EasyChair Preprint

№ 382

Industry 4.0: The challenges to intellectual property in Manufacturing

Marcos Kauffman and Marcelo Negri Soares

July 27, 2018

Industry 4.0: The Challenges to Intellectual Property In Manufacturing

Abstract

The fourth industrial revolution or Industry 4.0 (I4.0) is affecting businesses of all sizes in all industries by using digital technologies to transform the innovation system. In the face of such paradigm shift current practices business models need to be adapted in view of new these new technologies which lead to smarter products and services. The workforce must also adapt and acquire new skills to master all those digital challenges.

As a consequence of this digital transformation, many questions have been raised, amongst which is the role and suitability of the existing legal tools, which may not be completely novel, but that will have been seen and dealt with in a limited scale in the past and now will exponentially increase in new dimensions.

These legal questions relate to areas such as data protection, copyright, contract law, trade secrets law and other regulatory aspects are most prominent. This article explores, in particular, the challenges related to Intellectual Property (IP), which is increasingly recognised as a paramount intangible asset influencing the companies' value, corporate strategies, and its management.

The study concludes that challenges related to IP in this new environment must be counteracted by a robust IP strategy underpinned by the contractual agreements which clearly define the ownership of IP in data exchanged in the manufacturing value chains and embodies the particular business strategy and the business model.

Keywords: Fourth Industrial Revolution; Intellectual Property; Business Strategy; Intellectual Property Strategy.

Marcos E. Kauffman
PhD Student
Centre for Business in Society – Faculty of Business and Law
Coventry University, 113A Gosford Street, Coventry CV1 5DL
kauffmam@coventry.ac.uk

Professor Dr. Marcelo Negri Soares
Professor of Legal Sciences
UNICESUMAR – Centro Universitário de Maringá
Av. Guedner, 1610 - Jardim Aclimacao, Maringá - PR, 87050-900, Brazil
negri@negrisoares.com.br

1. INTRODUCTION

The fourth industrial revolution, also known as Industry 4.0 (I4.0), is described as a "digital revolution" in which the deployment of the Internet of Things (IOT) and the interconnecting of all things and businesses in the manufacturing industry lead to "blurring the lines between the physical and digital spheres" (Schwab, 2016). This shift in paradigm brings the prospect of disrupting global manufacturing industry, while potentially leading to substantial economic growth and prosperity.

The available literature indicates that the I4.0 levels of integration and data exchange between businesses will lead to extensive organisational consequences resulting in risks and opportunities to manufacturing business (Bauernhansl et al., 2014; Botthof, 2015). Furthermore, it also recognises that established manufacturers will be required to re-evaluate and innovate their Business Models (BM) in order to stay competitive (Jonda, 2007; Kagermann et al., 2015; Loebbecke & Picot, 2015), as the phenomenon will lead to new ways of creating value, disrupting the current supply chain structures (Kagermann et al., 2015).

This paper evaluates the changes taking place in this digital transformation and their impact and challenges to IP. As such, this article aim to do so by exploring in the concept of I4.0 in section 2; the challenges to IP in manufacturing business in section 3; the current legal stance on data ownership in IIOT is covered by section 4; In section 5 we offer a set on suggestion to help manufacturers address the challenges to IP; and finally, in section 6 concludes this work.

2. INDUSTRY 4.0

The term industry 4.0, despite its popularity, struggles to achieve a clear definition. In fact, even the "Industrie 4.0 Working Group", which was created by the German government with the objective of promoting and developing I4.0, arguably only provides a description of the I4.0 vision and the basic enabling technologies and applications, but not a clear definition (Kagermann et al., 2015).

Furthermore, even though the I4.0 has, since its conception, moved up the agenda for universities, companies and governments, the definition provided by the myriad of publications in both academic and practitioner domains has varied massively and accomplished little (Bauernhansl et al., 2014). Therefore, we begin with an overview of a key concept at the core of I4.0, the Internet of Things (IOT).

A simple way to explain the IOT is to use the wide spread well understood technological concept known as the Internet. The Internet is comprised of a global network of interconnected computer servers which can be accessed simultaneously by multiple users via a range of endpoint devices (mobile phones, laptops, tablets, PCs, etc.). These connected users access the internet and utilise the information contained in those servers.

The next step, then, is to expand the concept of connecting these users and imagine that everyday objects containing embedded sensors capable of communicating information, are also connected to networks and to the Internet. Such objects can include mobile phones, wearable devices, washing machines, light bulbs, vehicles, etc. In an industrial setting, these devices include robots, machines, jet engines, etc.

All of these "things" are now "smart" objects which are capable of communicating and exchanging data with the wider network about itself (e.g., what, where, when, temperature, pressure, acceleration, speed, status, etc.), making this network the Internet of Things.

Thus, with a basic understanding of IOT, one can relate to the concept of I4.0, which can be characterised as a form of "Industrial Internet of Things" (IIOT) (Leber, 2012). This alludes to the IOT applied in the industrial context, as already mentioned above in the form of connected robots, machines, jet engines, other equipment, etc.

This characterisation is similar to the one made by Kirazli & Hormann (2015, p.864), which provides the following definition for I4.0:

> "***Industry 4.0 is the systematic development of an intelligent, real-time capable, horizontal and vertical networking of humans, objects and systems.***"

Therefore, I4.0 can be characterised as the deployment of IIOT within the boundaries of an individual business, also known as "Vertical Integration", as well as, across the value chain, industry or even cross-industry, also known as "Horizontal Integration" (Kagermann et al. 2015).

Of particular importance to this article, the data generated by the humans, objects and systems will be uploaded at different frequencies depending in the use case and utilised in conjunction with other data sets from other devices and other businesses in the manufacturing value chain connected in the IIOT ecosystem.

This will typically include a number of different stakeholders, ranging from device and sensor manufacturers, software and application companies, as well as, infrastructure and data analytics companies. These companies will be involved, not only in the manufacturing process, but rather, in the process of collecting, transferring, storing and analysing data which give rise to challenges to IP in the form of data, knowledge and information protection and ownership.

Concluding this section, we note that the deployment of IIOT within individual businesses can undoubtedly lead to operational gains and other benefits such as increased speed, control and overall productivity.

It is argued, however, that the deployment of IIOT across value chains and industries, crossing individual business boundaries, will pose particular challenges to IP, especially with regards to data and knowledge sharing. To this end, the next few sections will explore the key challenges to IP in manufacturing businesses embarking on the digital transformation

journey, as well as, the need for the businesses to adapt their approaches to IP strategy in order to address some of these challenges and secure value.

3. THE CHALLENGES TO IP IN MANUFACTURING

Historically, the focus of IP practitioners working on the manufacturing industry has been to use IP rights as the traditional "Shield and Sword" to protect the physical things, devices, structures and even the configuration of physical systems, physical outputs, or the operation of physical systems, physical connections, etc.

However, with the implementation of I4.0, the focus needs to be expanded to the IP protection of intangible things such as methodologies, the configuration of virtual systems, data ownership, handling and storage, processing algorithms, brand recognition, etc.

It is argued that the digital transformation resulting from the implementation of I4.0 challenges the current understanding and use of IP protection and commercialisation strategies in manufacturing. This in turn, justifies the development of new approaches that will be better suited to the rapidly changing, highly integrated business networks.

Such position was clearly made in the Made Smarter Review issued in the second half of 2017 which recognises the importance of IP as a key intangible asset which can make up over 80 percent of the value of a company (Ocean Tomo 2015) and many times is the key to securing a competitive advantage in globalised manufacturing value chains.

Furthermore, the review which was commissioned by the UK government and led by Professor Juergen Maier (CEO Siemens UK) also recognised that IP theft is one of the key threats related to the digitalisation of businesses (Made Smarter. Review 2017). The review also points out that due to the intangible nature of IP which is typically found in digital information it is susceptible to digital piracy.

Therefore, it is argued that as a result of the implementation of interconnected communications and the increased utilization of standardised application programming interfaces (APIs) to increase inter-company collaboration, manufacturing businesses are faced with the challenging task of carefully considering how to protect their IP, whilst at the same time how to facilitate interoperability between businesses in the value chain.

The next few sections will explore one of the key challenges for IP in the face of this new highly collaborative and interoperable environment emanating from I4.0, the protection and ownership of data.

3.1. THE INCREASING VALUE OF DATA

In the typical, pre-I4.0 environment, IP strategies have focused on protecting hardware and software which processes and stores data. However, the data itself, especially in the newly interconnected environment, is of high value and worthy of protection. This value emanates from the ability to perform analytics on data from integrated smart objects, generating new knowledge which can be the source on competitive advantage and innovation. As such, the rights to these data sets, as well as the bigger aggregated data sets and the knowledge and insights emanating from them, are of critical importance to businesses.

Data, in its more simplistic from, is typically protected by trade secrets and copyright law. Save in the case of databases under EU jurisdiction via the "sui generis" protection scheme provided by the EU Directive 96/9/EC (Directive 96/9/EC, European Parliament and of the Council (March 11, 1996)).

Although the above methods of data protection can be useful in many circumstances, these very often fall short in scope and are considered by many not adequate DLA Piper, Rights in Data Handbook (2013). In this case, it is very likely that businesses and IP practitioners will have to resort to contractual agreements in order to govern the operation and the inter-company relations and the protection of IP in the I4.0 environment.

Therefore, it is argued that both IP practices and strategies will have to take account of the required contractual agreements surrounding data exchange, particularly addressing the types of, rights to, and licensing constructs related to I4.0 interconnected data.

4. HORIZONTAL INTEGRATION AND DATA OWNERSHIP

Due to the above mentioned increased value of data, data ownership rights have been subject to constant debate. Questions regarding whether the companies collecting, storing, transferring, sharing and analysing data has a right to the data it processes has very often been fuelled by the lack of a clearly established right to data in the EU (European Commission 2017).

This section focuses of the current legal position regarding data ownership rights in Europe and how IP and contract law are the best option for manufacturing business seeking to assert their rights over data in the IIOT environment.

4.1. RIGHTS TO DATA – PROPERTY LAW PERSPECTIVE

Property law is one of the most ancient systems of rights, which experts claim to predate the development of human language (Mattei 2000). The concept of property and ownership thereof, concerns the regulation of tangible assets scarcity, the reality of or limited resources (Malgieri 2016a). Such limit however, is atypical of the digital world where bits and bytes are rarely scarce and can easily be copied and multiplied without excluding others from the enjoyment of the same resource. This is commonly referred to as non rivalrous nature of data and a feature which can be found in certain IP Law theories (Lessig 1999). In this sense, data

ownership, at least from a theoretical perspective, is not scarce, nor rivalrous (Samuelson 1999).

One of the most important aspects, if not the most important, is the right to exclude others to possess the thing owned. This aspect goes to the core of Property Law and the concept of ownership, the right to possess (Clarke and Kohler 2005). This aspect gives rise to the first challenge regarding data ownership, the act of possessing "data", as such possession can be easily affected as the thing itself can be copied and replicated making it very difficult to exclude somebody else from using the same data, for cases with limited access due to technical protection.

This copy-ability of the thing owned is another challenge as a traditional aspect of any property right is the ability to exclude the world (Purtova, 2016). This aspect of property ownership is a key differentiator when compared with other rights such as rights under a contractual agreement as property rights are arguably stronger due to its enforceability everyone else, not just a contracting party.

A property right emanates from the law in vigour in a particular legal system and is independent of contractual agreements between parties. Nevertheless, the situation can be complex in certain jurisdictions as in the case of the EU as there is no harmonisation within the EU on property law and individual rights are determined by national legislation in each of the EU Member States. Therefore, depending on the individual national rules, there may be different solutions to the legal challenges in relation to property rights to data.

An example of this lack of harmonisation can be found between the legal position in Germany, where there has been a rather extensive debate on the issue (Hoeren 2014), and the UK, where the courts have ruled in a case that questioned the UK position on data ownership (*Your Response Ltd v Datateam Business Media Ltd [2014] EWCA Civ 281; [2014]3 W.L.R. 887*).

In summary, it can be argued that no explicit property right to data is currently available in EU legislation or case law. Therefore, it follows that in order to create such right over data would demand new law or a new interpretation of the current law. In addition, even if such law existed, there are other questions regarding data in the IIoT context such as; i) who should have such right? ii) Should the right be exclusive? iii) is this right transferable?

4.2. RIGHTS TO DATA – IP LAW PERSPECTIVE

Copyright in Data

Copyright is one of the IP rights used to protect intangibles. Nevertheless, to obtain legal protection in the form of copyright, one must satisfy the requirement for originality and creativity, both international copyright conventions which establish that only works that exceed this threshold can be granted copyright protection. However, the data collected by manufacturing businesses via machines and smart devices deployed in a manufacturing

operation is not “created” in the traditional sense as there is no artistic or literary work in the data, but rather, it is collected automatically from an individual device measuring a process parameter or its surroundings.

Such forms of automatically collected data fail to have the required creative element of copyright (Article 2 of the Berne Convention (1886), as it would be impossible to demonstrate that any artistic or literary effort has been made. Furthermore, even if such creative element was found, it would arguably be the result of the user’s efforts in generating the data. In this case, business generating as the owners of the copyright would need to grant a license to any other company using the data in the process of collecting, transferring, storing and analysing.

Furthermore, in the cases where user data is paired with the surrounding data, created by external sensor and smart objects, it could be argued that companies responsible for such devices would own the copyright; for example in measuring the weather information in a particular location or even traffic data. Nevertheless, this sort of data would not satisfy the copyright hurdles of originality or creativity.

Another copyright possibility lies in database rights, where legal protection is given based upon how the data is structured, rather than in the data itself. For database copyright, the database itself must pass the originality test i.e., there is originality in the selection or arrangement of the database contents (article 3 Directive 96/9/EC; Kemp 2014).

Alternatively, a reduced level of protection can be given where a substantial investment in the work is shown, this is known as a sui-generis right (Article 7 Directive 96/9/EC). No creativity or originality is needed here, but a sufficient level of time and effort in the structuring of data must be shown; protection can therefore even apply where a significantly large amount of data is involved.

Nevertheless, this type of protection is more likely to ensue in relation to the wider IIoT data, due to the amount of data and the time and effort involved. In any case, it is unlikely originality in the selection or arrangement of data could be shown for the database arrangements of the manufacturing data being automatically generated and collected. The sui generis right protects another party from benefiting from the result of the original investment, prohibiting the use of the whole or a substantial part of the contents.

The term of protection is only 15 years, which is shorter than for copyright, but can be renewed if a new investment is made (Directive 96/9/EC Article 10). However, this type of rights would be likely to reside with the companies storing the data and offer no rights to the manufacturer generating the data themselves.

4.3. RIGHTS TO DATA – CONTRACT LAW PERSPECTIVE

Another obvious alternative to address the lack of explicit rights to data from property law and intellectual property law is contract law, which can be used to guarantee a basic level of legal protection.

Actually, contracts are the most common method currently in use to govern the rights and control of data between stakeholders in the IIoT environment (European Commission 2016; Kemp 2014). This fact is evident in the position of the European Commission which considers contracts to be "a sufficient response" to the challenges and encourages standard agreements in certain sectors (European Commission 2017).

Contractual agreements offer a key advantage as they impose obligation and are enforceable against the other contracting parties. Furthermore, the standard of proof for breach of contract is less stringent than for breaches of intellectual property rights.

On the other hand, a disadvantage of a right to data based on contract is that, due to privity of contract, such agreement it is only enforceable against the other contracting party, and not against any other party (Kemp 2014). Thus, in a scenario relating to wearable data in complex IoT relationships between multiple parties, questions also arise in regards to which contractual agreement outweighs other terms and conditions.

Furthermore, it is important to remind ourselves that contractual agreements can be overridden by other rights contained in legislation such as personal data rights and in bankruptcy proceedings.

Having explored the current legal position and the challenges in relation to data ownership by manufacturing businesses in the IIOT environment, attention now turns to a set of alternatives on how to address the IP challenges in relation to I4.0.

5. ADDRESSING THE CHALLENGES TO IP IN MANUFACTURING

With the current rate of technological and industrial change, and the unpredictable nature of technologies involved in the I4.0 environment, a variety of techniques should be utilised in order to effectively identify and protect IP.

While there are a number of common strategies to be deployed in the area, it is important to emphasize that a one-size-fits-all solution does not exist as each individual business performs to achieve its own strategic objectives and will be set up according to a particular business model. As such, it is recommended that the various legal mechanisms be considered alternatively or concurrently, with the non-legal mechanisms as part of a comprehensive IP strategy.

IP management involves a lot more than just law and legal knowledge. Even so, IP management is very commonly left to a particular technical or legal department within the business. These departments will typically focus narrowly on the protection of the business

from potential infringement of other businesses IP and the protection from the infringement of its IP by competitors.

A manufacturer's approach to IP Strategy should be considered as part of a wider business strategy. The ambition should be to retain a competitive edge while remaining responsive and flexible so as not to stifle innovation.

The following paragraphs contain a non-exhaustive list of recommendations that are aimed at addressing some of the shortcomings highlighted in the previous sections with a view improve the position of manufacturing businesses' and their IP strategies in the I4.0 interconnected environment.

5.1. DATA SHARING PROTECTION

The success of IIOT is reliant on vast amounts of data shared and aggregated across the entire manufacturing value chain. The rights to the individual data sets, as well as the bigger aggregated data sets and the knowledge and information emanating from it, are of critical importance to businesses.

In order to address this challenge it is argued that a non-exhaustive set of with three basic actions can improve the manufacturing businesses' IP strategies and intangible assets protection in horizontally integrated data exchange within a value chain (Soares and Kauffman 2018).

I – Categorise the different data types

Manufacturing businesses should be aware of the main data types to be shared in these inter-organisational relationships emanating from I4.0 and implement appropriate measures to protect each type. In this regard, it is recommended that contractual terms between manufacturing businesses and the supply chain regulating the exchange of data should cover at least the data types listed below:

"

a) *Raw data, machine data and unprocessed data*

This is simply the big data sets that are collected from the relevant smart objects at issue in the IoT-related contract;

b) *Processed data*

This is the set of data resulting from the analysis of the raw data by any actor (suppliers, manufacturers, customers, end users) in the Industry 4.0 environment; and

c) *Input data*

This is any data that is entered by the end-users who interact with the relevant smart objects at issue (and/or their respective customers).”

(Soares and Kauffman 2018, p. 282 - 283)

5.2. IP OWNERSHIP PROTECTION

Manufacturing businesses should consider the fact that, similar to joint IP ownership clauses, data ownership and rights clauses contained in I4.0 contracts will be the subject of much negotiation. These will often be contentious negotiations, as the powers of the various parties in a value chain will influence how much each party will give away.

Nevertheless, such contracts should at least consider the following ownership, rights and licensing constructs surrounding IP: What data is subject to the contract?; What rights are allocated to which party to the contract?; What specific IP is owned or licensed to which party?; Who is the licensor and the licensee?; What is the particular business model?; What products or services or industries of use?; In what territory?; What is the term (time) of such right?; Are the rights exclusive or non-exclusive?; Is there a right to sublicense?

Manufacturers should include these constructs into the particular contractual agreements which suppliers, partners and customers. The following draft clauses are an example of an ownership clause where a smart-object manufacturer owns the raw and processed data, but the manufacturing company “the customer” receives a license to some of the data.

“The Customer acknowledges and agrees that the product Manufacturer owns all rights, titles and interest in the Equipment Data. The Customer will upon request deliver such data to the Manufacturer.

The Manufacturer hereby grants the Customer a perpetual, non-exclusive, non-transferable, royalty-free license to use, reproduce and store the Equipment Data solely to the extent required to operate Customer’s equipment.”

(Millien and George, 2016 pg. 22)

Furthermore, in case such as this involving machine generated data, it is important to provide a clear definition of data subject to the particular clause as illustrated in the following example:

"Equipment Data" means any data, metadata, logs or other information generated by the operation of the Software or the Device, but does not include any personally identifiable information, nor any information entered into the Software or the Device by the Customer's employees, agents or end-users, except to the extent portions of such information appears in anonymized or

aggregated form or in automated logs or similar records through the normal operation of the Software."

(Millien and George, pg. 22)

The above draft clauses can be adjusted to suit the different aims in relation to data ownership or rights in a particular case.

5.3. DATA OWNERSHIP PROTECTION

Due to the lack of clear data ownership protection in the EU as explained in the previous section, manufacturing businesses should be aware of the different data ownership rights in relation to inter-organisational data exchange.

Furthermore, it is argued that in order to improve the protection of IP contained in the data exchanged in the IIOT environment it is critical that contractual agreements incorporated at least the following areas (Soares and Kauffman 2018, p. 284):

a) The smart-object manufacturers may simply own the data regardless of whether the smart object itself is sold or leased to a customer;

b) The smart object manufacturers may own the data, but the customer will receive a license to some or all of the data;

c) The smart-object manufacturer may own the data, but the customer and some third parties will receive a license to some or all of the data; or

d) The customer may own the data, but the smart-object manufacturer will receive a license to some or all of the data and for all or some specific purposes.

Finally, it is also important to also define the expectations, responsibilities and liabilities regarding data security and privacy, as both suppliers and customers may be vulnerable to breaches of data security and privacy.

As such, contracts incorporate such expectations, responsibilities and liabilities very clearly and carefully. They should include the details regarding gathering, anonymizing, notifying and using suppliers, partners and customer's data.

6. FINAL REMARKS AND CONCLUSION

This article relies on evidence available in the current literature to conclude that I4.0 will impact manufacturing businesses of all sizes and across all industries, generating rich data which, when coupled with analytics, will enable more efficient monitoring and controlling of operations leading to increased levels of flexibility and efficiency.

Nevertheless, the while the I4.0 technologies have no effect on IP themselves, they do affect how business related to each other, and in particular how data containing IP is exchanged between manufacturing businesses and their value chains.

Furthermore, as explored above, the current EU legal framework does not provide clear data ownership rights to address the IP challenges in the face of IIOT. As such, manufacturers will need to explore new venues for legal protection in copyright or trade secrets law or even, where possible, the protection of the data as a whole in through database protection.

Finally, we conclude that this change in paradigm has a direct impact and pose a set of challenges to IP and IP strategies, which should be formulated to protect and commercialising IP in such an environment, where manufacturing businesses will be left to negotiate individual agreements governed by the law of contracts. These in turn, provide a strong protection against the contracting partner, but are weak against any third party who also has the data.

7. VII. REFERENCES

Bauernhansl, T., M. ten Hompel, and B. Vogel-Heuser, eds., Industrie 4.0 in Produktion, Automatisierung und Logistik, Springer, Wiesbaden, 2014.

Berne Convention for the Protection of Literary and Artistic Works. (1886). 1st ed. [ebook] Berne. Available at: http://www.wipo.int/treaties/en/text.jsp?file_id=283698#P123_20726 [Accessed 9 Apr. 2017].

Botthof, A. (2015) Zukunft der Arbeit im Kontext von Autonomik und Industrie 4.0. In A. Botthof, & E.A. Hartmann (Eds.) Zukunft der Arbeit in Industrie 4.0 (pp. 3-8). Berlin, Heidelberg: Springer.

Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014) How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. International Journal of Mechanical, Aerospace, Industrial and Mechatronics Engineering 8(1): 37-44

Business Insider (2015) The Internet of Things. http://uk.businessinsider.com/internet-of-things-2015-forecasts-of-the-industrial-iot-connected-home-and-more-2015-10. (Accessed on 3 July 2017)

Clarke, A., Kohler, P. Property law: commentary and materials. Cambridge University Press, Cambridge, 2005

Department for Business, Energy & Industrial Strategy. (2017) Made Smarter. Review 2017 [Online]. London. https://www.gov.uk/government/publications/made-smarter-review. (Accessed 11 November 2017)
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

DLA Piper (2013) Rights in Data Handbook. https://www.dlapiper.com/en/uk/insights/publications/2013/01/rights-in-data-handbook-2013/ (Accessed on 5 July 2017)

Emmrich, V., Döbele, M., Bauernhansl, T., Paulus-Rohmer, D., Schatz, A., & Weskamp, M. (2015) Geschäftsmodell-Innovation durch Industrie 4.0: Chancen und Risiken für den Maschinen- und Anlagenbau. München, Stuttgart: Dr. Wieselhuber & Partner, Fraunhofer IPA.

European Commission (2016) Commission staff working document, advancing the internet of things in Europe, SWD (2016) 110 final

European Commission (2017) Building a European data economy, communication from the commission to the European Parliament, the Council, The European Economic and Social

Hoeren, T. Big data and the ownership in data: recent developments in Europe. European Intellectual Property Review (2014) 12:751–754

Kagermann, H. (2015) “Change Through Digitization – Value Creation in the Age of Industry 4.0”, in: Albach, H., H. Meffert, A. Pinkwart, and R. Reichwald, eds., Management of Permanent Change, Springer, New York, 2015, pp. 23-45.

Kirazli, A. & Hormann, R., (2015). A conceptual approach for identifying Industrie 4.0 application scenarios. Proceedings of the 2015 Industrial and Systems Engineering Research Conference.

Leber, J. (2012) General Electric Pitches an Industrial Internet, MIT Technology Review [Online] (28 November 2012). https://www.technologyreview.com/s/507831/general-electric-pitches-an-industrial-internet/ (Accessed on 11 June 2017)

Lessig, L. Code: and other laws of cyberspace. Basic Books, New York 1999

Loebbecke, C., & Picot, A. (2015) Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. The Journal of Strategic Information Systems 24(3): 149-157.

Malgieri, G. (2016a) "Ownership" of customer (big) data in the European Union: quasi-property as comparative solution? Journal of Internet Law 2016:3–18

Mattei, U. Basic principles of property law: a comparative legal and economic introduction. Greenwood Publishing Group, Westport, 2000.

Millien, R., Geoge, C. (2016) Intellectual Property Lawyering in the Fourth Industrial Revolution (the IoT). https://www.researchgate.net/publication/313504500_Intellectual_Property_Lawyering_in_the_Fourth_Industrial_Revolution_the_IoT (Accessed on 22 May 2017)

Purtova N (2015) The illusion of personal data as no one's property. Law Innovation Technology 7(1): 83–111

Richter, K., Walther, J. (2016) Supply Chain Integration Challenges in Commercial Aerospace - A Comprehensive Perspective on the Aviation Value Chain, Springer, Hannover.

Rose, K., Eldridge, S., Chapin, L. - The Internet Society (ISOC), 2015 https://www.internetsociety.org/resources/doc/2015/iot-overview (Accessed on 23 April 2017)

Schwab, K. (2016) The Fourth Industrial Revolution: What It Means, How to Respond, World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/. (Accessed on 13 April 2017)

Symantec Corporation (2013) Intenet Security Threat Report 2013 – Volume 18 [Online] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (Accessed on 7 April 2017)

UK Intellectual Property Office, Eight Great Technologies, The Internet of Things: A Patent Overview (August 2014) https://www.gov.uk/government/publications/new-eight-great-technologies-internet-of-things. (Accessed on 3 May 2017)

Ocean Tomo, 2015 Annual Study of Intangible Asset Market Value (March 2015) http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/ (Accessed on 23 March 2017)

Symatec (2013) What's Yours Is Mine: How Employees Are Putting Your Intellectual Property at Risk. https://www.symantec.com/connect/blogs/what-s-yours-mine-how-employees-are-putting-your-intellectual-property-risk

(Accessed on 5 May 2017)

Soares, M., Kauffman, M. (2018) Industry 4.0: Horizontal Integration and Intellectual Property Law Strategies in England. Revista Opiniao Juridica, Fortaleza – Brazil. Ano 16, n.23, p. 268-289, Jul-Dez 2018

WIPO Intellectual Property Report (2011) The Changing Face of Innovation
http://www.wipo.int/publications/en/details.jsp?id=227
(Accessed on 2 June 2017)

Your Response Ltd v Datateam Business Media Ltd [2014] EWCA Civ 281 (14 March 2014)