make and use the invention. This move was accentuated by the understanding that not all patents are granted for the introduction of new industries.[44] As the doctrine of enabling disclosure evolved, the requirement of working the invention increasingly became confined to what the patentee said in the specification and what the skilled person could do with it.[45]

The story unfolded in a different way in developing countries. These countries saw local working as a means to promote technical progress that assisted them in capacity building and insisted, in their patent laws, for the requirement of local working. Scholarship, too, recognized the importance of local production and manufacture.[46] These countries hoped that by granting patent protection the technology covered by the patent would be made available locally.[47] These countries geared their patent laws to make an allowance for working the technology locally; some of them made the grant of a patent upon the condition of working them locally.[48] Some countries even imposed an obligation one very patentee with the responsibility of filing working statements annually indicating whether the inventions were

---

faithful to history and as their investments were not motivated by the hope of serving developing country markets that did not yet exist).

43 Penrose, *supra* note 1, at 138.

44 E. Wyndham Hulme, *On the Consideration of the Patent Grant Past and Present*, 13 L. Q. Rev. 314, 317–18 (1897) (noting that the doctrine of instruction of the public by means of the personal efforts of the patentee was finally abandoned in favour of the novel theory that this function belonged to the patent specification).

45 Merges & Duffy, *supra* note 17, at 265 (noting that the enablement requirement requires the inventor to describe her invention clearly enough so that one skilled in her art can understand it well enough to make and use it).

46 *See, e.g.*, U.N. Conf. on Trade & Dev., Investment in Pharmaceutical Production in the Least Developed Countries: A Guide for Policymakers and Investment Promoting Agencies, http://unctad.org/en/docs/diaepcb2011d5_en.pdf [hereinafter Pharmaceutical Production](describing the impact of local production of pharmaceuticals in Least Developed Countries).

47 Vojáček, *supra* note 37, at 59.

48 *See* The Patents Act, No. 39, § 83(a) (India).

being worked locally.[49] The emphasis on working took stronger ground as developing countries saw a peculiar problem which did not happen in the developed countries, especially in the case of pharmaceutical patents.[50] Some of the pharmaceutical patents were not worked locally and they were not made available to the local market at an affordable price given the disparities in the purchasing power of the masses compared to their counterparts in developed countries.[51] Consequently, these developing countries had to deal with the problems that arise when patents picket.

C. When Patents Picket

Patents picket when they are not worked locally. These patents are not worked locally on a commercial scale and because of their exclusionary nature, others are not allowed to work the invention covered by the patent.[52] By doing so, these patents picket.[53] In other words, patents picket when they do not work at all or are worked insufficiently. Like a labour strike which involves a concerted stoppage of work for an enhancement of wage, picketing patents too result in a stoppage of working of the patent in expectation of a monopoly price. Sometimes the price set by the patentee is too high for most of the population to afford, as it often happens in the case of patented pharmaceutical drugs sold in developing countries where only a small percent of the population can afford the drug.

What amounts to working is not clearly defined in any of the international conventions on patents.[54] Scholars, however, are in agreement that this gives the countries room to define what working means.[55] The term has

---

[49] *Id.* § 146.

[50] Of all fields of technologies, patents play the most significant role in the pharmaceutical industry. *See,* James Bessen & Michael James Meurer, Patent Failure : How Judges, Bureaucrats, and Lawyers Put Innovators at Risk 14, 89 (Princeton University Press 2008).

[51] *But cf.* Patricia M. Danzon, *The Economics of Parallel Trade*, 13 PharmacoEconomics 293 (1998) (suggesting that exempting on-patent products from parallel trade could preserve price differentials for pharmaceutical products).

[52] *See, e.g.*, Khomba Singh, *No interim stay on Cipla's Nexavar clone*, Econ. Times, Mar. 1, 2009, http://articles.economictimes.indiatimes.com/2010-03-01/news/28487477_1_nexavar-patent-linkage-prathiba-singh (describing Bayer's infringement suit against Cipla, a company that was manufacturing generic version of Bayer's patented drug, Nexavar).

[53] A picket refers to a person, either on strike or supporting that strike, who seeks to prevent other persons from gaining access to a place of work during the course of an industrial dispute. *Picket Definition*, credoreference.com, http://www.credoreference.com/entry/collinsecon/picket (last visited Feb. 14, 2013).

[54] *But cf.* Penrose, *supra* note 1, at 3 (referring to the phrase "working a patent" as an unfortunate piece of technical jargon which meant "producing with the use of the patented invention").

[55] Bodenhausen, *supra* note 39, at 71.

been interpreted "to mean working it industrially, namely, by manufacturing the patented product or industrial application of a patented process" while excluding importation or sale of the patented article or of the article manufactured by a patented process.[56]

A peek into history shows that the compulsory working requirement was an integral part of patent law in the United States, the United Kingdom and many other countries.[57] The reason for its absence from the modern patent system can be explained by the economic conditions prevalent today in these nations. Patent laws were intricately linked to the stage of development of a country and every time there was an issue related to development, patent law was flexed to suit the local developmental needs.[58] Scholars have noted that there was little that has been said either for or against the patent system in the 20th century that has not been said in the 19th century.[59] Both United States and United Kingdom have gone through cycles where they had to adjust the terms of IP protection to suit their stage of economic development.[60]

Local working or failure to work in the local market is one of the original grounds on which compulsory licences were granted.[61] The premise was that a compulsory licence could be granted if the patent holder did not manufacture the patented invention locally. Patents evolved historically with the expectation that the patent holder would make the patented invention locally.[62] Countries held a view that apart from being beneficial to the industry,

---

[56] *Id.*

[57] Penrose, *supra* note 1, at 137–43 (noting that the United States was the first country to remove this requirement from its laws).

[58] *See, e.g.*, B. Zorina Khan, The democratization of invention: patents and copyrights in American economic development, 1790-1920 289 (2005) (noting that the intellectual property institutions stimulated early American economic growth because of their flexible responses to economic and social circumstances).

[59] *See* Fritz Machlup & Edith Penrose, *The Patent Controversy in the Nineteenth Century*, 10 J. Econ. Hist. 1, 10, 28 (1950).

[60] *See, e.g.* Christopher May & Susan K. Sell, Intellectual Property Rights 109 (Boulder, Colo., Lynne Rienners Publishers, 2006) ("The diversity of intellectual property policies between countries was, and remains, in part a function of their different stages of development."). The 19th century also saw the House of Lords passing a bill for "a reduction of patent protection to seven years, strictest examination of patent applications, forfeit of patents not worked after two years, and compulsory licensing of all patents." Machlup & Penrose, *supra* note 59, at 4. In the United Kingdom, the working of a patent was introduced by the Patent Law Amendment Act of 1902, which compelled people to work, or to allow others to work, their patents, instead of allowing them to use the patent to stop others from working it. *See* Thomas Henry O'Dell, Inventions and Official Secrecy: A History of Secret Patents in the United Kingdom 66 (1994).

[61] *See* Penrose, *supra* note 1, at 78.

[62] *See* Paul Champ & Amir Attaran, *Patent Rights and Local Working under WTO TRIPS Agreement: An Analysis of the U.S.-Brazil Patent Dispute*, 27 Yale J. Int'l L. 365, 370–71 (2002).

"patents should also be *used for working the patented invention in the country where the patent is granted*, and not merely as an exclusive right to prevent others from doing so or to control importation."[63] Failure to work the patented invention, which included insufficient working, was regarded as an abuse which could not be alleviated by importation.[64] The echoes of local working from the past can still be heard today.[65] In the modern context, the TRIPS Agreement allows Member States to take appropriate measures to prevent the abuse of intellectual property rights by right holders.[66] It implicitly recognizes the right of the Member States to define abuse of Intellectual Property rights.[67] In modern economies, the governments decide the rules of the game as they define fair competition, anticompetitive conduct and other behaviour that amounts to an abuse.[68] Thus, the provision of local working in the domestic patent law may not be in contravention of the TRIPS Agreement.[69]

What could be the relevance of local working in a global economy? Local working is tied to the concept of local manufacture and local production. It is expected to bring in the benefit of 'learning by doing' to the domestic market and thereby result in the transfer of technology.[70] Local working of

---

[63] Bodenhausen, *supra* note 39, at 70 (emphasis in original).

[64] Bodenhausen, *supra* note 39,at 71; *See also,* Cynthia M. Ho, Access to Medicine in the Global Economy: International Agreements on Patents and Related Rights 131 (2011).

[65] When Indonesia threatened originator pharmaceutical companies with compulsory licence, it also indicated that it would expel those companies from the market unless they were willing to invest in local production of pharmaceuticals. *See* Sinfah Tunsarawuth, *Indonesia Mulls Compulsory Licences On Three More HIV/AIDS Drugs*, Intell. Prop. Watch, Nov. 26, 2007, http://www.ip-watch.org/2007/11/26/indonesia-mulls-compulsory-licences-on-three-more-hivaids-drugs/. Brazil was taken to the WTO for making local working a requirement under their law. India had provisions for local working built into its law which required submission of timely information to the patent office on whether the invention was being worked. *See generally* Champ & Attaran, *supra* note 62, at 365.

[66] *See* Agreement on Trade-Related Aspects of Intellectual Property Rights, Marrakesh Agreement Establishing the World Trade Organization, art. 8(2), Apr. 15, 1994, Annex 1C, 33 I.L.M. 1197 (1994) (hereinafter TRIPS Agreement),

[67] *See* Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, as last revised at Stockholm, July 14, 1967, 25 Stat. 1372, 828 U.N.T.S. 305 (hereinafter Paris Convention).The TRIPS Agreement states that the provision of the Paris Convention shall be complied with by the member states implying that the Paris Convention is to be read as a part of TRIPS Agreement. *Id.* Art. 2(1); Article 5(A)(2) of the Paris Convention states that each member shall have the right to take legislative measures providing for the grant of compulsory licences in order to prevent any abuse of patent rights, such as failure to work.

[68] Joseph E. Stiglitz, The Price of Inequality 30 (New York, W.W. Norton & Co. 1st edn., 2012).

[69] Michael Halewood, *Regulating Patent Holders: Local Working Requirements and Compulsory Licences at International Law*, 35 Osgoode Hall L. J. 244, 260 (1997).

[70] *But cf.* Gabriel Szulanski, *The Process of Knowledge Transfer: A Diachronic Analysis of Stickiness*, 82(1) Org. Behav. & Hum. Decision Processes 12 (2000) (acknowledging

patents is an important cog in developing capacity, as capacity building is seen as the long-term solution by developing countries for the problem of access to affordable medicines and in handling health crises where drugs are needed in large quantities.[71] While local working could result in the availability of higher quantities in the local market, it does not necessarily translate into cheaper prices, especially for patented drugs.

There appears to be no consensus on whether local production will have an effect on the local availability of the drug. Patent holders on the one hand hold that local production need not necessarily mean that the drug is made available in sufficient quantity for local consumption, as the demand of the market is subject to various conditions. Given that pharmaceutical companies are in the businesses of efficient production, a patent holder can be expected to only make available such quantities that the local market can afford.[72] Since patented drugs would be covered by monopoly prices, the number of individuals who can afford them in a developing country will be few in number. As a result, importation of the invention would suffice to meet the small demand. Developing countries on the other hand, which insist on local working, cite the transfer of technology, availability of drug in large quantities, and developing local capacity for manufacturing in times of crises as the significant reasons for their insistence.[73] That local working could have an impact on the pricing of the drug is a matter which both the patent holders who charge monopoly prices and prefer importation and the developing countries which have the regulatory authority to control prices of drugs tend to ignore.[74]

---

that learning by doing entails resolution of unexpected problems that arise when new knowledge is put to use by the recipient in an intra-firm context).

[71] Frederick M. Abbott, WTOTRIPS Agreement and Its Implications for Access to Medicines in Developing Countries 13-14 (2000) [hereinafter, Abbott, Access to Medicines] (U.K. Commission on Intellectual Property Rights (CIRP) Study Paper 2a), *available at* http://www.iprcommission.org/papers/pdfs/study_papers/sp2a_abbott_study.pdf.

[72] *See Natco Pharma Ltd.* v. *Bayer Corpn.*, CLA No. 1 of 2011, 9-3-2012(Controller of Patents, Mumbai), 38-39, [hereinafter Nexavar licence] available at http://www.ipindia.nic.in/ipoNew/compulsory_ License_12032012.pdf (India.) (citing Bayer's argument that the quantities required in India do not economically justify setting up a manufacturing facility in India).

[73] *See, e.g.*, The Patents Act, 1970, No. 39, § 83 (India) (detailing the reasons for the grant of compulsory licences).

[74] Not many countries have linked the local working requirement to the issue of compulsory licences. India, for one, has a provision in the patent law which calls for revocation of patents that are not worked. *See id.* § 85.

The relationship between local working and the price of the drug has not been explored in detail.[75] Patentees could argue that since the prices are high, only few units need to be made available to the local market based on the ability to afford. The contrary argument would be that it is the high price that makes the drug unaffordable to much of the population in the developing country though they have a need for it. Though the patents create monopolies, there appears to be no effective way of eliminating the associated deadweight loss.[76]

The question that, then, arises is that why drugs are not differentially priced in the developing countries? There are at least four theories that explain why companies do not practice differential pricing: the first theory states that since patents grant monopoly control over prices there is no incentive to price-discriminate in the absence of any competition; the second theory postulates that pharmaceutical companies do not practice differential pricing due to the fear of reference pricing, the apprehension that prices marked in developing countries could be used as benchmarks in developed countries; the third theory looks at the profitability of selling medicines and holds that selling medicines at high prices to the rich in the developing countries is more profitable than selling at lower prices to the masses;[77] and the fourth theory offers a defense against parallel importation, the practice of low-priced medicines eating into the market of higher priced medicines when they are imported into developed countries.[78] These theories indicate that the concept of price is intricately tied to the availability of the drug in the local market. The availability of the drug, both in times of normalcy and crisis, is dependent on the capacity of local production, which in turn is dependent on the local working for a patented drug.

---

[75] Few studies exist on the effect of local production on access to drugs. *See, e.g.*, Pharmaceutical Production, *supra* note 46.

[76] Pankaj Tandon, *Optimal Patents with Compulsory Licensing*, 90 J. Pol. Econ. 470, 470-71 (1982) (suggesting compulsory licences as a way to reduce deadweight loss).

[77] In the primary market of pharmaceutical companies, the United States, of the 12 drugs approved by the Food and Drug Administration, 11 were priced above $100,000 per patient per year. *See The Real Cancer Killer: Rip-off Prices for Drugs Set by "Profiteering" Big Pharma Giants*, The Independent, Apr. 29, 2013, http://www.independent.co.uk/news/uk/home-news/the-real-cancer-killer-ripoff-prices-for-drugs-set-by-profiteering-big-pharma-giants-8591825.html.

[78] Frederick M. Abbott & Jerome H. Reichman, *The Doha Round's Public Health Legacy: Strategies for the Production and Diffusion of Patented Medicines Under the Amended TRIPS Provisions*, 10 J. Int'. Econ. L. 921, 971(2007) [hereinafter Abbott & Reichman, Doha Round's Legacy].

Countries have addressed the issue of non-working of both home-grown and foreign patents with their compulsory licensing regimes.[79] Compulsory licences are liability rule entitlements where the state sets the rates of compensation to be paid to the patent holder based on the submissions of the parties.[80] Countries have addressed this not just by their compulsory licensing regimes but also by having an effective working requirement built into their patent laws.[81] Though the compulsory licensing regime relieved the patentee from the danger of forfeiture of its patent, it did create an obligation to work the invention locally.

III. Redefining Non-working as Abuse

Improper exploitation of patents falls into two categories. A patent may be improperly exploited by, first, violating the antitrust laws or, second, extending the patent beyond its lawful scope.[82] The doctrine of patent abuse or misuse refers to an equitable concept designed to prevent a patent owner from using the patent in a manner contrary to public policy. The doctrine applies to practices by the patentee which appears to extend its patent grant beyond its statutory limits.[83] The doctrine of patent misuse was first expounded by the Supreme Court of United States in the *Morton Salt* case.[84] Since patent misuse is traditionally defined as an enforcement of a non-statutory patent right i.e., a right which is not conferred on the patentee by the grant of the patent, the demarcation of the limits of the statutory right conferred by a patent can have a bearing on determining and defining patent misuse.

---

[79] Penrose, *supra* note 1, at 162–87 (making a separate case for compulsory licensing of foreign patents).

[80] *But cf.* Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 Cal L. Rev. 1293, 1296 (1996).

[81] For instance, in India, a patent is granted subject to certain condition, one of which is an expectation that the patent would be worked; The Patents Act, 1970, No. 39, § 83(a) (India).

[82] *See* 6 Donald Chisum, Patents §19.04[1] (1990). *See also* Dan L. Burke & Mark A. Lemley, *Policy Levers in Patent Law*, 89 Va. L. Rev. 1575, 1662-63 (2003).

[83] *See* Burke & Lemley at 1664 ("More generally, the courts could use patent misuse to enforce a conception of the proper scope of a patent in a given industry in the face of efforts by patentees in different industries to change that scope."). *See USM Corpn.* v. *SPS Technologies Inc.*, 694 F 2d 505 (7th Cir 1982).The instances of misuse include resale price maintenance (fixing the price at which the purchaser of the patented item could resell it).

[84] *Morton Salt Co.* v. *G.S. Suppiger Co.*, 86 L Ed 363: 314 US 488 (1942). The case involved the patentee making use of its patent monopoly to restrain competition in the marketing of unpatented articles, the salt tablets, for use with their patented machines. The trial court, without getting into the merits of validity and infringement, summarily dismissed the complaint for infringement. On appeal by the patentee, the Court of Appeals reversed the decision. The Supreme Court found the conduct of the patentee as one amounting to a patent misuse.

Traditionally, abuse of patent meant more than just the failure to work.[85] Non-availability and non-affordability of a patented drug in the local market were instances of abuse as well. Since these two grounds have traditionally been regarded as public interest grounds, and more importantly are not the chief grounds for initiating a market-initiated compulsory licence, the relevance of these two grounds is not discussed here. In contrast, the ground of non-working has been more contentious and its affiliation to abuse of patent right has been controversial. The following discussion is confined to an analysis of non-working as an abuse of patent right.

A. Compulsory Working and Compulsory Licensing

Historically, abuse of patents has been addressed by two broad approaches: (1) by compulsory working and (2) by compulsory licensing.[86] Compulsory working of patents had its origin in the belief that foreign patents would protect the market for their exports by retarding domestic industrial development.[87] Compulsory working came with a strong penalty: failure to use the invention in countries that had compulsory working requirement led to its forfeiture.[88] Some countries who had strong export potential saw these provisions as harsh and bargained for restricting the compulsory working requirement to the country of origin, i.e., they introduced the principle that working in one country can be regarded as working in others.[89] Other countries continued to retain compulsory working in their laws. In the Madrid Conference of 1890, the compromise that was suggested was that compulsory licensing should be substituted for compulsory working as a way to reconcile the conflicting interests.[90] Thus, compulsory licensing emerged as an alternative to compulsory working.[91] While non-working would have

---

[85] When the concept of abuse was first introduced in United Kingdom, it encompassed 6 types of abuses, namely,(1) failure to work, (2) prevention of production in Britain by importation, (3) failure to meet the demand to an adequate extent on reasonable terms, (4) refusal to grant licences on reasonable terms to the prejudice of trade or industry in the United Kingdom when it is in the public interest that a licence be granted, (5) the imposition of conditions on sales, leases or licences which are prejudicial to trade or industry, and (6) the use of a patent which covers a process involving the use of unpatented materials in order to control the materials in such a way as unfairly to prejudice their manufacture, use or sale in the United Kingdom. Penrose, *supra* note 1, at 178-79.

[86] Paris Convention, Arts. 5(A)(2) and (3); *See also* Penrose, *supra* note 1, at 78.

[87] Penrose, *supra* note 1, at 137.

[88] Penrose, *supra* note 1, at 137.

[89] Penrose, *supra* note 1, at 79-81.

[90] Penrose, *supra* note 1, at 81.

[91] Vojáček, *supra* note 37, at 60. ("The best method seems to be to put an obligation on the patentee to grant licences on reasonable terms, and to reserve the penalty of forfeiture of patent only for cases of flagrant misuse of the monopoly rights, particularly wilful neglect or fraudulent dealing.").

resulted in forfeiture of the invention in a regime that mandated compulsory working, the option of compulsory licensing saved the patentee from the danger of forfeiture of his patent. Local working as it exists in modern legislations is different in this sense from the compulsory working requirement. Local working is mostly used as a trigger for initiating a compulsory licence rather than as a tool for forfeiture.

Thus, it is not difficult to justify local working in modern patent legislations. First, they are used as a trigger, the absence of which can lead to the issue of a compulsory licence. Second, if the working requirement is inbuilt into the patent law such that the patentee is required to furnish working statements to the patent office or if the patent law requires all inventions to be worked locally, the provision by itself may not be regarded as harsh and unfair.

When the compulsory working requirement was relaxed, countries began to argue that importation of the invention should suffice as working. The concept of working encompasses two things: use of the patent by the patentee and licensing of the patent to a third party. Whether importation of a drug would amount to working or not remains unsettled.

B. Importation as Working

One of the most serious objections that have been raised against the concept of working is that importation amounts to working.[92] As noticed, Bayer's contention that importation satisfies the requirements of working was rejected by the Controller.[93] In doing so, the Controller relied on Section 83(c) of the Patents Act, a provision which explicitly states that importation would not satisfy the requirements of working.[94] The Controller drew an analogy between working by the compulsory licensee and working by the patentee. Section 90(3) provides that no licence granted by the Controller shall authorize the licensee to import the patented article from abroad. By citing this provision, the Controller concluded that what is good for the compulsory licensee holds good for the patentee. This interpretation has

---

[92] The confusion on the issue of importation is justifiable. Article 5(A)(1) of the Paris Convention provided the importation of patented articles by the patentee shall not entail forfeiture of the patent. This was done to move on-working patents from the greater threat of revocation to the lesser threat of non-voluntary licence. Jerome H. Reichman & Catherine Hazenzahl, ICTSD-UNCTAD Project on IPRs & Sust. Dev., Non-Voluntary Licensing of Patented Inventions 10 (2003). The TRIPS Agreement is however silent over this issue.

[93] *Nexavar licence*, *supra* note 72, at 39. However, the IPAB reversed this finding to hold that in some cases importation can amount to working provided the same is proved.

[94] *Nexavar licence*, *supra* note 72, at 43.

been criticized for equating the rights of the patentee with that of a licensee.[95] The key to the puzzle lies in Form 27 of the Indian Patent Rules, which are statements of working that patentees are required to file annually at the Indian Patent Office. Those critical of the working requirement have argued that if importation did not amount to working, there would have been no need to mention importation under the heading of 'working the invention' in Form 27.[96] Since importation is regarded as one of the elements of working, the critics conclude that importation alone would satisfy the working requirement. What they overlook is the fact that Form 27 mentions importation conjointly with local manufacture. Keeping in line with the statutory mandate in Section 83(c) that importation does not amount to working of the invention, a more reasonable reading of Form 27 would be to regard importation as a relevant factor when the drug is locally manufactured. In such cases, importation could show the extent to which the drug is made available in the market, either by manufacturing or by import.

C. Economic Efficiency of Local Working

Some of the objections for local working come from the fact that it is often economically inefficient.[97] Local working, it is argued, would prevent a patentee from choosing to exploit only one of the many lines of its products it has developed much to the detriment of specialization. There is also the question as to who will determine whether the patentee is satisfying the working requirement.[98] Some hold a view that it is "physically impossible and economically absurd" for a patentee to work his patent in every country or even in most of the industrial countries of the world.[99]

Much ink has flown from the pens of scholars arguing for and against local working.[100] But local working is not the only reason for the grant of the licence though it may be touted as the most vociferous of the grounds. As mentioned earlier, market-initiated compulsory licences become indefeasible when granted on multiple grounds combining local working grounds with public interest grounds. Thus, even if non-working were to amount to

---

[95] Ritushka Negi & Vineet Rohilla, *Compulsory licensing: Is the working requirement legitimate?*, Managing Intell. Prop. (2012), http://www.managingip.com/Article/3084083/Compulsory-licensing-Is-the-working-requirement-legitimate.html.

[96] The Patents Rules, 2003, Form 27, Gazette of India, part II section III(2) (May 2, 2003).

[97] Penrose, *supra* note 1, at 156–58.

[98] Hovenkamp et al., *supra* note 27, at 7. In India, that question is answered by the working statement which patentees are required to file every year. Feroz Ali Khader, The Law of Patents: With a Special Focus on Pharmaceuticals in India 319 (2007).

[99] Penrose, *supra* note 1, at 158.

[100] Ho, *supra* note 64, at 131 (discussing the diverging views of scholars on the permissibility of local working).

discrimination under Article 27 of the TRIPS Agreement, it would not be a ground to cancel a compulsory licence if it is also granted, as would most likely be the case, on the grounds of public interest. Further, the non-discrimination clause appears to affirm the patent owner's rights to enjoy the patent to the exclusion of others and is silent as to whether it suggests that the patent owner would lose his right to exclude others if he failed to make the product locally.[101] Here again, by the grant of a compulsory licence, the patent owner's right to exclude others remains largely intact except for the compulsory licensee who alone would be able to make the product now.[102] Hence, there would not be a total taking away of the right to exclude either. Since TRIPS is built upon the foundation of the Paris Convention, it could throw some light on how the provision is to be interpreted.[103] The Convention expressly considers lack of local working as an abuse of patent right that is a ground for the issuance of compulsory licensing.[104] Since there is no clear indication in the TRIPS Agreement on repealing local working, the default position that was carried over from the Paris Convention should continue.

It is true that local working may not work for all countries.[105] Increasing the local production of pharmaceuticals by developing countries may not reflect a wise use of available scarce resources except for a few developing countries which possess a comparative advantage in this field.[106] India is one country which has a comparative advantage in the development of cheap and cost-effective drugs. But recent evidence shows that local production could benefit the developing countries, more particularly, the LDCs.[107]

---

[101] Ho, *supra* note 64, at 132.

[102] *Nexavar licence*, *supra* note 72, at 62 (stating that the residual rights of the patentee remain intact).

[103] Bryan Mercurrio & Mitali Tyagi, *Treaty Interpretation in WTO Dispute Settlement*, 19 Minn. J. Int'l L. 275, 296–325 (2010) (arguing that the non-discrimination clause in the TRIPS should be interpreted so as not to nullify the requirement of non-working inherited from the Paris Convention).

[104] Paris Convention, Art.5(A); TRIPS Agreement, Art.2(1).

[105] Frederick M. Abbott & Graham Dukes, Global Pharmaceutical Policy: Ensuring Medicines for Tomorrow's World 136-140 (2009).

[106] *See generally* Roger Bate, *Local Pharmaceutical Production in Developing Countries: How Economic Protectionism undermines Access to Quality Medicines*, Int'l Pol'y Network (2008) (Campaign for Fighting Diseases discussion paper no. 1); Warren Kaplan & Richard Lang, *Local Production of Pharmaceuticals Industrial Policy and Access to Medicines*, WHO Report (2003) (Paper prepared for World Bank Meeting on the Role of Generics and Local Industry in Attaining the Millennium Development Goals (MDGs) in Pharmaceuticals and Vaccines Conference Washington, D.C., June 24, 2003).

[107] *See* Pharmaceutical Production, *supra* note 46.

D. The 'Rule of Reason' Justification

The right to refrain from using one's Intellectual Property is not an absolute right.[108] Working requirement would be enforced when the right to refrain from using and refusing others from using becomes abusive. This view does not change the settled understanding of intellectual property rights as a negative right. This only qualifies the right in circumstances where the exercise or non-exercise of the right amounts to an abuse. Working is required, not in all cases, but at least in cases where non-working would lead to an abuse. Like the 'rule of reason' in antitrust law which limits the prohibition of restraint of trade,[109] courts interpreting the working requirement in patent law could evolve a similar rule that limits the local working to instances where the absence of working amounts to an abuse.

Thus, the duty to interpret the term "worked in the territory of India" would require a reasonable meaning which would not destroy the patentee's right to exploit the patent. Patents are applied for at an early stage in the life of an invention, and in many cases inventors will require time to further develop and commercialize their inventions for financial, regulatory and business reasons.[110] Indeed, a rule that required all patents to be offered for licence would be wasteful and burdensome. Thus, working requirement should be applied only in cases where non-working or inadequate working amounts to an abuse such as non-availability of the drug, non-affordability of drug or in cases where there is a need to build capacity locally. Such an understanding will distinguish the local non-working of patents from the broader concept of a patent abuse. The remedy for local non-working could be the local working of the patent, which could be satisfied by 'sham' working without any real benefit, whereas the remedy for an abuse would be to address the situation caused by the abuse, where local working will not necessarily address the abuse.[111]

---

[108] A reasonable fetter on the patent rights in the form of compulsory licence is within the purview of the Paris Convention and TRIPS Agreement, when there is an abuse of patent rights. *Nexavar licence*, *supra* note 72, at 42.

[109] Lee Loevinger, *The Rule of Reason in Antitrust Law*, 19 A.B.A. Antitrust Section 245, 246 (1961) (stating the Supreme Court's decision in *Standard Oil* case that the rule of reason was not that acts which the statute prohibited could be removed from its prohibitions by a showing that they were reasonable, but that the duty to interpret the term restraint of trade required a reasonable meaning which would not destroy the individual right to contract and carry on trade).

[110] Feroz Ali Khader, *Making Patents Work*, Spicy IP Blog (Mar. 11, 2010, 12:41 AM), http://spicyipindia.blogspot.com/2010/03/guest-post-by-feroz-ali-making-patents.html.

[111] Penrose, *supra* note 1, at 170–71.

IV. Conclusion

Unexpectedly, the grant of market-initiated compulsory licences allowed originator pharmaceutical companies to practice price differentiation without the fear of parallel import as the terms of the grant restricted the sale locally. Moreover, since it is the government of the developing country that sets the price of the licensed product, such instances may not be used for reference pricing of products in the primary market. The grant of such licence protected the inventions made in the developed countries by removing the threat of forfeiture of patents, which would have opened the invention to all domestic firms by limiting third-party use to one entity.[112] In countries where generic companies that engage in proactive infringement and do not face the threat of treble damages, a market-initiated compulsory licence restricts the entry of generics to a single entity and operates as a disincentive for generics to compete on lower prices.[113] The terms of the grant strictly imposed restrictions on the licensee allowing the patentee to hold the patent and exploit the residual rights. Market-initiated compulsory licences also allow originator companies to profit from newer, untapped and highly differentiated markets like India, where the market is segmented with the originator companies catering to the rich, high-income consumers and generics to the poorer, middle and low income consumers.[114]

The Nexavar licence episode is a testimony to the resilience of the compulsory licensing regime which has grown stronger with every effort to constrain it.[115] The emergence of market-initiated compulsory licences as an alternative to government use-licences, to some extent, democratizes a regime that was seen as arbitrary. Different from those issued in times of a health emergency, market-initiated compulsory licences are responses to

---

[112] Penrose, *supra* note 1, at 159. When a compulsory licence is issued, the monopoly becomes a duopoly.

[113] It is unlikely that another generic company will enter the market after the grant of a compulsory licence. Cipla's case in the Nexavar episode was exceptional as it had entered the market before the grant of the licence. Cipla's profit margins after the grant of licence plummeted when the price was set at Rs. 8800. Cipla had to reduce its prices to survive in the market. *See* Priyanka Golikeri, *Natco's Compulsory Licence has had the Intended Effect*, Daily News & Analysis, May 22, 2012, http://www.dnaindia.com/money/report_natcos-compulsory-licence-has-had-the-intended-effect_1691978.

[114] *See* Interview by V. Venkatesan with Shamnad Basheer, Chair Professor Intellectual Property Law, National University of Juridical Sciences, Kolkata (Apr. 21, 2012), http://www.frontlineonnet.com/fl2908/stories/20120504290802600.htm

[115] Jerome H. Reichman, *Compulsory Licensing of Patented Pharmaceutical Inventions*, 37 J.L. Med. & Ethics 247, 248 (2009) (noting that while international minimum standards of patent protection have gradually and progressively risen over time, every attempt to limit or constrain a state's power to issue compulsory licences has invariably resulted in a strengthening of that power at the international level).

a special situation caused when patents picket—a condition identified as a refusal to work the patent locally, either by the patentee on its own, or by a third-party licensee. Like any compulsory licence, market-initiated compulsory licences are exceptions which need to be used exceptionally.[116] And their assertion is not without accompanying costs: it takes a special legal regime, vibrant local talent, political will and economic incentives to work the system. Not all countries, given the disparities in development even amongst developing countries, may have the ability to work a market-initiated licensing regime. And, more significantly, not all countries with the capability will take it lightly to issue such licences. For when such licences are issued, they significantly affect the redistribution of entitlements.

Given the history of development of compulsory licences, countries will continue to use them and justify their use. Since market-initiated compulsory licences are triggered by an abuse of patent, countries have to declare what amounts to an abuse to avoid uncertainty in the market and to balance the policy implications, both for the patentee and for the consumers, in granting such licences. The responsibility is, however, not one-sided. Patentees of life-saving drugs who operate in markets where the majority cannot afford their products should devise ways in which they can address the issues of consumers who pay a heavy price for their inability to pay the price of a live-saving drug. While harmonization of international laws enabled these giants to cross borders with ease, these companies need to adapt to meet the local needs in the developing markets, which are different from those in advanced markets, and may through ingenious adaptations even profit from these markets.

If there is one lesson that the Nexavar licence tells us, it is this: the world is not fully ready for complete harmonization. The world, as some see it, is at best partially globalized or semi-globalized.[117] A semi-globalized world is still a divided world. The Nexavar licence, strangely, tells us that there could be some benefits that flow from the disparities in development between countries, as strictly enforced compulsory licensing regimes will offer protection for the originator company from the dangers of parallel importation and reference pricing and encourage them to practise price differentiation.

---

[116] *But cf.* Robert P. Merges, *Of Property Rules, Coase and Intellectual Property*, 94 Colum. L. Rev. 2655, 2656 (1994).

[117] *See generally* Pankaj Ghemawat, Redefining global strategy: crossing borders in a world where differences still matter (2007) (noting that while the world's market and economies are becoming increasingly integrated, the process is far from complete).

Technology Innovations in Securities Trading: Can SEBI's Bicycle Catch the High-Frequency Trading Ferrari

Armaan Patkar[†]

Abstract: Algorithmic high-frequency trading is a tech-innovation of securities trading. It is enabled by high-tech trading algorithms and communication and computing infrastructure that allows traders to profit based on the speed and volume of their trading, rather than by trading based on conventional trading fundamentals. However, its strategies have become ubiquitous with market manipulation, regulatory arbitrage and clouding the ability of investors to accurately read the market. Understandably, regulators have been making efforts to protect the markets and stay abreast with the rapid evolution of high-frequency trading.

In this endeavour, the U.K. Financial Services Authority remarked that regulators are riding bicycles to chase down the high-frequency trading Ferrari. Further, this Ferrari seems to constantly change its license-plate, routes and appearance. This has complicated efforts to prescribe preventive measures and seems to have resulted in a disproportionate reliance on post-facto remedial measures. In this light, this Article evaluates SEBI's proposals in its recent discussion paper on algorithmic trading and proposes certain measures to strengthen SEBI's regulatory framework.[1]

† Associate at AZB & Partners, Mumbai. The author can be contacted at *armaanpatkar@gmail.com*.

1 See John Bates, *Algorithmic Trading and High Frequency Trading: Experiences from the Market and Thoughts on Regulatory Requirements*, Meeting of the Technical Advisory Committee, Commodity Futures Trading Commission [CFTC], (Technological Trading in the Markets) (July 14, 2010), http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/tac_071410_binder.pdf.

I. Introduction

> "*Social uselessness - It's hard to imagine a better illustration than high frequency trading. The stock market is supposed to allocate capital to its most productive uses, for example, by helping companies with good ideas raise money. But it's hard to see how traders who place their orders one-thirtieth of a second faster than anyone else do anything to improve that social function.*"[2]
>
> —P. Krugman

The function of technological development is to reduce human inefficiency and to make human life easier. In the securities markets, this function translates into increasing market efficiency and enabling easier and faster trading, by bypassing human limitations. High-frequency Trading ("**HFT**") is a manifestation of this function, which has catalyzed a tech-(r)evolution of the securities markets by allowing traders to profit from trading milliseconds before others, instead of requiring them to make informed trading decisions. In theory, if made milliseconds before a slightly worse trade, even a bad trade can make money for a high-frequency trader ("**HF Trader**"). This has the potential to obfuscate investment principles and divert capital markets from business-based value creation. This can cloud the view of the markets, to the point where investors cannot be certain whether they are looking at the market or an HFT mirage.

This mirage is best explained with reference to an anecdote from Flash Boys, an exposé on HFT; in 2007, Bradley Katsuyama, a trader with the Royal Bank of Canada (RBC) tried to execute trades based on price quotes displayed on their computer screens. However, as soon as he would place orders, the prices would change and he would end up buying or selling at a worse price than what was shown on the screen. This was happening to other RBC traders as well. Eventually, the Bradley realized that the prices on his screen were changing in reaction to his orders, before they could be executed into trades. This is because HF Traders were fast enough to react to these orders and race ahead with better-priced orders of their own, at a better price.[3]

Unsurprisingly, HFT's technological prowess has allowed it to dominate the Indian securities market. From 2011-12 to 2015-16, the percentage of

---

[2] Paul Krugman, *Rewarding Bad Actors,* The Opinion Pages, Aug. 2, 2009, http://www.nytimes.com/2009/08/03/opinion/03krugman.html?_r=2. P. Krugman won the Nobel Memorial Prize for Economic Sciences in 2008.

[3] Michael Lewis, Flash Boys: A Wall Street Revolt (W.W. Norton & Company 2014) [Lewis].

HFT orders in India increased from 65% to 94% in cash equity and from 78% to 98% in equity derivatives.[4] Following this growth, SEBI has been incrementally regulating HFT through circulars, in exercise of its powers to protect the interests of securities investors and markets.[5] However, in my view, the extant regulatory framework is disproportionately reliant on post-facto remedial measures and does not inspire confidence. In fact, SEBI itself admitted last year that it cannot stop all instances of manipulative HFT.[6] Accordingly, on the back of the examination by various securities markets and regulators of proposals to contain and regulate HFT, SEBI issued a Discussion paper on '*Strengthening of the Regulatory framework for Algorithmic Trading & Co-location*' ("**Discussion Paper**"), soliciting comments from Indian market participants on proposed changes to the extant regulatory framework.[7]

This Article is a critique of the Discussion Paper. Part II of this Article contains a prefatory description of the key features and characteristics of HFT. Part III discusses and evaluates SEBI's current regulatory approach and framework, including a section on co-location, a key feature of HFT. Part IV evaluates SEBI's proposals proposed by SEBI in the Discussion Paper and other measures that may be considered in place of, or in tandem with, SEBI's proposals. Part V addresses a fundamental concern that touches upon the current market structure of Indian stock exchanges, arising out of such exchanges being self-regulatory delegatees of SEBI's regulatory responsibilities. Part VI contains findings and recommendations with regard to the proposals discussed in Part V. In Part VII, I conclude that SEBI should carry out a pre-emptive upgrade of its HFT rules, which must be flexible enough to react to arbitrage, but must always be grounded on India focused and comprehensive economic research.

---

4 Jayshree Upadhyay and Sachin Mampatta, *Sebi looking at ways to limit algo trading, co-location benefits*, LiveMint:Money (Apr. 13 2016), http://www.livemint.com/Money/fK2Uiuoal9lzOuTFP2E7DK/Sebi-looking-at-ways-to-limit-algo-trading-colocation-bene.html.

5 §11(1), Securities and Exchange Board of India Act, 1992.

6 *Sebi to take stern action on algorithm trades misuse, says chairman U.K. Sinha*, Business Today (Jul. 30, 2015), http://www.businesstoday.in/markets/stocks/sebi-to-take-stern-action-on-algo-trades-misuse-chairman/story/222241.html.

7 SEBI, *Discussion paper on 'Strengthening of the Regulatory framework for Algorithmic Trading & Co-location'*, Aug. 5, 2016, http://www.sebi.gov.in/cms/sebi_data/attachdocs/1470393485587.pdf. [Discussion Paper]

II. Understanding High-Frequency Trading

Algorithmic trading is a method of trading securities on stock exchanges using computer algorithms, without human direction or control. It was first defined by SEBI in 2012 to mean generation of orders by using automated execution logic.[8] A more descriptive definition was proposed by the U.S. Commodity Future Trading Commission ("**CFTC**"), which is expressed in processual terms and traces the life cycle of a trade from preliminary decision-making to post-submission order management, as trading:

- Where algorithms determine whether to initiate, modify, or cancel an order, or makes other determinations with respect to an order such as relating to the target security, the market where the order will be placed, the order type, timing, sequencing, price, quantity of the order, etc.;
- electronic submission of such order for processing to the concerned market; and
- post-order submission management.[9]

HFT is a sub-set of algorithmic trading, where trading is implemented in large volumes within a short period of time.[10] It developed due to the securities markets observing the first-in-time rule, which allows trading in milliseconds to matter.[11] This rule means that at the same price, time-priority

---

[8] SEBI Circular dated March 30, 2012 bearing Ref. No. CIR/MRD/DP09/2012 [March 30, 2012 Circular].

[9] Algorithmic trading is trading where algorithms automatically, or with limited human direction, decide whether to initiate orders and make decisions relating to timing, price, quantity and post-submission order management; *See* CFTC, *Q & A – Notice of Proposed Rulemaking on Regulation Automated Trading ("Regulation AT")*, Office of Public Affairs, (Proposed §1.3(ssss)), November 24, 2015 www.cftc.gov; [CFTC Q&A]; *See also* §4.1.(39), (40) Directive 2014/65/E.U, European Union, 15 May 2014 on markets in financial instruments [MiFID II]; This must involve computerized decision-making processes and not merely a system which only routes, confirms or processes executed orders. It is generally characterized by infrastructural attempts to minimize latency, avoiding human intervention and high intraday message rates in form of orders, quotes or cancellations; *See* Bundesanstalt für Finanzdienstleistungsaufsicht, *Translation of the main provisions of the High Frequency Trading Act (Hochfrequenzhandelsgesetz)*, Jan. 8, 2014, http://www.bafin.de/SharedDocs/Aufsichtsrecht/EN/Gesetz/hft_en.html [HFTA].

[10] For example, in October 2008, one HF Trader traded over 2 billion shares in one single day, accounting for over 10% of U.S. equity trading volume on that trading day; *See* Carol L. Clark, *Controlling risk in a lightning-speed trading environment*, Federal Reserve Bank of Chicago Financial Markets Group, Policy Discussion Paper Series PDP 1 (2010), https://www.chicagofed.org/publications/policy-discussion-papers/2010/pdp-1.

[11] Frank Pasquale, *Law's Acceleration of Finance: Redefining the Problem of High-Frequency Trading*, 36 Cardozo Law Review 2088, 2089 n. 15, (2015), http://www.cardozolawreview.com/content/36-6/PASQUALE.36.6.pdf.

determines which order should be executed. HF Traders exploit this rule by using their ultra-fast trading systems. But how fast is fast? Measuring HFT speed against human time horizon – the blink of an eye, shows that it is possible for a trader to issue roughly 400,000 trades in the blink of an eye:

Sr. No.	Description	Time Taken (Seconds)	Time Taken (Nanoseconds)
	The blink of an eye[1]	0.3	300,000,000
	Preparing an algorithmic trade.[2]	0.000,000,74	740
Number of Trades in the blink of an eye: 300,000,000 = 405, 405.41 Trades 740 = 1.2 Million Trades per Second (approx.)			

1 William Briggs, *How long is A 'Blink of an Eye' astronomically?* (William M. Briggs Oct. 24, 2010), http://wmbriggs.com/post/1750/.

2 Brendan Conway, *Wall streets need for trading speed: The Nanosecond age* (Wall Street Journal), http://blogs.wsj.com/marketbeat/2011/06/14/wall-streets-need-for-trading-speed-the-nanosecond-age/.

The speed of communicating these orders is key. HF Traders look to have low 'latency' i.e. the time-taken to transmit an order from the HF Trader's server to the markets servers (which match buy and sell orders). Each millisecond of reduced latency is worth over USD100 million.[12] This resulted in exchanges permitting co-location, which as the name suggests, refers to the system of stock exchanges allowing algorithmic traders to set-up their I.T. servers within the premises of the stock exchanges. In India, the Bombay Stock Exchange ("**BSE**"), National Stock Exchange ("**NSE**") and the MCX Stock Exchange offer co-location racks in their server rooms on lease to traders.[13] This is done to get as close as possible to the trade-matching servers of the stock exchange and achieve a speed advantage in data-transmission. This is system is quite controversial and a lot of criticism of HFT is linked to strategies enabled by this system.

Given that HFT implements speed-based strategies rather than investment-based value creation, its strategies are generally implemented from day-to-day, with the goal of achieving a flat net position overnight (where the buying and selling of positions offset each other and the HF Trader has no

12 Ciamac Moallemi and Mehmet Saglam, *The Cost of Latency in High-Frequency Trading*, 2 n.4 (February 5, 2013), http://ssrn.com/abstract=1571935.

13 Similarly, exchanges in other countries such as the Tokyo Stock Exchange, London Stock Exchange, New York Stock Exchange, etc., offer co-location to their stock brokers; *See* SEBI, *Discussion paper on Co-location/ Proximity hosting facility offered by the stock exchanges*, http://www.sebi.gov.in/cms/sebi_data/attachdocs/1367581007462.pdf.

un-hedged positions).[14] However, defining HFT is not easy as the term is *ex facie* precise, but actually covers a large and diverse set of constantly evolving strategies.[15] Ostensibly, this is why some regulators have defined HFT inclusively with reference to its characteristics, discussed above.[16] A ring-fenced definition could allow regulatory arbitrage, especially since traders are constantly evolving their strategies and algorithms to stay ahead of the regulators.[17] For example, Athena Capital LLC tweaked '*Gravy*', its trading algorithm to knowingly manipulate the NASDAQ in the last few seconds of trading days in 2009, by placing orders which they had no intention of fulfilling and then cancelling them soon thereafter.[18] Knowing very well that Gravy was violating U.S. securities law, Athena Capital internally discussed that they should modify and contain their trading strategies appropriately, so that they do not '*kill the golden goose*'. This was caught by the Securities Exchange Commission (SEC) and Athena Capital was sanctioned for a sum of one million U.S. dollars.[19]

Seemingly to avoid ring-fencing HFT, SEBI did not define HFT separately from algorithmic trading.[20] However, SEBI prescribed HFT targeted regulations, discussed in Part III below. These are generally motive-agnostic and quantitative in approach (for example, SEBI imposes a penalty on trading in excess of prescribed order-to-trade thresholds), based on the assumption that

---

[14] SEC, *Concept Release on Equity Market Structure*, 17 CFR PART 242 Release No. 34-61358; File No. S7-02-10 (Jan. 14, 2010) at 45, https://www.sec.gov/rules/concept/2010/34-61358.pdf.

[15] O'Hara, *High Frequency Market Microstructure*, at 4 (April 2014), http://www2.warwick.ac.uk/fac/soc/wbs/subjects/finance/fof2014/programme/Maureen_ohara.pdf

[16] *Supra* note 9. The Securities Exchange Commission (SEC) has also identified similar characteristics of HFT, such as high-tech infra, programs, co-location, access to data feeds, minimized latency, frequent cancellations, reversals in positions and the goal of a flat-close of the trading day. *See* SEC Release *supra* note 16, at 45.

[17] On average, algorithms last only a few days before they need to be replaced; *See* Tor Brunzell, *High-Frequency Trading—To Regulate or not to Regulate - That is the Question*, 2:1 J.B.F.A. 3, 2013, http://www.omicsgroup.org/journals/high-frequency-trading-to-regulate-ozyr-not-to-regulate-that-is-the%20question-does-scientific-data-offer-an-answer-2167-0234.1000e121.pdf.

[18] *In the Matter of Athena Capital Research, LLC*. Administrative Proceeding File No. 3-16199 Release No. 73369/ October 16, 2014 at ¶8, 11, 23. *See also* In the Matter of Hold Brothers On-Line Investment Services, LLC *et al* Administrative Proceeding File No. 3-5046 Release No. 67924/September 25, 2012 at ¶32.

[19] *Id*. at ¶11, 54. *See also* ¶30, 35 [when Athena's trading strategies were successful, Athena described this in internal emails as "*dominating the auction*", "*owning the game*", "*Looks like we have some Mach chips….going to Vegas tonight….*"]. *See also* ¶39 [A marketing officer informed Athena Capital's CTO that he was concerned that the firms trading strategies were "*punching the stock*." This prompted Athena to cease email exchanges with respect to Athena's trading strategies on Athena's email servers and to use certain search terms to research Athena's trading "*at home, not here*."]

[20] The CFTC did this consciously and sought to extend its proposed regulatory framework (Regulation AT) equally to all algorithmic traders; *See* CFCT Q&A at 12.

breaches are unwanted, even where traders employ *bona fide* and legitimate trading strategies. Such an approach is cautious and appropriate, until SEBI tightens its regulatory framework. When it does do so, it may consider defining HFT with respect to, and by underscoring, its true motive (i.e. to profit from speed-based trading). This would allow SEBI to differentiate between legitimate and fraudulent or manipulative HFT on a qualitative basis.

Currently, SEBI has the power to regulate HFT on a qualitative "*smell test*" basis under the SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003 ("**PFUTP Regulations**"). These regulations generally prohibit and regulate fraudulent and manipulative HFT practices, which could include HFT activities, even if they do not violate SEBI's quantitative provisions.[21] For example, the PFUTP Regulations prohibit activities such as:

- creating false or misleading appearances of trading or entering into a securities transaction without the intention to complete it;
- dealing in securities in a manner which inflates, depresses or causes price fluctuations and price manipulation;
- using or employing manipulative, deceptive or fraudulent devices, schemes or artifices, etc.[22]

While these regulations clarify that the list of fraudulent and unfair practices is not intended to be exhaustive, SEBI may consider specifically prohibiting HFT specific activities, such as activities which:

- are unnecessarily aggressive or disruptive (including order cancellations);
- over-load or destabilize systems or which initiates or exacerbates market trends;
- create pricing illusions or obscure identification of genuine orders;[23]

---

[21] For example, HF Traders can rapidly place large volumes of rapid-fire orders to overload market systems to slow down other traders or ignite market trends. *See* John McPartland, *Recommendations for Equitable Allocation of Trades in High Frequency Trading Environments*, (Revised July 2014), https://www.chicagofed.org/publications/policy-discussion-papers/2013/pdp-1. [At 7- 9, McPartland describes the HFT strategies of '*spoofing*', '*layering*' and '*quote-stuffing*'.] In this regard, it is reported that 96% of orders submitted to the U.S. markets are not executed and may not be *bona fide* Dave Michaels, *Wall Street to Get Graded on How Much Spoofing It's Facilitating*, Bloomberg, January 5, 2016, http://www.bloomberg.com/news/articles/2016-01-05/wall-street-to-get-graded-on-how-much-spoofing-it-s-facilitating.

[22] *See* §3, §4(2) r/w §2(1)(b), 2(1)(c), PFUTP Regulations.

[23] A similar prohibition is contained in the E.U. Market Abuse Directive II; For the text of the E.U. MAD II, *see* http://ec.europa.eu/finance/securities/abuse/index_en.htm.

- or where traders enter orders on one side of the buy-sell equation with the knowledge that a similar order on the other side of the equation will be placed, etc.[24]

Wherever required, the PFUTP Regulations qualify the above provisions with words like '*unnecessarily aggressive*' or '*disruptive*' to provide built-in safeguards for HF Traders to prove the legitimacy of their strategies in legal actions. Additionally, SEBI may consider prefacing these clauses with the words "*unless the contrary is established*" to clarify that these criteria are rebuttable.

III. Regulatory Approach & Framework

Knowing what we know about HFT (or rather, what we do not), allowing HFT to be unregulated or to completely ban HFT would not be advisable. Instead, a suitable regulatory blend of mandatory requirements and *post facto* enforcement should be adopted, which reduces risk exposure without unnecessarily impeding tech-advancement.

Currently, SEBI regulates HFT through circulars and liability regulations.[25] The first move in this regard was a circular in March 2012 which introduced broad guidelines for algorithmic trading.[26] This was after admitting earlier that month, that neither SEBI nor the exchanges were capable of handling HFT.[27] These broad guidelines were supplemented by later guidelines and circulars, issued by SEBI from time to time, and currently, provide for the following:

---

[24] *See* FINRA Manual, Rule 6140 - Other Trading Practices, http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=4322.

[25] *See* SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003.

[26] March 30, 2012 Circular *supra* note 8. SEBI allowed algorithmic trading in 2008 when it allowed direct market access (DMA) to institutional investors, without manual intervention but through broker systems; *See* Anuradha Guru and Rasmeet Kohli, *Direct Market Access: New Kid on the block*, NSE Newsletter Aug. 2009, http://www.nseindia.com/content/press/aug2009_2.pdf; QuantInsti, *Algorithmic trading in India: History, regulations and future*, Industry Regulations and New Developments (Jun. 10, 2015), http://www.quantinsti.com/blog/algorithmic-trading-india/.

[27] *See* Mobis Philipose, *SEBI should study the impact of algorithmic trading before taming it* (Dec. 2012), http://www.livemint.com/Opinion/LmtMQAa8sM4pVZ65XJq2ZO/Sebi-should-study-the-impact-of-algorithmic-trading-before-t.html.

A. Co-location

Co-location (discussed in Part II above) should be effectively available to all, on a uniform and non-discriminatory basis. This has been emphasized by the U.S. Securities and Exchange Commission ("**SEC**"),[28] CFTC[29] and the IOSCO.[30] In this regard, SEBI provides that exchanges must, in order to ensure fair and equitable access to co-location facilities, provides that exchanges must:

- ensure that sufficient rack space is available for all traders who wish to co-locate;
- disseminate information relating to co-located orders, trades, latency and charges, for the purpose of transparency;[31]
- ensure fair, transparent and equitable access to exchange facilities and data feeds to all co-locaters and similar latency to all co-locaters *inter se*.

However, it remains possible to have different data feeds for co-locaters, non-co-locaters and the public. This was a problem in the U.S. where data feeds for co-located traders also contained enriched data, including data relating to cancellations, modifications and executions and revealed the identity, origin, time-stamps of orders, *etc*. HF Traders can use such enriched data to game the system and trade ahead of investors who rely on public feeds to make informed trading decisions.[32] Some exchanges have given preferential access to data to HFT firms, while data-transmission to the public was delayed.[33] Similar concerns exist in India as well, for example,

---

[28] *See* SEC Concept Release *supra* note 9, at ¶58. This is required under §6(5) of the U.S. Securities Exchange Act, 1934, which requires that exchange rules should not be designed to permit unfair discrimination in the markets.

[29] *See* CFTC, *Co-Location/Proximity Hosting Services Proposed Rules*, 33198, Federal Register Vol. 75, No. 112, June 11, 2010, http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2010-13613a.pdf.

[30] *See* SEBI Discussion Paper *supra* note 7; IOSCO, *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency*, Consultation Report (CR02/July 2011) at 28, http://www.iosco.org/library/pubdocs/pdf/IOSCOPD354.pdf.

[31] *See* SEBI Circular dated May 13, 2015 bearing Ref. No. CIR/MRD/DP/07/2015.

[32] *See* McPartland *supra* note 23 at 21, 23-25, 31.

[33] *In the Matter of New York Stock Exchange LLC, and NYSE Euronext*, Administrative Proceeding File No. 3-15023; The NYSE was held to have violated a rule that requires data to be distributed on fair, reasonable and not unreasonably discriminatory terms and which prohibits exchanges from releasing data through proprietary feeds before such data is sent for inclusion in the consolidated feeds [Rule 603(a) of Regulation NMS]. *See also Lanier* v. *BATS Exchange, Inc*., *et al*., 14-CV-3745 (May 23, 2014).

last year, a whistleblower claimed that the NSE is/ has given algorithmic traders inside information.[34]

In this light, I recommend that:

- Data feeds should be equitably disseminated to co-located traders, non-co-located traders and the public. This is an important lesson to be learned from the U.S. which, due to a lacuna in its regulations, allowed HF Traders to get a sneak-peek at the U.S. markets.[35] Such differentials in data feeds should be eliminated. The information in all data feeds should the same, be given at the same time and from the same source, with full transparency. Thereafter, co-locaters can be left free to exploit speed-advantages in data processing and communication to the exchanges. This will balance public policy with the interests of HF Traders as equal access to information is ensured, without unreasonably restricting HFT and tech-innovation. Further, SEBI should clarify that traders should be provided equitable access across different exchanges *inter se* as well.[36]
- Exchanges should be prohibited from implementing measures which effectively deny access to co-location or data feeds to certain traders, such as prohibitive or preferential pricing. Theoretical support for this measure can also be found in the SEBI (Prohibition of Insider Trading) Regulations, 2015 ("**Insider Trading Regulations**"), especially if HF

---

[34] Sucheta Dalal, *High-frequency trading needs a detailed probe* (Moneylife Jul. 8, 2015), http://www.moneylife.in/article/high-frequency-trading-needs-a-detailed-probe/42620.html; U.S. exchanges have also created special types of orders for HF Traders, for example, "*hide not slide*" orders that are not displayed to other traders; *See* Lee Sheppard, *A Tax to Kill High Frequency Trading*, Forbes, October 16, 2012, (Page 2, 4) http://www.forbes.com/sites#/sites/leesheppard/2012/10/16/a-tax-to-kill-high-frequency-trading/.

[35] SEC's Regulation NMS requires a consolidated Securities Information Processors feed to consolidate and calculate a National Best Bid and Offer ("**NBBO**"), before it disseminates market information to the public. This is not required for proprietary data feeds and therefore, instead of waiting for the NBBO, algorithmic traders could use the proprietary feeds to make their calculations faster than the NBBO calculation. *See* Testimony of Bradley Katsuyama before the Permanent Sub-committee on Investigations, *Conflicts of Interest, Investor Loss of Confidence, and High Speed Trading in U.S. Stock Markets*, June 17, 2014, at 5, http://www.hsgac.senate.gov/subcommittees/investigations/hearings/conflicts-of-interest-investor-loss-of-confidence-and-high-speed-trading-in-us-stock-markets. *See* also Scott Patterson & Jenny Strasburg, *For Superfast Stock Traders, a Way to Jump Ahead in Line*, Wall Street Journal (Sept. 12, 2012), http://www.wsj.com/articles/SB10000872396390443989204577599243693561670.

[36] This has recently (November, 2015) become an issue for BSE co-locations, because allegedly the NSE gives tick-by-tick data to its co-locaters, but does not provide the same date for BSE co-locaters. The NSE denied that it does not provide its fast market data to BSE co-locaters, in response to a query raised by Business Standard; *see* StockMarkets.in, *Brokers cry foul over NSE's data feed speed in BSE colo facility*, (November 19, 2015), http://stocksmarket.in/225677/2015/11/19/brokers-cry-foul-over-nses-data-feed-speed-in-bse-colo-facility/.

> Traders can access enriched data before such data is made public. In my view, this falls within the spirit, though not the letter, of the Insider Trading Regulations.[37] Such data may be viewed as unpublished price-sensitive information ("**UPSI**") relating to Indian listed securities. For example, an HF Trader may use such enriched data to detect a sale of a large block of shares by an institutional investor or the promoters of a company, before such news becomes generally available. Assuming such information is UPSI, HF Traders would be prohibited from trading in the securities of the company, for so long as the information does not become public.[38]

The counter to this argument is that the data provided by the exchange, in its raw form, is not UPSI as it is of no use by itself. It only becomes useful trading information when algorithms analyze the data and the market for such securities. Merely because this analysis can be completed before this data becomes public (usually mere milli or micro-seconds later), is not sufficient to label such data as UPSI, even though this small time-window is sufficient for the algorithmic trader to profitably trade based on such information. In support of this argument, the Justice Sodhi Committee Report recommended that '*generally available information*' (which is linked to the test for UPSI as above), should be defined as information available on a non-discriminatory basis; this was incorporated in the Insider Trading Regulations.[39] This was after the Committee stated that '*conclusions, deductions and inferences drawn from information analyzed by an insightful mind*' should not be treated to be UPSI.[40] Therefore, it is arguable that the results of the data analysis undertaken by HFT algorithms are not UPSI since they are conclusions drawn from market data.

However, the Committee also considered information which is priced in a manner which allows only certain identified persons to acquire such

---

[37] The New York Attorney General labeled HFT as "*insider trading version 2.0*" as it falls outside the parameters of traditional insider trading; but it gives certain traders access to market-moving information which is not available to the rest of the market; *See* N.Y. Attorney General, *Remarks on High-Frequency Trading & Insider Trading 2.0*, New York Law School Panel on "Insider Trading 2.0 – A New Initiative to Crack Down on Predatory Practices", (as Delivered, Mar. 18, 2014), Eric T. Schneiderman, http://www.ag.ny.gov/pdfs/HFT_and_market_structure.pdf.

[38] *See* SEBI (Prohibition of Insider Trading) Regulations 2015 ("Insider Trading Regulations"), §4 r/w 2(n).

[39] *See* Proposed §2(f), N.K. Sodhi Committee, *Report of the High Level Committee to Review SEBI (Prohibition of Insider Trading Regulations, 1992* (SEBI), Dec. 7, 2013, http://www.sebi.gov.in/cms/sebi_data/attachdocs/1386758945803.pdf.

[40] *Id*. at ¶30, Note to Proposed §2(f); *See also* Corporations Act 2001, §1042C(1)(c) (Australia), "*When information is generally available*", http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s1042c.html, which contains a similar provision.

information, as being information having discriminatory access, *ergo* not generally available, *ergo* UPSI. Therefore, there is policy support for SEBI to restrict the exchanges from prohibitively pricing access to co-location and data feeds.

- SEBI may consider providing that co-location facilities should be provided by independent third-parties and not the exchanges. For example, to remove any conflict of interest, BSE does not own its co-location facilities and allows co-location data-centre vendors to set-up at the exchange.[41]
- Equal latency amongst all co-locaters at one exchange should be provided for, instead of similar latency, simply achieved by providing for equidistant cabling;[42]
- SEBI should reconsider its minimalist regulatory role in co-location and should require exchanges to frame co-location rules and seek SEBI approval prior to their implementation.[43] This issue is discussed in greater detail in Part IV and V of this Article.
- Exchanges should be required to disclose to the public, details of the structure, mechanics, features, attributes, etc. of their systems, trading platforms, their effects on the markets or trading experience, including disclosing any effects which are not readily apparent;[44] and
- Lastly, SEBI should thoroughly investigate allegations of preferential access or inside information being given to HF Traders and the claims of the NSE whistleblower, discussed above. This is on the heels of SEBI's Technical Advisory Committee finding that the NSE violated fair access norms, allowing some traders to benefit therefrom. In this case, SEBI should appoint an independent tech-consultant to study the vulnerabilities of Indian exchange systems and to investigate allegations of fraud, collusion, etc., who must report directly to SEBI.[45]

---

41 *Supra* note 4.

42 For example, the Chicago Mercantile Exchange and the Hong Kong Exchange. *See also* Association of National Exchanges Members of India, *Comments on Proposal on Co-location / Proximity hosting facility offered by the Stock Exchanges*, May 31, 2013, http://www.anmi.in/admin/anmiatworkfiles/Letter%20to%20SEBI%20-%20Comments%20on%20Proposal%20on%20Co-Location%20-%20Proximity%20hosting%20facility%20offered%20by%20the%20Stock%20Exchanges.pdf.

43 This is required in the U.S. where co-location services are subject to the U.S. Exchange Act, which requires prior SEC approval for rule changes, including co-location rules. *See* SEC Concept Release *supra* note 16, at 58.

44 Proposed revisions to §38.401(a) and (c), CFTC, Q&A *supra* note 9.

45 Mobis Philipose, *What action should Sebi take in NSE algo trading case*, In the Money: April 12, 2016, http://www.livemint.com/Money/R34WpIgkgLuVrFZVnHKCbM/What-action-should-Sebi-take-in-NSE-algo-trading-case.html.

B. The Order-to-trade Penalty Rule: monetary disincentive to aggressive trading

HFT commonly involves highly aggressive trading strategies, involving high volumes of cancellations and modifications of orders without any legitimate purpose. These can have a manipulative effect on the market and therefore, in 2012 SEBI introduced monetary disincentives for high daily order-to-trade ratios, known as the '*Order-to-trade Penalty Rule*'.[46] The penalty is a charge prescribed and collected by exchanges for each order that exceeded the prescribed ratios.[47] Where traders are penalized for such breaches more than ten times within a span of thirty days, exchanges could suspend traders for one hour on the next trading day.[48] However, traders can still hide bursts of manipulative HFT activity in the course of the trading day, so long as the prescribed daily limits are maintained. This should be deterred by requiring intra-day calculations as well, which should be calculated at the time of testing and approval of algorithms.

In contrast to this quantitative approach, the German *Hochfrequenzhandelsgesetz* (High-frequency Trading Act) imposes fees on disproportionately high order entries, modifications or cancellations. The amount of fees is to be determined by the exchanges on a case-to-case basis, in a manner which effectively counteracts excessive usage and associated adverse impacts on system stability and market integrity.[49] Suspension for up to 6 months can also be imposed for breaches of prescribed order-to-transaction ratios, with revocations of the participants admission to the exchanges in case of repeated failures.[50] While the German approach is nuanced and fairly strict, SEBI's approach is better suited to India's current needs, given that exchanges have monitoring systems to place to identify and initiate measures to impede order-flooding and especially, if Execution Throttles (discussed in Part IV below) are implemented. Further, it is simple to implement, has predictable consequences and SEBI can always target illegitimate, excessive or aggressive trading (or other qualitative violations), under its PFUTP Regulations.

---

[46] Discussion Paper *supra* note 7.

[47] March 30 Circular *supra* note 8; The initial rates prescribed by the exchanges pursuant to this requirement were perceived by SEBI to be far too low and in 2013, SEBI directed the exchanges to double these rates; SEBI Circular dated May 21, 2013 bearing Ref. No. CIR/MRD/DP/16/2013 [May 21, 2013 Circular.

[48] May 21, 2013 Circular *Id.*

[49] *See* §17, HFTA *supra* note 9.

[50] *See* §19, HFTA *supra* note 9.

C. Testing, exchange approval and risk-controls

At the very heart of HFT, is the technology that enables it. Like all forms of technology, HFT algorithms can malfunction. For example, in 2012 a U.S. based HFT firm, Knight Capital Americas LLC lost USD440 Million from taking unwanted positions, when its algorithm went rogue for merely 45 minutes and executed over 4 million orders.[51] This threat pushed the U.K.,[52] MiFID II[53] and Germany[54] towards implementing risk-controls for algorithmic trading.[55]

SEBI had already put such measures in place in 2003, before HFT came into vogue. It required all brokers to undertake to use only authorized software.[56] In 2012, noticing the growing trend in algorithmic trading of financial instruments, SEBI added the following testing and approval requirements:[57]

- Algorithmic traders must satisfy the exchanges that algorithms have pre-defined trading limits outside of which orders cannot be pushed to the exchange's trading servers;
- Algorithmic traders must undertake that they have sufficient risk controls to prevent misuse of algorithms and real-time monitoring to identify malfunctioning algorithms;
- Algorithm software requires pre-deployment testing (functional and technical) and traders require prior exchange permission before they can provide algorithmic trading services; and

---

[51] *In the Matter of Knight Capital Americas LLC,* SEC Administrative Proceeding File No. 3-15570 Release dated October 16, 2013.

[52] *See* Financial Conduct Authority, *CP15/22 Strengthening accountability in banking: Final rules*, July 2015, https://www.fca.org.uk/static/documents/consultation-papers/cp15-22.pdf.

[53] *See* Cheryl Jones, *Financial services*, Financial Services (Oct. 28, 2013), http://blogs.lexisnexis.co.uk/fs/italys-ftt-on-hft-catching-up-with-high-frequency-trading/.

[54] *See* HFTA *supra* note 9.

[55] The SEC also has a Market Access Rule (Securities Exchange Act Rule 15c3-5) which requires the establishment, documentation and maintenance of a risk management system and supervisory procedures; Further, CFTC's Proposed Regulation AT includes pre-trade risk controls (maximum order message and execution frequency per unit time, order price and maximum order size parameters), and order cancellation systems. (proposed §1.80). It also provides implementation of standards for development, testing and real-time monitoring (proposed §1.81); *See* CFTC, Q&A *supra* note 9.

[56] SEBI Circular dated August 21, 2003 bearing Ref. No. SEBI/MRD/Policy/SE/15864/2003

[57] *See* March 30, 2012 Circular *supra* at 8; May 21, 2013 Circular *supra* at 50; SEBI Circular dated August 19, 2013 bearing Ref. No. CIR/MRD/DP/24/2013 [August 19, 2013 Circular]

- All algorithmic traders are required to submit their algorithmic trading systems to a system audit every 6 months by a qualified system auditor.

However, even tested and approved algorithms may malfunction and risk-controls may not be foolproof; such controls were in place for Knight Capital, but failed. In this regard, SEBI requires traders to set-up a preventive measure called an automated execution check. This is required to ensure that algorithms account for all executed, unexecuted and unconfirmed orders placed by it, before releasing further orders. Importantly, it must ensure that malfunctioning algorithms are automatically stopped. Keeping in mind that algorithms and automated execution checks can malfunction, on the curative side, exchanges are required to ensure that they have systems to identify malfunctioning algorithms. Further, they are allowed to remove outstanding orders from malfunctioning algorithms, levy discretionary deterrent penalties including suspensions and even shut down trader terminals in case of emergencies.[58]

SEBI also requires traders to '*consider*' taking suitable insurance against software malfunctions, which should be made mandatory given the possibility of malfunctions leading to great losses. In this regard, Korsmo suggested a mixed liability-government '*responsibility waterfall*', where the first recourse would be to the funds of the trader, including insurance payouts. If the trader becomes insolvent before the losses can be recouped, recourse may be had to a common fund, like SEBI's Investor Protection and Education Fund, which should comprise compulsory contributions made by algorithmic traders or the recoveries of an HFT-targeted tax (if implemented).[59] If the fund also fails to discharge this loss, the last resort would be to approach the Government.[60]

D. Audit trails and surveillance

SEBI requires algorithmic traders to maintain logs and records of algorithmic trades. These trades are to be tagged with unique identifiers provided by the stock exchanges to establish an audit trail.[61] This is an important measure which allows *post facto* reconstruction of trading activity, which helps in the effective identification and investigation of trading violations and in the consequent assignment of responsibility for such violations. It also

---

[58] March 30, 2012 Circular *supra* note 8; August 19, 2013 Circular *supra* note 59.

[59] See the section on Securities Transaction Tax in Part V below.

[60] Charles Korsmo, *High-Frequency Trading: A Regulatory Strategy*, 48 University of Richmond Law Review 588-593 (2014).

[61] March 30, 2012 Circular *supra* note 8.

helps SEBI understand market forces and serve as valuable tool for crafting regulatory strategies.

SEBI also requires traders to have real-time monitoring systems to identify malfunctioning algorithms and immediately inform the exchanges of any abnormal behavior. Exchanges are also required to put monitoring systems in place to identify and initiate measures to impede order-flooding.[62] In 2012, recognizing that there was a need to strengthen surveillance mechanisms and prevent market manipulation, SEBI directed all exchanges to ensure effective monitoring and surveillance of algorithm orders and trades.[63] However, SEBI's involvement was limited to receiving monthly reports on algorithmic trading submitted by exchanges.[64]

E. Circuit-breakers

Circuit-breakers are systems which automatically halt trading when prices move beyond prescribed limits within a trading day. These prevent excessive price fluctuations and have been implemented in India market-wide since 2001, in incremental thresholds of 10%, 15% and 20%. Once triggered, exchanges are required to stop matching orders and purge all unmatched orders in the system. Depending on the point in time in the trading day when these movements happen, trading resumes either on the same or on the next trading day.[65] To ensure that circuit-breakers are triggered as soon as possible, circuit-breaker limits are calculated daily, based on the previous day's closing level.[66]

These circuit-breakers are intended to be instantaneous. For example, pursuant to a *suo motu* special purpose inspection, SEBI censured NSE for a six-second delay between the trigger at 09:50:58 a.m. and trading halt at 09:51:04 a.m. NSE contented that it was sufficient to stop the entry of fresh orders into the system after triggering the circuit-breakers, but after executing executable orders already in the system. Stating that the legislative intent of circuit-breakers is to stop the securities market from panicking and making impulsive, irrational decisions, SEBI rejected NSE's contentions.[67] To

---

[62] *Id*..

[63] May 21, 2013 Circular *supra* note 50.

[64] These reports include, apart from statistical data pertaining to turnover, volumes and percentages, details of action taken in respect of malfunctioning algorithms, status of grievances, if any, received and processed, etc. *See* March 30, 2012 Circular *supra* note 8.

[65] SEBI Circular dated June 28, 2001 No. SMDRPD/Policy/Cir-37 /2001.

[66] SEBI Circular dated September 03, 2013 bearing Ref. no. CIR/MRD/DP/ 25 /2013.

[67] *In re: National Stock Exchange of India Limited* bearing SEBI Order dated October 10, 2014 Ref. No. WTM/PS/38/MRD/DSA/OCT/2014. This resulted from an erroneous trade which was supposed to be a sell order for 17 lakhs in value but was instead placed for 17

prevent such situations from occurring and to ensure real-time monitoring, in 2015 SEBI required BSE and NSE to compute their market-wide index after every trade and run the computations through the circuit breakers. Further, SEBI required exchanges to ensure that their systems give priority to circuit-breakers and ensure immediate response times.[68]

IV. Incremental Regulatory Strategies & Measures

Despite the measures implemented by SEBI, discussed in Part III above, there are still concerns in the Indian markets with respect to market fairness and integrity. The Discussion Paper is the first step towards identifying, exploring and addressing these concerns. The first portion of this Part discusses SEBI's proposals in the Discussion Paper and is followed by a section discussing incremental measures and recommendations, based on economic and legal theory and experience gained from other markets:

Minimum Resting Time: A Minimum Resting Time ("**MRT**") is the minimum time between when an order is received by an exchange and when it can be amended or cancelled by the trader. If an order is placed during the MRT and if a matching order is placed on the other side of the buy-sell equation during the MRT, the order will be converted into a trade. This would deter traders from placing orders that they do not intend to execute and directly counteract manipulative strategies which rely on immediate modifications or cancellations to orders. For example, a common strategy is to place an order on one side of the buy-sell equation, with the actual intention of the trader being to trade on the other side. The reason for placing the initial order on the other side is to create artificial perceptions of demand and supply and to trigger a market response. If the market moves in the desired direction, the trader cancel the initial order, switches over to the other side and profits from the market reaction.[69]

However, this measure does not discriminate between valid and invalid modifications to orders, for example, valid modifications in response to new incoming news or orders versus invalid orders with the intent of creation virtual liquidity or to detect the reaction of other market participants.

---

lakh scrips amounting to 980 crores. In the six seconds that it took halt trading when the NIFTY Index crashed and breached the 10% circuit-breaker, the 15% circuit-breaker had also been breached.

[68] SEBI Circular No. CIR/MRD/DP/02/2015 dated January 12, 2015.

[69] *See* FINRA, *FINRA Joins Exchanges and the SEC in Fining Hold Brothers More Than $5.9 Million for Manipulative Trading, Anti-Money Laundering, and Other Violations*, News Release, September 25, 2012, www.finra.org/Newsroom/NewsReleases/2012/P178687.

Randomized Speed Bumps: Speed-bumps echo Krugman's statement that trading in milliseconds serves no social purpose,[70] and consequently, impose delays on incoming orders. If the delay exceeds the speed-advantages enjoyed by HF Traders, it would counter latency-sensitive strategies.[71] For example, the IEX Group, a stock exchange founded by Bradley Katsuyama, the protagonist of Flash Boys, proposed an anti-HFT speed-bump of 350 microseconds.[72] It did so by placing a box containing 32 miles of fiber optic cable outside the exchange through which HF Traders have to connect to the IEX.[73] This causes a speed-bump which gives IEX enough time to process trades before HF Traders have time to receive and act on that information. Similarly, the TMX Group in its new TSX Alpha Exchange model has implemented a non-discriminatory speed-bump on order processing and believes that this will assist natural order flow and improve liquidity.[74] However, TSX Alpha's speed bump is of a random duration, within a set lower and upper limit of 1-3 milliseconds, which is perceived as reflective of existing network latencies.[75] This adds another variable to negate arbitrage and latency-sensitive strategies. Such a randomized speed-bump is one of the proposals in the Discussion Paper.

Frequent Batch Auctions: Eric Budish *et al* (2015) devised Batch-auctions as a market-design solution to HFT. Their proposal was to divide the trading day into extremely frequent but discrete time-intervals. During these intervals, exchanges would collect orders which would be matched at the end of such intervals. This would replace the continuous matching of orders on a

---

[70] Krugman *supra* note 2.

[71] *Id.*

[72] *See* Exhibit E, Investors' Exchange, LLC, Form 1, September 15, 2015, (Application for Registration as a National Securities Exchange under Section 6 of the Securities Exchange Act of 1934), http://www.sec.gov/rules/other/2015/investors-exchange-form-1-exhibits-a-e.pdf#page=2.

[73] Jacob Adrian, *Informational Inequality: How High Frequency Traders Use Premier Access to Information to Prey on Institutional Investors*, 14 *Duke Law & Technology Review* 256-279 (2016), http://scholarship.law.duke.edu/dltr/vol14/iss1/11.

[74] Barbara Shecter, *TMX Group to install 'speed bump' to slow HFT traffic, ahead of Aequitas launch*, (October 23, 2014), http://business.financialpost.com/news/fp-street/tmx-group-to-install-speed-bump-to-slow-hft-traffic-ahead-of-aequitas-launch. *See also* §5.9, Alpha Exchange Inc. Notice of Proposed Rule Amendments and Request for Comments, http://www.osc.gov.on.ca/documents/en/Marketplaces/alpha-exchange_20141106_amd-request-for-comments.pdf.

[75] Ontario Securities Commission, *OSC Staff Notice – Notice of Commission Approval to Proposed Changes to Alpha Exchanges Inc.*, www.osc.gov.on.ca/documents/en/Marketplaces/alpha-exchange_20150421_noa-proposed-changes.pdf; Originally, this interval was to be between 5-25 milliseconds, with a fixed difference to be established between the lower and upper limits between 1 to 10 milliseconds. The limits would be fixed and communicated to all participants in advance. *See* John McCrank, *IEX responds to critics of 'flash boys' speed bump* (Reuters 2015), http://www.reuters.com/article/iexgroup-exchange-response-idUSL1N13B2I320151116.

first-come first-serve basis.[76] The chosen interval would be small enough to be economically insignificant, for example 500 milliseconds. This system would operate like an auction, where the best price would win, not the fastest move. Time-priority would therefore take a back seat, only to be resorted to in case of a dead-lock *i.e.* if two orders are priced the same, an earlier order would win over a later order; importantly, this would mean that a later but better price would win over an earlier but lower price within the same interval.

McPartland points out that Batch-auctions would probably reduce I.T. load on exchange servers as the trade matching servers need not run continuously. This could negate the practice of "*quote stuffing*" where HF Traders intentionally clog trading systems with orders. It would also reduce the audit trail and consequently improve supervisory capabilities. Further, given that a batch-auction is like executing a large order (for example, 10,000 lots) versus executing many small orders (for example, 10,000 small lot orders) and that processing one small lot order consumes the same amount of I.T. resources as one 10,000 lot order, Batch-auctions should materially reduce the operating expenses of trading venues, clearing organizations, and trade intermediaries.[77]

An additional layer of complexity can be introduced into this system by matching orders at a random point in time in the batch-auction trading interval (instead at the end of the trading-interval). This would prevent HF Traders from knowing (or being able to estimate) how long their orders will have to wait in the system before they can be matched and whether their speed-advantage would still exist at that point in time. This may result in non-*bona fide* orders (i.e. which the HF Traders intended to cancel or modify), being converted into trades, if such orders are present in the system when the exchange matches orders. Consequently, genuine orders will have a greater probability of execution. In theory, this would result in lower HFT executions, which would increase their order-to-trade ratios and the risk of breaching the Order-to-trade Penalty Rule, which would therefore act as a

---

[76] Eric Budish *et al*, *The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response*, 130:4 Q.J.E. 2015; Currently the most widely-used trading mechanism in financial markets is the "*continuous double auction electronic order book with time priority*". This method is continuous and execution priority is assigned based on the price of quotes and their arrival order. J. Doyne Farmer, *Review of the benefits of a continuous market vs. randomised stop auctions and of alternative Priority Rules* (policy options 7 and 12) c1, 28 March 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289050/12-1072-eia11-continuous-market-vs-randomised-stop-auctions.pdf; However, a form of batch-auctions are implemented by the BSE and NSE for opening and closing sessions; *See* Discussion Paper *supra* note 7.

[77] McPartland *supra* note 23, at 22.

deterrent to HFT. Another version of the batch-auctions is an order-randomization batch auction where orders are randomized (not the trade-matching point within the interval) before being executed. For example, ICAP's EBS introduced what it calls a "*latency floor*" on certain trades where orders are bundled into small batches and their place in the queue would be randomized i.e. not based on time-priority.[78] However, it may be possible to overcome order randomization by submitting a larger number of orders so that more HFT orders make it into every batch. Therefore, order randomization may need to be implemented in tandem with a speed bump.[79]

Maximum Order-to-Trade ratios or Execution Throttles: Execution throttles are measures which prevent HF Traders from exceeding a set order-to-executed trade ratio i.e. ensuring that at least one trade is executed for a set number of orders issued by the trader. Unlike the current '*Order-to-Trade Penalty Rule*' which allows traders to exceed prescribed ratios subject to penalties, the execution throttle would not allow the trader to issue orders in excess of the prescribed ratio.[80] Currently, the NSE has prescribed a throttle to prevent algorithms malfunctions.[81] Going further, the attempt in the Discussion Paper is geared towards prevention of volume-based market manipulation (and not merely algorithm malfunctions) and is expected to increase the likelihood of a viewed quote being available to trade. However, this measure is blunt, given that it seeks to prescribe a fixed quantitative rate regardless of the legitimacy of the underlying trading strategies.

Separate Queues for Co-located orders and non-co-located orders: In furtherance of a consultative effort to revise co-location rules in 2013, SEBI proposed in the Discussion Paper to implement an order handling architecture, where orders would be segregated into two separate queues for co-located and non-co-located orders. Validated orders from each queue would be time-stamped and forwarded based on a round-robin methodology i.e. orders would be picked up from each queue alternatively. The only situation where two orders from the same queue would be executed one after another

---

[78] Wanfeng Zhou and Nick Olivari, *Exclusive: EBS Take New Step to Rein in High-Frequency Traders*, REUTERS (Aug. 23, 2013), http://in.reuters.com/article/us-markets-forex-hft-idUSBRE97M0YJ20130823.

[79] Jacob Adrian *supra*, note 75.

[80] The CFTC contemplated such measures which would inform a trader and the exchanges if the prescribed rate has been exceeded; CFTC, *Concept Release on Risk Controls and System Safeguards for Automated Trading Environments*, 6351-01-P CFTC 17 CFR Chapter I RIN 3038-AD52, ¶96 at 83, www.cftc.gov/ucm/groups/public/@newsroom/documents/file/federalregister090913.pdf.

[81] Mobis Philipose, *Algorithmic trading: Curbing the risks involved* (In the Money: 2016), http://www.livemint.com/Opinion/ng7YwcspZXIqmOtFab9BkK/Algorithmic-trading-curbing-the-risks-involved.html

(without the exchange executing an order from the other queue in between these two orders), is if the other order-queue is empty. Until a valid order arrives in the empty queue, orders can be picked up sequentially.[82]

Review of Tick-by-Tick data feed: Part II of this Article highlighted that data feeds provided by exchanges should be equitably distributed and accessible. In furtherance of this objective, I recommended in Part IV of this Article that differentials in data feeds should not be permitted. However, SEBI is considering a more fundamental issue i.e. whether exchanges should give every piece of market information. This refers to Tick-by-Tick ("**TBT**") data feeds provided by exchanges which provide details of additions, modifications and cancellations to orders, and trades on a real-time basis. These can be used by HF Traders to virtually recreate the order-book whilst most ordinary traders either cannot afford to buy access to these feeds, or properly analyze these feeds, which creates information asymmetry.

In this regard, SEBI proposed that exchanges should only provide '*Structured Data*' which would contain the only the top 20-50 bids, asks, market depth, etc. to all market participants, either at prescribed time intervals or in real-time. This measure is probable far too regressive to seriously consider. I believe that exchanges need to be fully transparent and should disclose all data available to it. The focus instead, should be on measures (such as prohibiting preferential or prohibitive pricing, improving public dissemination systems, etc.) that enhance access and reach to the public.

These proposals cover the chief regulatory options that are already in the contemplation of regulators and markets across the globe. In addition to these proposals, the following measures may be considered:

Securities Transaction Tax: In the 1970's, Tobin called for a tax on securities transactions ("**STT**") to throw "*sand in the wheels*" of international trading markets.[83] This was aimed at encouraging long-term, value based investments, since the effect of STT on such investments would be negligible;[84] though some consider this to be an unnecessary economic impediment.[85] It also has the dual benefit of, like other prohibitive taxes such as

---

[82] Co-location Discussion Paper, *supra* note 15.

[83] This was first proposed by Keynes in 1936 reduce destabilizing speculation in equities by Keynes and later, in 1978, by Tobin in relation to destabilization of currency speculation; Edward Sun and Timm Kruse, *Optimal High-Frequency Trading with Financial Transaction Tax,* https://editorialexpress.com/cgi-bin/conference/download.cgi?db_name=CEF2015&paper_id=71.

[84] Kavaljit Singh, *India introduces securities transaction tax*, Counter Currents (Jul. 20, 2004), http://www.countercurrents.org/eco-singh200704.htm.

[85] *See* Tyler Durden, *First Ever High Frequency Trading Transaction Tax Introduced In Italy*, Zero Hedge, February 9, 2013, http://www.zerohedge.com/news/2013-09-02/

Cigarette taxes, discouraging unwanted activity and earning revenue at the same time.

India already imposes STT which applies equally to HFT as it does to ordinary trading. In contrast, the French imposed an HFT specific tax in 2012 on modified and cancelled orders for securities of large public companies, which was the first of its kind.[86] Italy too imposed a tax in 2013 on HFT, in addition to ordinary STT. For this purpose, the Italian tax differentiated between HFT and ordinary trading, and applied STT to rapid-fire trades (*i.e.* trades generated, modified or cancelled within intervals of 500 milliseconds (or less)), where the sum of such trades exceed 60% of the total orders of a particular trading day.[87]

This has recently gained favour in the E.U.[88] and the U.K.[89] In line with this European trend, Hillary Clinton, in her Presidential campaign proposals, also promised to tax HFT cancellations, believing them to be risky and harmful practices, which should not be allowed to hide under the cloak of risk-management practices.[90]

Minimum Tick Sizes: Minimum tick size ("**MTS**") is the smallest pricing increment by which the price of a listed security can be improved. To illustrate: if one rupee is the MTS, increments in paise are not allowed. The

---

first-ever-high-frequency-trading-transaction-tax-introduced-italy. [Zero Hedge is a conspiracy/activist blog, whose editors/writers collectively use the pseudonym Tyler Durden to maintain anonymity. This refers to a character in the movie "*Fight Club*", a mysterious extremist who launches "*Project Mayhem*" to erase debt by bombing buildings used by credit card companies to keep records.]

86 Maria Coelho, Dodging *Robin Hood: Responses to France and Italy's Financial Transaction Taxes*, July 17, 2014, https://www.sbs.ox.ac.uk/sites/default/files/Business_Taxation/Events/conferences/doctoral_meeting/2014/coelho.pdf

87 *See* Tyler Durden, *supra* note 94. Market-making, subject to certain other compliances, is exempted from this tax.

88 *See High-frequency trading is a blight on markets. Tobin tax can help*, Financial Crisis (Capital Institute Apr. 4, 2014), https://capitalinstitute.org/blog/high-frequency-trading-blight-markets-tobin-tax-can-help/; Basserdan, *A Tax to Kill High Frequency Trading* (Investors Hub Oct. 16, 2015), http://investorshub.advfn.com/boards/read_msg.aspx?message_id=80680768

89 *See* The Kay Review of UK Equity Markets and Long–Term Decision Making, House of Commons Business, Innovation and Skills Committee, Third Report of Session 2013–14, http://www.publications.parliament.uk/pa/cm201314/cmselect/cmbis/603/603.pdf. (Recommending that the UK Government should consider the viability, benefits and risks of an FTT on HFT)

90 Jennifer Epstein, *Hillary Clinton to propose high-frequency trading tax, Volcker rule changes* (Bloomberg.com/politics Oct. 8, 2015), http://www.bloomberg.com/politics/articles/2015-10-08/hillary-clinton-to-propose-high-frequency-trading-tax-volcker-rule-changes.

U.S.,[91] Europe[92] and Indian exchanges have prescribed MTS; in fact, the BSE is targeting HFT by increasing MTS for certain securities, since MTS benefits HFT by allowing HF traders to easily improve quoted prices.[93]

Given the above, a greater MTS should reduce HFT opportunities by reducing pricing options available to algorithmic traders. By ruling out finer pricing increments, orders will get clustered at certain price points i.e. there will be increased liquidity at such price-points. However, Yao and Ye disagree; they believe that a higher MTS takes away non-algorithmic trading options to complete with algorithmic traders based on price, since the likelihood of both kinds of traders quoting the same price is increased (due to the lack of options). Therefore, HFT would be favoured in time-priority based dead-lock resolution.[94] This would increase speed-based competition and take away price-based competition.

V. Who Should Ride The Regulatory Bicycle?

Parts II, III and IV of this Article address the '*what*', '*why*' and '*how*' to regulate HFT. This section explores '*who*' should be regulating HFT. Currently, as discussed in Part III, SEBI has heavily delegated its regulatory responsibilities to the exchanges. This allows it to regulate the securities market from the vantage point of the exchanges, being the point of intersection of all market-participants. However, investor associations have alleged that such delegation is against the letter and spirit of securities law.[95] This issue was brought to light by whistleblower allegations that the NSE is/has colluded

---

[91] *See* Maureen O'Hara *et al*, *Relative Tick Size and the Trading Environment*, December 2013 at 2, n.4, https://www.sec.gov/spotlight/investor-advisory-committee-2012/wallman-roper-iac.pdf.

[92] *Id*.

[93] Palak Shah, *BSE increases minimum price movement of stocks and Sensex futures to attract more volumes* (timesofindia-economictimes Dec. 2, 2011), http://articles.economictimes.indiatimes.com/2015-01-05/news/57705327_1_sensex-futures-destimoney-securities-tick-size.

[94] Chen Yao and Mao Ye, *Tick Size Constraints, Market Structure, and Liquidity*, December 28, 2013 (draft), at 33, 34, https://www.aeaweb.org/aea/2014conference/program/retrieve.php?pdfid=842.

[95] Sundaresha N. Subramanian, *Investor Association Moves House Panel on Algorithm Trades*, Oct. 1, 2015, http://www.business-standard.com/article/markets/investor-association-moves-house-panel-on-algorithm-trades-115100100703_1.html. An investor association has also filed a Writ Petition against SEBI, in this regard. *See Intermediaries And Investor Welfare Assn. (India)* v. *SEBI*, WP (C) No. 5082 of 2012, decided on 28-3-2016 (Del); *See also* Mobis Philipose, *Has Algorithm trading hurt investors*, (In the money: Jun. 2016), http://www.livemint.com/Money/5BPyj4B5tET3O8ruIzY8BK/Has-algorithmic trading-hurt-investors.html.

with traders to manipulate the stock markets.[96] The whistleblower claims that bribery in the NSE is rampant and that the management and promoters of NSE unfairly favored a trading company, of which the NSE was the second largest shareholder.[97] Similar concerns have been expressed in other jurisdictions as well.[98] If that were true, is it not dangerous to allow the exchanges to regulate HFT?

The exchanges that should be protecting investors have been allowed to become profit-making bodies, which can have direct physical relationships with certain traders (co-location). Their profitability and the compensation of their management is often contingent on trading volume.[99] HFT brings the most volume and naturally, there is an expectation of bias. Given this in-built conflict of interest in market structure, it may not be wise to allow exchanges to regulate the very activity that it promotes and profits from. While some would simply eliminate the self-regulatory status of exchanges,[100] I believe that the focus should be on greater oversight by SEBI and on checks and balances to ensure that HFT is not allowed to flourish unrestricted.

---

[96] This is based on an anonymous whistleblower's letter made public last year, which alleges that the NSE allowed co-location services on a preferential basis and inside information to an HF Trader, which allowed the trader to exploit inherent loopholes in the co-location system and cheat the market. *See* Sucheta Dalal, *Blowing the whistle on manipulation in NSE* (Jun. 19, 2015), http://www.moneylife.in/article/blowing-the-whistle-on-manipulation-in-nse/42337.html. This letter was made public by Sucheta Dalal it her article in Moneylife, which claimed that no action was being taken by the NSE to investigate the matter. The NSE filed a defamation suit against Ms. Dalal and her editor at Moneylife, in relation to her article, which was dismissed by Justice G.S. Patel in September, 2015. *See National Stock Exchange of India Ltd.* v. *Moneywise Media (P) Ltd.*, 2015 SCC OnLine Bom 4790: (2015) 132 SCL 312 (Bom).

[97] This is not true *per se* as NSE indirectly held 26% of the trader through Dotex International Ltd. a wholly owned subsidiary of NSE. Therefore, though it controlled 26% of Omnesys shares, it was not a shareholder of Omnesys. *See* National Stock Exchange of India Ltd., In re, 2014 SCC OnLine Comp at 37. The letter also suggests that once co-location was made multi-cast, the traders' market share fell off the charts (since it could no longer cheat the system) and the NSE sold its stake in to Reuters. *See* Sachin Mampatta, *NSE, Others Sell Stake in Algo-Venture Omnesys*, Sept. 16, 2013, http://www.business-standard.com/article/markets/nse-others-sell-stake-in-algo-venture-omnesys-113091600641_1.html.

[98] Lewis, *supra note* 3.

[99] *MCX Stock Exchange Ltd.* v. *National Stock Exchange of India Ltd.*, 2011 SCC OnLine CCI 52.

[100] Stanislav Dolgopolov, *High-Frequency Trading, Order Types, and the Evolution of the Securities Market Structure: One Whistleblower's Consequences for Securities Regulation* (May 8, 2014), University of Illinois Journal of Law, Technology & Policy, Vol. 2014, pp. 145-175, 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314574; [quoting Haim Bodek.]

VI. Findings & Recommendations

The Discussion Paper explores concerns relating to market quality, integrity and fairness arising from HFT and seeks to address these concerns with its proposals. While I concede that it is merely a preliminary step in the process of revising SEBI's regulatory framework, it does not add much value and is not much more than a general reiteration of measures and mechanisms, currently under the consideration of other stock exchanges and regulators. Its key failings are on account of the fact that it does not contain specifics of the proposals; or give details of the nature, scope and extent of the problems faced by Indian markets; is not grounded on India focused empirical evidence; and does not provide an implementation plan for any of its proposals. This has resulted in a *prima facie* examination of these proposals in vacuum. Nonetheless, and subject to the over-arching requirement to support each recommendation with robust economic research, the following recommendations best meet the objective of the Discussion Paper:

- Given the concerns discussed in Part V above, deeper involvement of SEBI may be critical in regulating HFT. If SEBI wishes to delegate regulatory powers to the exchanges, it should require prior SEBI approval to rules framed by the exchanges before they are implemented. As recommended above in Part IV (in relation to co-location), I recommended that SEBI may consider requiring exchanges to seek SEBI approval before such exchanges implement any new rules. Alternatively, SEBI may consider a separate licensing regime for HF Traders, which would impose continuous '*fit and proper*' criteria to be maintained by licensees. For example, the U.S. Financial Industry Regulatory Authority ("**FINRA**") plans to issue non-public report cards to HF Traders based on the legitimacy of their trading strategies.[101]

SEBI may also consider setting up an independent supervisory body to supervise HFT, which function under the aegis of SEBI. This would body should be given the power to seek information from algorithmic traders, on a confidential basis, including descriptions of HFT strategies and details of trading activity, especially details of when these algorithms and strategies were implemented.[102] This body should constantly monitor the markets for violative, fraudulent and manipulative activity and report any actual or suspected fraudulent, manipulative or illegitimate activities to SEBI. In this

---

[101] David Michaels, *Wall Street to Get Graded on How Much Spoofing It's Facilitating*, Jan. 5, 2016, http://www.bloomberg.com/news/articles/2016-01-05/wall-street-to-get-graded-on-how-much-spoofing-it-s-facilitating.

[102] §1(a), HFTA, *supra* note 9.

regard, Dolgopolov suggested, as a possible alternative to the U.S. securities market structure, to have exchanges delegate enforcement and surveillance functions to an independent third party.[103] For example, Direct Edge and NASDAQ have voluntarily delegated some surveillance functions on their equity markets to the FINRA.[104]

- Amongst the measures proposed by SEBI, MRT, speed-bumps and execution throttles appear promising, for the time being. Of these, execution throttles should have the fewest risks and unknowns, given that it is an extension of the existing '*Order-to-Trade Penalty Rule*'. Further, execution throttles only restrict trading strategies while a MRT or speed-bump could possible entirely negate the benefits of co-location, and are therefore likely to be better received by the market. However, SEBI would have to determine an appropriate cut-off level for the throttle which will involve the delicate exercise of distinguishing between legitimate and illegitimate throttle ratios.[105] To begin with, SEBI should start with a conservatively high throttle-rate and target only serious manipulative strategies. After observing the throttle in practice, it may consider lowering the throttle-rate, or even providing for variable rates for different cases, situations or securities, if required.

However, SEBI will have to think this measure through, since currently the Discussion Paper does not explain how the throttle will be implemented; *e.g.* it does not specify what is to happen when a trader hits the throttle limit. At this point, if such trader cannot issue fresh orders, his order-to-trade ratio cannot be brought down and he would effectively be in limbo.

- Batch-auctions and randomization would increase pre-execution order exposure and significantly reduce, if not eliminate, the speed-advantages enjoyed by algorithmic traders and therefore negate the value of co-location. A review of the research on associated effects of these measures, reveals conflicting results. In 1998, researchers significantly concluded that the call market method was half as volatile as the continuous auction method, including in high volume stocks, on the Taiwan Stock Exchange. Further, they found that it did not impair liquidity and price discovery in the call market appears more

---

[103] Dolgopolov, *supra* note 102.

[104] See, e.g., Press Release, *Direct Edge & Fin. Indus. Regulatory Auth., Direct Edge Selects FINRA for Market Surveillance* (May 22, 2013), http://www.finra.org/Newsroom/NewsReleases/2013/P265419.

[105] SEC Chair Mary Jo White, *Enhancing Our Equity Market Structure*, Speech at the Sandler O'Neill & Partners, L.P. Global Exchange and Brokerage Conference, New York, N.Y. (June 5, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370542004312.

efficient than in the continuous auction market.[106] Similarly, other studies between then and now associate the presence of call auctions with reduced volatility.[107] Given that these studies are conducted on different exchanges with different market characteristics, the most relevant piece of research is Camilleri's 2015 study on the effects of the opening and closing call-auctions at the NSE, which indicated increased volatility during the auction period (though he Camilleri declared that the increase was statistically insignificant).[108] Assuming that this is true (and which will need to be confirmed across other exchanges and platforms as well[109]), batch-auctions may be a viable option. However, the revised market structure should be well thought through and supported by robust research.

- With respect to separate queues for co-located and non-co-located traders, there is likely to be heavy opposition from co-located traders; though as SEBI rightly pointed out in the Discussion Paper, co-locaters would still receive data feeds faster due to their proximity to the trading servers. This, coupled with the ability to make trading decisions faster than ordinary traders, would allow HF Traders to retain their competitive advantage. However, SEBI should note that there may be ways for HF Traders to work around these queues; the Association of National Exchanges Members of India (ANMI) pointed out that non-colocated order queue can be gamed by issuing orders proximity hosting locations (a variant of co-location offered by stock exchange, where traders can set up their systems outside, but close to, the exchanges premises, with direct connectivity with the trading platform).[110] This would allow HF Traders to use the speed benefits of co-location to receive and process market information and thereafter, issue non co-located orders from the proximity location

---

[106] Rosita Chang *et al, The Effects of Trading Methods on Volatility and Liquidity: Evidence from the Taiwan Stock Exchange,* (Aug. 1998), http://www2.hawaii.edu/~rheesg/Belgrade/Taiwan/TSEfinal.pdf

[107] Silvio Camilleri, *The Impact of Stock Market Structure on Volatility: Evidence from a Call Auction Suspension, University of Malta*, March 23, 2015, http://www.sciedu.ca/journal/index.php/ijfr/article/viewFile/6700/4014.

[108] *Id*.

[109] Haas and Zoican (2016) recently found that batch-auctions did not have stock-specific impacts and could therefore be implemented exchange wide; Marlene Haas and Marius Zoican, *Discrete or continuous trading? HFT competition and liquidity on batch auction markets*, February 26, 2016, http://people.stern.nyu.edu/jhasbrou/SternMicroMtg/SternMicroMtg2016/Papers/36.pdf. This should be confirmed in the context of Indian markets.

[110] ANMI, Response to SEBI Discussion paper on Strengthening the Regulatory framework for Algorithmic Trading & Co-location (Aug. 30, 2016), available at http://www.anmi.in/pdfs/SEBI-Discussion-paper_Algorithmic-Trading_Co-location_29062016.pdf.

servers (which may be placed in the non co-location order queue). Further, HF Traders can overcome separate queues by placing multiple orders in both queues and once either order is executed, cancelling the other order. This would add noise to both trading and market data and load on the exchange's servers. Furthermore, HF Traders may be to develop predatory algorithms to take advantage of the non co-located order queue.[111] However, if an MRT is imposed during which orders cannot be cancelled, at least the concern of HF Traders placing orders in both queues will be solved.

- An HFT specific tax is not advisable, since India already imposes a generic STT and economically de-incentivizes excessive trading. Further, it would probably wipe out HFT's slim profit margins.[112] It also has the disadvantage of not being able to differentiate between legitimate and unfair or manipulative HFT practices.
- An HFT-targeted MTS can be implemented with caution, possibly in tandem with some form of time-based speed breakers. This measure in particular, will depend on supporting economic research and an analysis of the associated effects on transaction costs, market depth, liquidity and volatility.

Lastly, a word of caution. It is possible for each of these measures to have widespread disruptive effects on the markets, including driving trading volume overseas.[113] The complexity of these measures (depending on the final implementation plan) may result in increased operational costs and risks. Furthermore, some of its proposals *e.g.,* randomized speed-bumps are based on experiences of market microstructures, which may have completely different dynamics and characteristics than the Indian markets.[114] All of these will have to be kept in mind when SEBI finalizes its revised regulatory framework.

VII. Concluding Remarks

Given the explosive growth of HFT and the consequent paradigm shift in trading fundamentals, there is palpable regulatory unease in the securities

---

[111] Association of National Exchanges Members of India, *Comments on Proposal on Co-location / Proximity hosting facility offered by the Stock Exchanges*, May 31, 2013, http://www.anmi.in/pdfs/Letter%20to%20SEBI%20-%20Comments%20on%20Proposal%20on%20Co-Location%20-%20Proximity%20hosting%20facility%20offered%20by%20the%20Stock%20Exchanges.pdf

[112] Lee Sheppard, *supra* note 36.

[113] ANMI, *supra* note 112.

[114] ANMI, *supra* note 112.

markets. SEBI has the second-mover's advantage and should consider a pre-emptive upgrade on the lines discussed above, especially considering the frequency, variety and severity of risk and violations associated with HFT.

Dolgopolov rightly pointed out that technological developments cannot be reversed, and the search for regulatory arbitrage and loopholes cannot be stopped.[115] Therefore, these measures will have to be flexible enough to react to arbitrage as it happens. If SEBI implements the recommended measures in Part V above (subject to thorough India specific economic research and a well thought through implementation plan), it may well be successful in restoring the faith of the public investors in the integrity of the Indian securities markets.

[115] Dolgopolov, *supra* note 102.

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 a*t 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.

The Politics of Pirates: Jonas Andersson Schwarz's "Online File Sharing"

Gautam Bhatia[†]

The international debate over file-sharing is defined by polarities. Consider, for example, the confrontation between The Pirate Bay and the Swedish legal authorities, as documented in the film *TBP-AFK*.[1] The Pirate Bay is an online website facilitating peer-to-peer file-sharing, and the uploading and downloading of torrent files. The Pirate Bay has long been embroiled in numerous legal cases turning upon its facilitation of copyright violations. These include the arrest and imprisonment of its founders, the website itself being taken down, and its domain name being seized.

Some view this conflict as a battle for internet openness against the efforts of the film and music industry to bring about a second Enclosure Movement, this time against the worldwide digital commons. Others, however, consider it to be a legitimate law-enforcement operation against wilful facilitators of large-scale copyright infringement. Such characterization of the issue – as a zero-sum game – was (perhaps unwittingly) affirmed by the European Court of Human Rights, when it heard the appeals of the Pirate Bay founders against the hefty fines and prison sentences imposed against them. The ECHR, too, framed the issue as a clash between the interest of the freedom of expression (in sharing information) and the interest of protecting the rights of the copyright holders.[2] The Court stressed the importance of copyright, denigrated the strength of the expression interest because of its "apolitical" nature, and echoed the Swedish Courts in taking a dim view of the applicants' refusal to remove the torrent files despite being asked. In so doing, it too placed itself firmly on one side of a division that now appears almost Manichean.

---

† Practising Advocate, Delhi; BCL, M.Phil. (Oxford); LLM (Yale).

1 http://watch.tpbafk.tv/, visited on February 22, 2014.

2 Neij and Kolmisoppi v. Sweden, Eur. Ct. Human Rights, Feb. 19, 2013.

In his book, *Online File Sharing*, published in early 2014, Jonas Andersson Schwarz argues that this dichotomy is a deeply flawed way of understanding the file-sharing dispute. Using tools from critical theory and political philosophy, Schwarz aims to break down the binaries, and to demonstrate that the reality of file-sharing is simply too complex, and too nuanced, to be captured by way of dualities, no matter which side projects them. To the intellectual defenders of the Pirate Bay and other such operations, who base their case on values of openness, freedom and unlimited access to culture, Schwarz presents a series of internal contradictions that remain unresolved under all present models; on the other hand, the defenders of copyright must face up not only to an absence of credible evidence of harm, but also to the reality that unquestionably *legal* enterprises like Spotify have been built upon the concept and tools of file-sharing.

The task is particularly important because – as our overview of the ECHR discussion indicated – the debate right now isn't so much a debate as two sets of participants talking past each other. At the heart of the issue is the crucial – and often overlooked – point that freedom has never been a value-neutral term. As critical Marxist and feminist theorists of all stripes have pointed out over the years, it is socially and normatively constituted. Ultimately, the meaning of freedom depends on the default position that you take.[3]

For file-sharers, that default position is unhindered exchange of cultural products. And if that is the definition of freedom, then by stipulation, copyright and IPRs are freedom-inhibiting. On the other hand, if freedom is the freedom to exploit the fruits of your created (or validly purchased) product, then file-sharing assaults that freedom. Without a shared language or background, it isn't even possible to disagree.[4] Shwarz's project is to bring to the fore the shared context that he believes exists.

As the first point of departure, Schwarz calls into question file-sharers' positioning of themselves as pursuing an activity *alternative* to the capitalistic mode of production, distribution and consumption of culture. Schwarz points out that the demand that file-sharing is designed to sate is created and sustained by the very film and music industries that it sets itself against. Thus, *"file sharing, as a means of cultural exchange, can therefore never be equated simply with resistance – because it thrives on the same capitalist system of cultural exchange that it forms part of."* (163) In other words, file-sharing is *internal* to a capitalist structure. A modified account of the

---

[3] See, e.g., G.A. Cohen, *The Structure of Proletarian Unfreedom*, 12(1) Phil & Pub Affairs 3 (1983).

[4] Ranciere, Disagreement (1999).

activity, then, would present it as what Schwarz calls "escalationist" – that is, file-sharing is about "*harnessing desires generated by capitalism but implementing them in ways that are not capitalist*." (21) The music and the films and the other cultural products that are circulating for consumption are generated by capitalism, but it is the *manner* of their circulation – free or unregulated, whichever word you prefer – that is the very antithesis of capitalism.

Yet even when it comes to implementation, the issue is complicated. File-sharers split with IP-solicitous media corporations on a particular conception of democracy, or the values it represents: openness, participation and freedom. File-sharers see a right to participate in culture as central to their conception of democracy. IP-solicitous media corps, on the other hand, believe that the producers' rights to benefit from their work, in an overall atmosphere that fosters incentives for innovation, is fundamental to democracy. Ultimately, each version engages in a circular reciprocity with the other. Schwarz himself frames this issue in the context of the "Pandora problem": the nature of the internet is such that even the smallest leaks have the potential to go viral. Thus, to stop some leaking, one most stop *all* leaking. But to stop all leaking would require a totalitarian regime of control. Consequently, the only legitimate alternative is complete freedom. Yet *this*, argues Schwarz, creates its own "*undemocratic distributions, taking the form of extreme, long-tail curves*." (23) The long-tail curve refers to a distribution where the unregulated internet sees such a vast amount of information that – given finite human energies and attention-spans, a minute few cultural/artistic works achieve great popularity, while a "long tail" fades into anonymity and insignificance. Schwarz questions whether – from the creator's perspective – this is very different from the extant model, where record companies use revenues from a few certain earners to bankroll a greater number of "hopefuls", some of whom make it, and most of whom don't.

But whatever the normative implications of the argument, it isn't even true *descriptively*. The argument ignores the "*the highly institutionalized protocol-governed structure of the Internet and assumes it to be akin to a natural, premodern state of similarly free flows of culture*." (30) Indeed, as Schwarz goes on to demonstrate throughout the book, the freedom-and-openness premises upon which file-sharing is based rely upon a whole host of assumptions that are by no means universally applicable: a social-welfare State in the background, easy internet access and internet literary in the foreground, and – especially in recent years – sophisticated computer skills to access

information on the darknet. Thus, file-sharing is constituted by both libertarian and technocratic dimensions that are in tension with each other.

Yet the tensions don't exist only at the level of theory. Comparing, specifically, Napster – which was said to be the prime example of a "disruptive" internet innovation with what follows, Schwarz points out that *"many of the things that Napster was said to disrupt – the album as an art form, unit pricing of online music – have later been recaptured by newer business models such as iTunes and Spotify."* (63) Spotify, indeed, began life as an illegal, p2p service, which then transformed itself into a legitimate company by persuading media companies to latch on to the concept.

This leads Schwarz to question whether *"file-sharing acts to displace business models entirely or merely acts as a conduit for more efficient ways to perform consumerism."* (63) In other words, to what extent can file-sharing legitimately be considered transformative, if its models of choice exist for a time outside the law, appear antithetical to the interests of capital – but are then appropriated *by* capital? In the realm of the purely political, this would be what Gramsci called a "passive revolution" – marked by continuations and mutations, rather than ruptures, and one that proceeds within the framework of existing institutions.[5]

Schwarz's example of The Pirate Bay makes it clear how this works in practice. The attempted sale of The Pirate Bay to an entrepreneur, and subsequently, its hosting on the Swedish Pirate Party's website, with the SPP's logo, "*shows that a service such as TBP is ontologically "sticky"… it can be seen as a conservator of a mainstream cultural supply, as well as a radical opponent to the big media corporations, as a harbinger of free media distribution, or conversely, as a hedonist absorption of mere self-gratification – having commercial capacities and political clout.*" (156)

Reading this book left me wanting more. But just at the most dramatic moment – at the cusp of the SPP – it tails off, leaving a crucial task incomplete. For all the political aspects of file-sharing itself – and Schwarz is careful to problematize accounts that assimilate all file-sharing to political resistance by virtue of its illegal character – the SPP is an example *par excellence* of the translation of file-sharing into the *explicitly* political domain. How did the SPP understand this translation? How would a political party, that is the instantiation of the values of file-sharing, seek to resolve the inherent contradictions and tensions that we have discussed above, in its political mandate – or did it simply ignore them? What specific policy prescriptions

---

[5] Jon Bloomfield, Passive Revolution (1979).

– for IPR, internet governance and other related issues – did the SPP bring to the table as a political party, and how did these square with the abstract ethos of the file-sharing community? Was there a feedback loop between the pirate community and the pirate party? These things are left untouched by Schwarz.

For a book that sets out to ground file-sharing within critical theory and political philosophy, it is a curious omission. Nonetheless, insofar as it sets out to prove that we ought not to take the existing debate, with its categories, as it is given to us – but rather, understand it as a battle over "ontopolitics" (156) – that is, a struggle between two sets of organizing principles for the internet, which have commonalities as well as differences – it succeeds quite well.