Is The Current IP Framework Still Performing Well In Its Supporting Function Of Introducing New Technologies Into The Market?

By Matthieu Dhenne, Antonio Di Bernardo, André Gorius, Mark Marfé, Dario Mohammadian and Pierre Ollivier

Motivation

The LESI Innovation Trends (LIT) Task Force is a horizontal task force within the structure of LESI Committees. It is responsible for monitoring the factors of change brought by innovation that have a significant impact on the current IP framework, identifying any shortcomings, and proposing corresponding solutions.

In the present information-based economy, new technologies (NT)—for example, artificial intelligence (AI), blockchain, Internet of Things (IoT), "Big Data," and automatization—are very quickly starting to change how society as a whole operates, which has many consequences on industry and services themselves.

Although this trend is developing in an accelerated way around the world, in the last few years there have been voices raised to the fact that the current support given by the IP framework (IP law, practice and procedures) to developers (as the creators and implementers of the innovation) and its users is insufficient to enable implementing in a sustainable manner the benefits of NTs in society, and, as a consequence, leverage the impacts of "the fourth industrial revolution."

The objective of this paper is to analyse to what extent the current IP framework is still correctly aiding in bringing the benefits of NT developments to society, and to identify areas where it is lagging and, therefore, where there is room for improvement.

1. Scope of the Paper

In view of the above considerations, the task force has decided to present a synthesis of the present state of the art, in order to identify the necessary evolutions of the IP framework in view of the overall needs of the NT developers.

In order to achieve these objectives, first an overview of the present and future impacts of NTs on society as seen from the point of view of developers is presented. NT developers (individual Creator/Inventor, or SME, or Corporate, or University/Public Entity) are the creators of new technologies and services, and the long-term impact of the utilization and leveraging of the capabilities provided by new technologies is clearly in their hands. They invent, develop, enhance and implement new products and services. The present penetration of NTs into all activities, more or less intense depending on the amount of resources invested by companies and institutions, is a clear indicator that there is an increasing shift from traditional methods to new ones. The users of new products and services themselves are changing their habits and behaviors, which in turn affects the very objectives and impacts of the NT developments.

The way people create and put into practice NT developments, as well as the way society uses them, definitely represents ongoing drastic changes, and the IP framework (IP law, practice and procedures) will have to be adapted to support developers in their efforts towards innovation. This paper tries to explain in what manner and at what pace this is happening, and identify areas where the IP framework is lagging behind.

As is often the case, we tackle here a problem that will ignore country and zone boundaries. New technologies are developing fast worldwide, and already have huge impacts on everyday life. On one hand, as developers need to protect their effort in R&D, a global assessment and reasoning is needed; this implies understanding how local IP law is adapting, and how these changes impact IP management on a global basis. On the other hand, fast and global spreading of NTs also entails potential risks, such as privacy.

■ Matthieu Dhenne,
Partner,
Ipsilon,
Paris, France
E-mail: mdhenne@ipsilon-ip.com

■ Antonio Di Bernardo,
Founding Partner,
Thinx,
Milan, Italy
E-mail: a.dibernardo@thinx.expert.com

■ André Gorius,
Partner,
Winnotek,
Lyon, France
E-mail: andre.gorius@winnotek.com

■ Mark Marfé,
Legal Director,
Pinsent Masons LLP,
London, United Kingdom
E-mail: Mark.Marfe@pinsentmasons.com

■ Darío Mohammadian,
European Patent Attorney,
KUKATI,
Barcelona, Spain
E-mail: mail@kukati.com

■ Pierre Ollivier,
Managing Partner,
Winnotek,
Paris, France
E-mail: pierre.ollivier@winnotek.com

This paper therefore specifically focuses on this particular overlapping zone: where the IP framework meets NTs. It is of interest to identify whether NTs have intrinsic properties that are not catered for adequately by the existent IP framework, in order to bring them to light, and tag areas where the IP framework needs to adapt or improve if it wants to continue adequately supporting the tough task of bringing the benefits of NTs to society. We will thus start by a brief overview of these NTs, list problems related to NT protection and proposed solutions, and as a whole, try to understand which will be the impacts on licensing on a global basis.

2. An Overview of the Digital Economy as Enabled by New Technologies

The digital economy has become a key feature in most, if not all, aspects of society. From a curiosity a few decades ago, it has become a key analysis tool, if not a lever to create value. Nevertheless, under the broad definition of NTs, many complementary, sometimes contradictory, aspects are present. This section tries to identify some of the most important aspects.

To begin with, it is important to understand the present state of the (new) possibilities brought by these technologies, but also their projected evolution in the future. For example, specialists agree that machines will analyze data, describe complex systems, and propose actions based on the analysis of existing or new inputs. Although there is a lot of product development in this area, it is still debatable whether we will see real working systems in a reasonably near future. This does not, of course, mean that the IP framework should not get prepared for this drastic evolution; the timescale of this evolution in NT's capabilities, and thus the corresponding evolution associated to the IP framework, is nevertheless critical.

Machines will soon communicate with each other to perform a variety of functions, and there is little doubt that these complex processes will bear the risk of uncontrolled information flows.

In what follows, we try to synthetize our present understanding of the situation, most of it based on interviews with AI specialists and industrial users.

Artificial Intelligence

To the common public, AI is often associated with the replacement (and enhancement) of the human brain's functions by processes performed by machines. Although no one can rule out this eventual possibility, it appears today that the road is still long to such a scenario. Today, AI is essentially a complement to human reasoning, and a substitute for when systems are too complex, for instance, when analyzing enormous amounts of diversified data, or applying enormous quantities of rules.

For example, intelligent machines playing chess or Go were initially based on rules, and have now shifted to so-called machine learning. As far as the very definition of AI is concerned, one has to be aware that in the opinion of leading specialists interviewed for this study, it appears that no real consensus on the definition of AI exists today. Nevertheless, two main branches of AI can be described, both having been identified after more than 70 years:

- Symbolic AI: based on deterministic rules, having for example led to expert systems. This branch is generally adapted where experts exist, and it is possible to describe rules explicitly.
- Digital AI: based on the analysis of (large) sets of data, and for seeking implicit rules more than explicit ones, relating inputs to outputs; here, one needs data, and algorithms to analyze the latter, which are able to adapt their internal structure ("model" - mostly modification of the parameters of sets of Neural Networks) while new datasets generate new outputs. "Machine Learning," which is the present trend, is a branch of AI that takes advantage of the increased computational power available to use huge amounts of data ("Big Data") to produce statistically more accurate results. Big Data is not a limit to technology, but a resource. The question of the protection of both input and output of datasets becomes central and will be addressed in the rest of the paper.

  As of today, although machine learning is progressing at a fast pace, human intervention in machine learning efficiency is essential (for example, in having the right intuitions and ideas of how to use the algorithms, adequate model training, and parameter configuration, to name a few).

The main applications and services present in industry cited in our interviews can be categorized as:

- Improvement of internal enterprise processes: improvement of efficiency, automation, reduction of risks of mistakes, etc., representing a global cost efficiency.
- Creation of new services, leading to improvement of operating processes: for example, control of the quality of sub-contracted production of textile goods by optical sensors and image analysis instead of human control, support of production operators in their supervision using virtual reality (detection of leaks, etc.).
- Improvement of manufacturing processes while integrating huge amounts of input data (such as process data) as well as output data (such as quality, environment, costs, or client usage parameters).

For these purposes, mastering the characteristics of datasets is essential:

- Their origin: here, the question of origin and ownership of data is critical; when sensors are used, which is more and more the case, the exact description of the role and contributions of sensors and their environment must be integrated into the analysis.
- Their quality: for example, making sure the data represent really what one thinks they do. Here, a step of thorough "cleaning" is generally needed. Here again, the question of the protection and ownership of the cleaning processes involved are key.

The question of the ownership and protection, for example, through registered IP, of input and output data from all these processes must be clearly addressed.

The data has been collected and prepared for processing, it is used to train a model. However, many implementations use well-known existent underlying mathematical theories. The main contribution of AI has been in the data sphere, as AI makes extremely complex and otherwise unachievable data processing a reality. Should this fact strip the overall system of its intrinsic value? It is evident that well-trained models generate results that would never be achieved otherwise, hence, one has to re-evaluate how the AI contribution is to be acknowledged, as otherwise there is the risk that nothing might be acknowledged as a technological development if it happens to be in the data sphere.

Once the model has been trained, it is used to predict and/or generate outputs based on new input data. The output datasets can by themselves be unique. Following the sensing example described below, the result of innovative sensing is the generation itself of novel datasets that would otherwise not exist.

Internet of Things (IOT)

Physical devices (such as sensors, smartphones, home appliances, etc.) are now connected and exchange data through various communication networks. However, this communication is evolving to much more than mere data transfer for display on a screen. Machines (or any "thing") will form together larger systems, which, in conjunction with smart processing, such as through algorithm-based (AI or blockchain) information flows, will result in autonomously operating groupings that perform everyday tasks automatically. Here again, protection and ownership of the whole chain become critical, with a growing complexity since input data generate outputs that are used again as inputs. Almost all information and communication technologies (ICT) converge together in such an IOT structure, from the electronics of sensors, through the structure for wired or wireless communications, the protocols of data processing, and so on, globally generating a new digital economy that, in large part, operates autonomously with minimal human intervention.

DLT/Blockchain

As one can see from the above, securitization of data transfers and information flows is an essential part of the many challenges lying ahead: all inputs and outputs of these NTs, and associated working procedures, have to be under safe and controlled protection. In recent years the blockchain concept and network has appeared and is being further developed, aiding in addressing these issues, at least on all transactional information flows. For the sake of completeness, it should be mentioned that blockchain is one type of a wider family known as Distributed Ledger Technologies (DLT). Blockchain, however, is commonly used to refer to the whole family, as it is the most popular one to date.

A blockchain is a database, specific for the way it registers, stores and handles the data. New data is stored into blocks and made part of a chain in a chronological order; the new block is linked ("chained") to the previous one. Each of these blocks is attributed a timestamp, a "cryptographic hash" (a fixed size bit array impossible to invert) of the previous block. The data it contains can be of any sort, but today the majority of blockchain systems are used for transactional purposes, and so blocks contain transaction data. The evolution of the blockchain enables each block to contain more than transactional data: it also includes programmable data. This has taken the initial blockchain implementation to the next level. On one hand, each block can be programmed to perform certain tasks depending on specific input conditions. For instance, if a block represents a token with an economic value, it can be programmed to be used only for a particular transaction. On the other hand, the core network where the exchange and updating of the blocks takes place is also programmable, enabling all the blocks to be used as input parameters and be generated as outputs.

When the blockchain is decentralized, no single person or group has control, and only all users collectively have control. The data are then entered irreversibly, meaning that the transactions are permanently recorded and viewable to all users. This is the case, for example, for Bitcoin, the cryptocurrency, which was blockchain's first application.

However, DLTs are developing now to fully programmable global processors or computers, extremely well adapted for performing routine automated tasks and executing algorithms on a global scale. Similar to the case of AIs, the main contribution so far of DLTs has been in the data sphere, as it represents a new framework for data processing on a global scale ("The Global Computer" as some DLT specialists have coined).

However, when stripped down to the bones, DLTs

use existing computing networks for performing routine tasks. Should this fact strip the overall system of its intrinsic value? It is evident that no such technology has ever been developed in the past, and only just now an extremely low number of applications are being seen (compared to what is expected in the near future). Hence, one has to re-evaluate how the DLT contribution is to be acknowledged, as otherwise, similar to the case of AIs, there is the risk that nothing might be acknowledged as a technological development if it happens to be in the data sphere.

How the IP framework can help support the emergence of DLTs is clearly one of the challenges ahead.

The Digital Economy

For decades, the manner in which human beings conduct economical transactions has been evermore based on ICTs. Starting with e-commerce and online transactions through today, where not only private entities, but also public administrations are fully integrating the use of ICTs in their daily operations. The digital economy evolves as transactions between human beings integrate the evolution in ICTs.

New NT developments are appearing based on a single one of these NTs, or from a combination of two or more of them. Some experts postulate that the most common or routine tasks will be taken over by automatically programmed DLTs, whereas the creativity necessary for other implementations will be provided by AI. Hence, it is also possible that some IOT systems might comprise a DLT-based substrate running lower-level data processing with a higher-level data processing based on AI running on top.

Such systems exchange an enormous amount of data, both personal data and non-personal industrial data. There will be a number of actors specializing in the collection or generation of data. Since this data will be used by other actors for particular purposes, the data will have an intrinsic value, and can be traded. There is therefore an economy developing around data transactions in addition to that linked to the exchange of physical products and services. The most advanced representation is that of the crypto assets existing in all DLTs. Bitcoin is just one type of crypto asset, whereas in the future, everything is subject to having a crypto asset correspondent.

There are, and there will be, core technological developments performed on every NT mentioned. However, the larger share of useful NT developments will be based on how data are managed and processed. These NT developments are re-defining the way we inter-relate in the so-called new digital economy. This new paradigm is encountering a number of obstacles that have to be addressed by the current IP framework if it is to continue serving a useful purpose.

3. Societal and Industry Impacts

The societal impact, already existing or potential—for example, the right to be forgotten/oblivion, the guarantee of usage of privacy rights, that is generated by this new complexity (in terms of processes and huge amounts of personal or non-personal data) is such that the legal framework in which they will operate in a secure mode is probably far from being understood today.

One key parameter here will be the timescale involved: for example, the evolution of algorithms is very fast (on the scale of days and weeks), whereas the typical times offered by the IP framework (filing, prosecution, enforcement) is on a scale measured in years.

Most of the operational and transactional processes of companies will most probably be affected by the fast and massive arrival of these NTs, implying new ways of working and contracting with third parties. Supply chain, manufacturing, marketing and sales, and all support functions such as legal, HR, IP, IT, and so on, should be affected, both in their existing modes of operation as well as through new ways to operate.

One critical area where companies must make sure they have the right protection policies and procedures in place is whenever new concepts, ways to operate, or services enter the game- in a nutshell, all of innovation. As far as technologies are concerned, innovation covers a very broad spectrum of activities and results, from incremental manufacturing improvements or product modification R&D to breakthrough R&D. For example, IOT/AI/DLT systems will play an essential role in the determination of new ways to improve manufacturing processes or allow the discovery of new ones. The way to handle the IP around all the intermeshed processes involved (inputs, outputs becoming inputs, algorithms...) is not at all clear today.

For all the reasons explained above, it is apparent that a new way of thinking of IP is necessary.

4. Instruments Offered by the IP Framework to Further NT-based Developments

This section discusses the IP instruments available to the NT developers and identifies focus areas that should be closely monitored if they are to continue efficiently providing support in their task of bringing the benefits of NTs to society. This section does not focus on the pros and advantages, which are undoubtedly many, but rather on the areas in need of improvement for each type of instrument.

4.1. Patents

Patents represent the IPR best suited for packaging the technical aspects of an NT development. By means of the figure of computer implemented inventions (CII), which are regulated in most industrialized countries, both the hardware as well as the software

representations of an invention can be protected. Most NT-developments discussed will typically comprise a mixture of a hardware component (sensor, processors, communications network) and a software component (the algorithms and protocols executed by each hardware component separately, as well as the overall method implemented by the system). Utility models also exist in many countries. However, in most of them only the hardware component is eligible, whereas methods are excluded from protection.

CIIs are regulated differently in different countries. However, an NT-development is a global implementation as it readily uses the internet, or similar global communications networks, for its operation. It might very well be possible that data are gathered in a plurality of first countries, processed on servers hosted in different second countries, and the output served to users in the same or third countries. Also, although an NT-implementation might be completely local, it is desirable that it is readily exported, like any other product, to any country. Hence, harmonization of the IP framework is, as always, essential to facilitate trade and commerce in this sense.

There exists a variability across the globe on how CIIs are dealt with. Most jurisdictions are still busy coming to terms on how to deal with traditional CIIs (*i.e.*, simpler ICT developments), which differentiate themselves from the NTs discussed above (so-called developments in the *data sphere*). Before worldwide harmonization has been achieved on traditional CIIs, NT-developments have arrived with their specific higher emphasis on the data processing aspects of the technological implementation (again, innovations in the *data sphere*). It seems most (if not almost all) jurisdictions are rather slow at keeping up with the pace of this technological evolution. More often than not in the advancement of society, when an evolution is too sudden, it is rejected upfront rather than integrated or catered for. This potential rejection represents a complete stop-stone for the integration of new NT-related products and services to the market, the corresponding benefits to society, and the development of the digital economy.

The variability on how CIIs are dealt with across the globe sometimes is only apparent in actual practice, as the wording of the laws and regulations are similar in many jurisdictions. In some few countries with the most stringent standards among the most industrially developed and with the strongest economies, CIIs are almost *de facto* outright non welcome, and, in practice, not granted as patents. Other countries or regions have developed decade-long case law, having dealt with traditional CIIs on a frequent basis. However, even in these jurisdictions, higher standards seem to be applied to CIIs rather than to other technical fields of the same jurisdiction. One thing all countries seem to have in common is that the more humanity advances towards a world based on digital innovations in the data sphere, the further away the patent granting system seems to be drifting when accompanying companies on this journey.

From Concrete/Solid Inventions to Conceptual/Liquid Inventions: the Incapacity of Current IP Framework (Law, Practice and Procedures) to Adapt to the Times and the Needs of the Users of the IP Ecosystem.

There are some actors in the ecosystem that are of the opinion that the current IP framework (patent law, practice and procedures, first and second instances, as applied by PTOs or courts alike) do not adequately provide the legal support needed by NT developers—the ghost in the room is that there seems to be a "nothing is inventive in the data sphere" bias to inventive step analysis. The problem raised by this line of thinking is that the IP system developed throughout centuries of innovations based on *concrete/solid* inventions does not seem to be valid anymore for current *conceptual/liquid* inventions in the data sphere.

Other actors in the ecosystem do not see things as being so bad. Although they agree on the fact that obtaining patents for CIIs seems to be much more difficult compared with other fields of technology, they believe this difficulty is justified for two main reasons: (1) the intrinsic nature of software algorithms, which are nothing else than a sequence of method steps that—if not correctly defined—risk to be expressed as mental acts with no technical effect, and (2) the fact that NT's success very often does not depend on innovative software algorithms, but on the availability on the market of improved hardware systems having better computational power that makes possible successfully executing algorithms that were invented years ago.

In any case, patent law does not seem to have by itself a moral or ethical backdrop (unlike, for example, penal law). One should not forget this fundamental difference with other fields of law. The patent system only makes sense if technology developers make use of it as a tool to help bring their technical innovations to the market, ultimately benefitting society as a whole. All actors of the patent ecosystem, in particular PTOs, should remember their raison d'être: to help society advance and not hinder this advance based on over-complicated theoretical/conceptual high-level considerations (as if patent law had, by itself, a life of its own, or a different purpose than supporting the advance of humanity by helping bring well validated innovations to market). Any other non-technical considerations (such as ethical or moral considerations) are not the responsibility of patent-granting authorities, and each country should deal with them according to their local practices via independent administrations.

PTOs should realise that innovations have presently evolved to a different level: the era where innovations were made on mechanical structures that could be seen and touched (tangible in this sense) is only part of the whole. According to the European Patent Office, three quarters of applications are CIIs or related thereto. Technical innovations will no more necessarily be tangible in this sense, they will be mostly general-purpose processors or networks of computers, managing data carrying different types of information. This cannot be undervalued based on the tangibility difference between different types of technical innovations. They are equally valuable in *our times* as their more tangible forefathers were in *their times*. This realization does not seem to be integrated in the internal processing of applications by PTOs or by the technicality considerations of their legislators.

Therefore, the analysis has to go beyond simply concluding lack of inventive step if the only distinguishing feature is the data that the technical system is managing and information it contains. Presently, when confronted with a different problem to solve, or when in a different scenario, it is more frequently than not concluded that, starting from the generic prior art, it would be obvious to change the data input into the computing network to solve that problem or to apply in that scenario. This evaluation removes all the value the information component of the data can bring to a system.

The European Patent Office has developed case law related to CIIs over decades that deals with the issue of technicality under the requirement of inventive step. However, in many cases, contributions that are perfectly technical do not proceed to grant after being evaluated as being obvious for the skilled person starting from existing computer networks or communication systems. So, what's presently missing? One postulation of what's missing is the confirmation that data by itself, when containing technical information, generates a technical effect on the underlying computer network.

PTOs could argue that this has always been the case. The technical information contained in sensor data has always been acknowledged as producing a technical effect on a determination step applied to an industrial process in a factory. However, what if the "factory" is a generic network of computers/servers/databases? Here lies the bottleneck. Currently, most PTOs require the factory itself to be modified in order to confirm the existence of a technical distinguishing feature. However, what is needed is that, even if the factory is not itself modified but the information provided by the data does provide a different result, that this resulting technicality is acknowledged.

Taking AI as an example, at present, many innovations are using mathematical models developed decades ago. Therefore, the theoretical underlying basis has been widely discussed. According to some actors in the ecosystem, new applications of these models should not be refused on the basis that it would be obvious to apply these known mathematical models on existing generic computing systems, however using new data to obtain new results. The application of known models to different technical problems requires processing new data to obtain new results; this should be acknowledged as producing an inventive step if the prior art does not provide a hint or motivation to this effect. PTOs are currently insisting on either having the generic computing system (*factory*) developed, or the mathematical model used (which forms an integral part of the *factory*). This therefore reflects an out-of-date procedure that hinders the development of humanity in the age of digital innovations.

Other actors in the ecosystem agree that, once the mathematical basis is known, this cannot be patented anymore, nor can the sole use of different data justify granting of a patent, because this would create uncertainty to the industry. According to this line of thinking, inventions cannot rely solely on the use of new data on known AI algorithms, but in the way the data is used: how the algorithms are trained (selection of the datasets used as input, methods for training the model, and so on), or how the outputs are managed and used to control different entities.

Finally, the consideration of where does the final effect take place needs to be reviewed. Currently, whenever a final positive effect takes place solely in the cognitive space of the end user, inventive step is not acknowledged as lacking a technical effect solving a technical problem of the underlying technical system. This falls again under the developing the factory principle…however, it is time to go beyond the factory.

Therefore, taking the EPO's statistics as representative of worldwide filings, *i.e.*, three-quarters of all patent applications are in the field of CIIs, which represents an enormous share, the PTOs and corresponding entities should take these considerations seriously. It is not a question of allowing any and all developments in the data sphere to be patented, as this lacks sense, but in revisiting the issue more closely, being aware that a potential problem might become worse with time and starting work on a solution.

Prosecution Times—Too Slow for NT Developments

As stated above, the prosecution time to obtain a granted patent can take several years, while software applications often have shorter life cycles. This is often a problem making the patent system uninteresting for companies, preferring to maintain their inventions as secrets instead of disclosing them in exchange for a protection that will come too late, as the technology will probably be by then obsolete. Also, not all countries have provisions for enforcing patent applications, and

only granted patents can be enforced. Therefore, a need for real and effective accelerated examination exists.

The USPTO has a special Track One project that aims at giving applicants a final disposition within 12 months, which is fine for software applications. The limits associated with this program are the costs (very high) and the number of applications admitted to the program (10,000 only).

Both USPTO and EPO also have the possibility to request accelerated examination, but these programs do not appear to be effective. Some patent attorneys do not recommend requesting accelerated examination before the USPTO because the process is said to be cumbersome and the costs risk being more than those of the Track One project. The EPO allows applicants to request accelerated examination for free, but the applicants do not seem to perceive an actual acceleration.

One must consider that the global economy is presently moving at its fastest pace. Even for developments that are not specifically NT-related or ICT-related, the same considerations apply. The world of entrepreneurship is fast moving, working on short time scales, and often jumping from one round of investment to the next. Many entrepreneurs simply do not see how a slow-moving IP system can benefit them in their growth.

Therefore, a need exists for obtaining patents in shorter times.

The Issue of Inventorship—Can Machines be Designated as Inventors?

A hot topic, and a very much discussed question, is that of "inventorship" of NT-developments generated by machines. Supposing an AI algorithm is used to analyze data and the output is a new car body with improved aerodynamics: who is the inventor of the car body? The human being operating and instructing the AI algorithm or the algorithm itself? The question is not a philosophical one and has true legal and economic consequences.

The right to the patent belongs to the inventor and is then transferred to the applicant by way of an agreement between applicant and inventor or because of legal provisions, for example, if the inventor is an employee, some countries provide that the right to the patent belongs to the employer.

The question of inventorship is therefore legally important because an applicant is only entitled to a patent if he has acquired the right from the rightful inventor! A patent filed by a not-allowed applicant can be revoked or reassigned to the right applicant.

For instance, take the scenario where a company obtains a licence to use an AI software for inventing a technical solution (the car body). Is the company entitled to file the patent application? This would depend on the software licence: if the licence grants use of the software but no IP rights deriving from the use, there can be a problem, and the company would not be entitled to file the application.

Experts all around the world have been involved in this discussion, and the generally shared approach is that the inventor must be a physical person, while AI algorithms are considered tools that are used by inventors to generate new solutions. Artificial intelligence algorithms therefore cannot be named as inventors or co-inventors in a patent application.

4.2. Trade Secrets

Trade Secrets have been first used to protect know-how from being exploited by third parties. But its interest has expanded to protect some valuable NT that were not eligible for patent protection in many countries.

An important development in Europe has been the adoption of the Trade Secrets Directive on June 8, 2016. However, the current point of view is that the same protection is not offered in all European countries alike, generating uncertainty when using them in business transactions region-wide.

According to many laws, confidential information is legally protected with a legal status as long as it meets three criteria:

1. It is not publicly disclosed,
2. It has commercial value,
3. It is subject to reasonable protective measures.

Most of the time all company information is concerned, not just know-how (especially scientific and technical information). This now includes commercial, financial, organisational, and strategic information, etc.

Particularly in Europe, to benefit from legal protection since 2016, it is necessary to know whether the information to be protected meets the above criteria.

The current trade secret framework offers an opportunity with a new legal protection, which is welcome for innovation in the form of methods, AI, codes, algorithms, etc., and for inventions that must remain secret to avoid being counterfeited. But this legal protection is specific since, first, it does not provide a property title like patent does, and second, it exists only thanks to security measures applied continuously. The use of trade secret implies a specific care to be given to the confidentiality measures and to the traceability of the exchanges. The filing of a claim against trade secret infringers requires demonstrating precisely what information or data has been disclosed, to whom, and proving that this information was subject to sufficient confidentiality protection. Providing this proof is frequently extremely difficult for trade secrets exchanged via NT platforms or generated directly on an NT platform. To obtain the necessary evidence, it requires access to the IT management system to know

who has written what and when, who has modified it, or who read it. The new working practices for innovation need to be reinvented from a governance, a legal, and an IT point of view, to organize the traceability of digital information exchanges across companies as compared to paper-based information.

Data and Trade Secrets: Confidential Information in the Digital Era

In today's world where data is the new precious metal, identifying, protecting its trade secrets or sensitive data, and creating value out of it has become a crucial task.

The value and the need to protect trade secrets is generally implicitly recognized in enterprises, but recent developments have shown that taking into account the latter formally in the enterprise strategy and operations is now a must for all companies. High growth enterprises are naturally particularly concerned, but more traditional businesses, and also start-ups and SMEs, should not underestimate the consequences of not protecting their trade secrets.

Business secrets and trade secrets, including know-how, algorithms, methods, etc., are not always considered as an asset, which is a problem in an economy driven by NT. Indeed, some secrets are a key asset in potential jeopardy due to NT generalization, which may have similar or even greater value than patents. As a first-level response, a number of companies have protected some of their key business advantages by the use of trade secrets, which benefit from a longer period of protection than that afforded by a patent, and avoids competitors being able to have access, mostly digitally, to any information that could help them to find a way to circumvent. But this example is only a starting point. Generalizing this effort to encompass all aspects of assets related to trade secrets should be considered as the correct answer to the challenge of preserving and developing their value.

In general, the evolution of trade secrets in various legislations suggests referring practically to business secrets, company private confidential information of economic and commercial value that companies need to protect and preserve with reasonable protection measures for the sake of their business. These business secrets include any confidential information having a commercial value, more generally a strategic value, and benefiting from specific safety protections. Examples are:

- Know-how
- Methods
- Algorithms
- Other scientific or technical inventions not protected or not protectable by an IP title,
- Technical or quality specifications
- Commercial proposals, lists of suppliers, organisational charts, compliance alerts, and so on
- Any other confidential protected data that constitutes a competitive advantage for the company

In the Knowledge Economy Dominated by Digital Exchanges, a Number of Strategic Considerations Related to Secrecy Should Be Kept in Mind

A company must protect confidential information of two types:

1. The information it owns
2. The information received from a third party, who informed it of its confidential nature. Whether the third party is the owner of this information or not does not change company obligations.

In practice, due to the recent EU law, a privacy policy imposes the need to manage two types of data stocks:

1. The past (the information prior to 2016), covered by confidentiality agreements. There were many confidentiality agreements in place but, due to the rapid growth of digital exchanges and the volumes of data exchanged, the operational links between these contracts and the monitoring of the information disclosed by the parties have become more strained. There are few structured files (paper or digital) including the confidentiality agreement and the confidential information exchanged under the agreement. Their real protection therefore remains questionable, as the actual confidentiality of this data must be verified *a posteriori*.
2. The present and the future (information that has come to light after 2016). In order to meet the criteria of the law, it is necessary to design appropriate practices about detection, qualification, protection, and monitoring of information, and about using the appropriate tools.

It also requires dealing with six separate disclosure stream types:

1. Internally, on the "need to know" basis
2. Intra-group, between mother and daughter or between subsidiaries (reporting, shared databases, M&A, and so on)
3. Between the company and one or more third-party contractors
4. Toward any regulated profession (IP attorneys, lawyers, banks, etc.)
5. Toward administrative or judicial authorities
6. Toward the public

4.3. Copyright

Copyright allows protecting software, databases, and data contained in the DBs, in cases where relevant investment has been made. Copyright protects works

belonging to the literary, scientific and artistic domain. Most legal systems require originality of the work in order to grant copyright protection; under EU law a number of decisions of the European Court of Justice, starting from the 2009 Infopaq decision, have clarified that a work is deemed copyrightable provided that two requirements are met: (1) the work is objectively identifiable as an object of rights; and (2) the work is original, *i.e.*, is the "author's own intellectual creation," which means that the work is the result of free and creative choice by its author. Copyright law is mostly harmonized worldwide due to the Berne Convention of 1886 and the TRIPs Agreement. Copyright also protects software and creative databases.

Besides copyright, most legal systems recognize neighboring rights applicable to non-creative works or materials. This includes database rights provided by EU law for non-creative collections of data, provided relevant investments have been made. Other systems, such as U.S. law, do not currently recognize neighboring rights on DB, but apparently this has not blocked the creation of a vibrant NT market. This finding raises the issue of whether EU database rights for non-creative databases are still justifiable as a matter of policy or are an obstacle or an entry barrier for the development of NT and the Big Data economy.

On several occasions, AI has surprised human beings by its ability to compose autonomously, as a human being would, music inspired by the style of the Beatles, to write a novel, to make a film or a painting inspired by a famous painting by Vincent Van Gogh. The rise of these works created by AI, which can be qualified in law as artistic and literary works, raises questions, mostly about the recognition of copyrights, the ownership of these rights, and the moral rights.

The intertwining of copyright law and NT is twofold:

- Copyright law may be used to protect NT per se (*e.g.*, large databases, software); and
- Copyright law may be used to protect the results of NT—*i.e.*, works realized by AI systems.

Copyright Protection of NT

Software and databases belong to the domain of copyright law. Copyright law grants an immediate, powerful and extensive IP right immediately upon creation of the work, with no need for registration and with a low originality threshold for protection. In EU and most legal systems, copyright lasts for all the life of the author(s) and for 70 years after the death of the last author. Considering the average product lifespan of software/databases and the continuous improvements and modifications (each being potentially a new work derivative of the previous one), copyright on technological works such as software and database is virtually perpetual. This also means that the mechanism of public domain does not work for copyright on NTs: all expressions in the field of software are theoretically subject to third-party copyrights. The systems of "open source" and "creative commons" licensing mitigate this issue by introducing a library of building blocks for new software and works with free and standardized licence terms; however, the system depends on the developer's availability and will to share open codes for their solutions.

As a general rule, ideas are excluded from copyright protection; as a consequence, copyright cannot protect those expressions that are necessary to convey a certain idea or concept. A big issue for copyright on NTs is whether this exclusion applies to exclude copyright protection of the most efficient expressions to reach a certain result (*e.g.*, an efficient software routine to reach a certain result).

- Granting copyright protection of the most efficient expressions provides a powerful incentive for NT developers to reach such solutions, but on the other hand is capable of hindering competition and granting the copyright owner with a huge market power;
- On the other hand, denying copyright protection of the most efficient solution on the ground that the expression is necessary to reach a certain technical result and thus non-copyrightable would create disparity between sub-optimal copyrightable expressions and optimal non-protected expressions.

Copyright Protection of AI-generated Works

Another interesting chapter is the copyright protection of AI-generated works. Such works may be divided in (1) AI-implemented works, that is, works realized by human authors with the assistance of AI; and (2) AI-generated works, that is, works realized by the AI system independently with no creative human intervention. The general consensus view appears to be that AI-implemented works are copyrightable, while copyright protection of AI-generated work is still an open issue.

Some argue that copyright requires a "human" author to make creative choice, and propose to protect AI-generated works with a related right. Others argue that copyright law does not require the right owner to prove the creative process whereby the work has been created by the author; therefore AI-generated works that are indistinguishable from those of a human author should be recognized as original and thus protected.

A policy argument may be raised that, if AI-generated works are as a matter of fact indistinguishable from human creations, then denying copyright protection to AI-generated works would require the copyright own-

er to give evidence of human creation of the work in enforcement actions. This may create an obstacle to copyright enforcement.

Recognition of Copyrights

Among the creations resulting from processing by AI, we could schematically consider two types of "AI creations." First, computer-assisted creations for which AI acts only as a tool in the creative process supervised by a human being. Second, the creations generated spontaneously by AI without decisive human intervention at the time of creation, to the point that some people believe that in this case it is essentially the programmer and the machine that will generate the final work, or even consider that artificial intelligence is capable of its own creative process.

This diversity in "AI creations" requires a sophisticated approach in order to determine the nature of each creation generated through these AI tools, as well as the influence, if any, of the different actors involved (essentially the authors of the input data, the programmer—that is, the designer of the learning base—and the user).

In the case of AI-assisted creations where AI is used as a simple tool, it is possible to consider that the mark of the personal intervention of its author remains. The creation could thus become a work and be protected by copyright.

With regard to creations generated spontaneously by an AI, the advocates of their protection by copyright are divided between those who believe that one can still distinguish in these creations the mark of the subjectivity of the various participants and those who advocate the adoption of an objective conception of the key notions of copyright, and more particularly the notions of work of the mind and originality, in order to place these creations under copyright. In these two hypotheses, the characterization of originality will require an *in concreto* analysis of the creations, taking into account, depending on the design chosen, the AI method used, the scope of its intervention, and the latitude left to the user or to the person who, for example, selected the input data, proceeded with processing parameters, or intervened in post-production.

Finally, a third school argues for the incompatibility of copyright concepts as understood in their classical sense. Consequently, copyright protection should be rejected when AI is used to generate creations autonomously without being able to distinguish the personal imprint of any of the participants.

Ownership

The question also arises as to who will benefit from the ownership if the machine plays a determining role. Two solutions are possible. The first, unlikely because AI is an object and not a subject, is to consider it as an employee. The second, more likely, is to consider that the property belongs to the owner of the machine.

Moral Rights

Moral rights could pose limitations to the creation of outputs by AI, namely regarding the processing or displaying of embedded works, which acts may call into question, for example, the rights of integrity or attribution. We could imagine the possibility of creating a "sort of" moral right for AI, including the legitimacy, meaning, and enforceability of such a right. This would be a fundamental change in the nature of moral rights.

Focus Points and Problems

Currently copyright law is the main source of IP protection for new technologies. The concern is whether copyright law in the NT era is actually becoming an unbalanced system that perpetuates market power of a few technology owners and hinders independent follow-on innovation. This is especially true in the NT era, where the weight of CR Law for the protection of innovation is higher than patent law, which is construed as a more developed and balanced system.

The question arises whether the copyright system is currently "too strong" and unbalanced in favor of rights holders, creating huge market power in the hands of few copyright owners who create the main technological standards and platforms. If yes, which solutions may be incentivized to reduce the entry barriers for new developers? Examples may include:

- Denial of protection for *most effective solutions* on the grounds of lack of originality since they are necessary to reach a technical result;
- Introduction of compulsory licensing systems for derivative works in NT similar to patent law provisions on derivative patents;
- Open-ended "fair use" exceptions/limitation for technological standards.

Another question that arises is whether the EU DB right for non-creative databases, envisaged in the age of CD-Rom databases (1990s), is justifiable as a matter of policy in the NT and the Big Data era.

4.4. Trademarks

A trademark consists of any sign, *e.g.*, any word, image, color, or sound that is capable of distinguishing the goods or services of a company from those of other companies.

As such, a trademark registered for goods or services relating or connected to NT does not require special law provisions, nor is the current trademark framework affected by the fact that a product or service is NT-related. Therefore, the mark used in connection with an NT must be filed and registered, as would any trademark used in connection with any other product or service.

4.5. Licensing

Licensing is a valuable means of commercializing

IP and is therefore of fundamental importance to IP holders. This remains true in the context of NTs. However, there are a number of open questions that will impact the licensing of novel technologies. Many of these questions are interesting theoretical points, and others are addressed elsewhere in this paper (such as "does a human need to be named as the inventor of a patent?"). The most powerful tool to manage the potential uncertainties arising out of the licensing of NTs is by addressing such uncertainties in the contractual terms of the licence itself.

Despite the ability of the contractual terms to clarify uncertainties arising out of the licensing of NTs, certain grey areas exist and are discussed below. This section of the paper therefore generally addresses licensing considerations of NTs and the specific issues that arise in relation to particular NTs in order to consider if a change in legislation is needed to effectively licence NTs.

Licensing of NTs Generally

Whilst there are considerations to licensing NTs that are specific to certain NTs, which are discussed in more detail below, there are wider uncertainties in relation to licensing NTs in general.

Many NTs can be used for multiple purposes across multiple sectors, and some of these applications may not be known at the time the licence is entered into. This is exacerbated by the complex multi-party ecosystems in which NTs, such as IoT or AI, are likely to be deployed. This creates difficulties when attempting to contract for certainty with regards to the unknown, so addressing future proofing including scalability in a licence is important. Courts are reluctant to void contractual terms for uncertainty and will strive to give some meaning to contractual terms agreed by the parties if it is at all possible to do so. This means an unclear term may result in the licence having unintended consequences!

Many NTs rely on data as input (or create a data output), which by its nature can be constantly evolving in real-time and change in value. That data may be provided by a third party, that is, not a contractual party. While this paper specifically addresses the issues relevant to licensing data below, additional considerations need to be given where data is ancillary to the NT in question, for example, whether data privacy and competition law apply. Further, are there specific confidentiality provisions required in the licence to afford adequate protection to the use of data relevant to the NT?

Drawing the line between incorporating flexibility into a licence and maintaining contractual certainty can be difficult, but the licence is an important means to protect against uncertainty. A good starting point therefore is for the licensee of the NT to gain an understanding of the underlying technology sufficient to know to what extent the NT will achieve its business objectives. Having some clarity about the technology, the parties can then be clearer as to what legal rights can attach and to the relevant legal issues that may arise under the licence. A discussion around issues such as governance and allocation of liability would follow. At that point, a contractual framework can be prepared.

Artificial Intelligence

The development and use of AI can give rise to a whole host of IP rights, both in terms of the AI itself and the output that may arise from use of AI technology under a licence agreement. These rights can include patents, copyrights, database rights and confidentiality, and will depend on the type of AI and how it is utilised for the purposes of the licence. It is highly questionable whether, as AI advances, standard software licences are fit for the purpose.

Ownership

Whether works created by AI can give rise to IP protection is covered elsewhere in this paper. It is clear that a licence cannot be used to rectify any issues around IP subsistence, but a licence can be a useful tool when it comes to determining ownership of IP rights that do subsist in AI technology or its outputs. Typically, a licence will govern who owns background IP in the AI and who owns any improvements derived under the licence agreement.

Assuming the licensor is the owner of the AI technology at issue, he/she will want to ensure that any background IP to the AI is licenced to the extent necessary for the licence (and likewise, the licensee will need to ensure the licence scope permits it to use all IP rights required to use the AI for the purposes of the licence). A particular issue in the context of AI is who will own any improvements to the AI developed pursuant to the licence agreement. Typically, in "standard" licences, a licensor may wish to retain any improvements, but this can be complicated where AI technology is involved, as often the licensee's data and underlying know-how are used in the development of any improvements, or the licensee may train the AI to carry out tasks that may result in improvements. It can be difficult to predict exactly what improvements will be achieved prior to the AI technology being utilized, and improvements can change over time.

Where the licensee's data and know-how are used, the licensee should ensure that the licensor is not inadvertently given permission to use the licensee's information without adequate compensation through terms overly favorable to the licensor. For example, the licensor may wish to contract that it is free to use the licensee's data to train its AI to develop new prod-

ucts and that the licensor is then free to commercialize any improvements in its AI technology via a royalty-free non-exclusive licence. The licence terms should also provide flexibility to account for any unexpected improvements not foreseen by the parties.

Liability

A key area that may cause uncertainty for licensing AI technology is liability. For example, who is liable if the AI technology infringes a third party's intellectual property rights?

AI systems learn, change and improve with time, and in the future AI systems will act autonomously without any human effort or intervention to achieve results. This will also be the case for non-AI systems, as current blockchain and IoT implementations seek to produce machine-to-machine communications and exchange in the sense that machines will act as economic entities exchanging goods and paying for them. Even now, the nature of the technology means the decision making of some AI systems cannot be easily reverse-engineered in order to be assessed. Therefore, when there is a problem, it can be challenging to identify how and why an AI system went wrong. The liability issue is exacerbated by the complex, multi-party ecosystems in which AI systems are likely to be deployed. The success of an AI system often depends on the quality and sufficiency of the data, which may come from several data providers. The procurement and the processing of personal data need to interface with the relevant confidentiality and data protection regimes. The designer of the system architecture and the parties involved in developing the AI algorithm determine how the data will begin to be used, although the more autonomous the AI system becomes, the less input these people may have. That said, attributing liability for AI may be simpler in certain sectors than others, such as healthcare, where it is unlikely that AI systems will be allowed to function autonomously without any human oversight for some time to come.

Change to the legal framework around liability for use of AI is expected in the EU and elsewhere. In the meantime, robust and detailed governance mechanisms around the use of AI can help businesses adopting AI systems to address future risk of liability. Given the technical and the jurisdictional complexities of using AI systems, an option for businesses contracting with one another over the use of AI is to opt for arbitration proceedings to settle any disputes that may arise.

Warranties and Indemnities

Closely aligned with liability are the warranties and indemnities that should be included in a licence. Breach of contractual terms will, in the first instance, give rise to a claim for financial compensation. An injunction preventing commercialization of the AI system is more likely where there is an ongoing infringement of IP rights. Each party will wish to safeguard their interests. For example, the licensor will wish to restrict any warranties and indemnities (to the extent permitted by law) to that which the licensor knows about the AI technology. That said, parties should be aware that the courts may strike down overly broad disclaimers or exclusions of warranty.

How these situations will be dealt with in reality will, short of statutory intervention, be governed by existing contractual law and on the basis of what the parties are prepared to agree under the licence, as well as how the AI technology is to be used under the licence agreement. For this reason, a greater understanding of the underlying technology and what the parties are seeking to achieve is desirable.

Conclusion—AI Licensing

The EU has indicated that proportionate regulatory intervention will be required for certain high-risk sectors and applications. Given AI's potential to be ubiquitously applied, however, it is unlikely that there will be general legislation that covers all uses of AI. Absent legislation, businesses should consider certain specific requirements when licensing AI technology, particularly around ownership of improvements, liability, and warranties and indemnities. Given the nature of AI, particularly its unpredictability, it is important that licence agreements permit a degree of flexibility to address such issues that may arise during the course of the agreement. It would therefore be prudent for any licensor and licensee to understand the technology at issue to ensure their interests are adequately protected under an agreement and to agree on the scope of any mechanisms required to resolve legal uncertainties.

Data

Data, and in particular so-called 'Big Data,' is often described in terms of the 'three Vs,' where Volume relates to massive datasets, Velocity relates to real-time data and Variety relates to different sources of data. Each of these Vs has the potential to create new considerations when it comes to licensing data. As mentioned above, data underlies many NTs and can be vital to their success. It is therefore crucial that, despite the obstacles, adequate protection is put in place to protect data being licenced.

Scope of the Licence

As with every licence it is important for the parties to clearly define the scope of what is being licenced. In relation to licensing data, this can be difficult where the licence covers a data set that is subject to development or addition over time, or where data are collected in real-time from multiple sources. The data set will be constantly evolving, and what is originally licenced may not reflect the data that are ultimately used.

Both parties will want to ensure that the licence adequately reflects what they consider to be the licenced material. From the licensor's perspective, he/she may wish to ensure that the licence has a mechanism to reflect the scalability of the data that is licenced, whereas the licensee may wish the licence reflect any contributions that the licensee makes to developing the data set.

Value

The licence will set out the relevant payments to be made by the licensee. The mechanisms for payment and value attributed to material being licenced will be a commercial decision agreed between the parties, but it often comes in the form of royalties or a one-off payment. In the context of licensing data, a key obstacle is how parties attribute value to the data, and data valuation could be the subject of its own white paper. A good starting point is to think about what value a party attributes to its data. What level of investment has gone into preparing a dataset?

Any royalty mechanism that is agreed by the parties will still require a mechanism that can be adapted throughout the term of the licence to reflect the value of the data at the relevant times of payment. As with other aspects of licensing NTs, an element of flexibility in the mechanism is important to the successful licensing of data.

Intellectual Property Rights

There is no overarching legislative framework that governs the ownership of data. There are certain overlapping legal rights that may impact the use of non-personal data. In addition to contractual rights, the parties will need to consider confidentiality and trade secrets, copyright, and database rights. The protection afforded by these latter rights can be limited in certain circumstances. Parties to a licence will want to ensure that any legal rights that they own are covered by the terms of a licence, and that those rights are licenced to enable the licensee to achieve the purpose under the licence.

Liability—Quantification of Losses

Similar to the obstacles in relation to valuing data for the purposes of licensing, an additional obstacle is how to quantify losses arising from a breach of the licence or in the event that a third party exploits the data and/or the database. This is particularly important where unauthorised use or exploitation could lead to irreversible damage, for example, if data that has value by virtue of being confidential becomes widely publicly available.

Again, as with determining value, it is important that the licence sets out clearly the mechanism by which any losses would be quantified at a given time throughout the licence agreement so that the true value of the data at the time of breach can be calculated.

Warranties and Indemnities

In addition to quantification of losses, there are additional warranties and indemnities that parties should consider when licensing data. This will involve a commercial negotiation assessing factors such as the potential for a third party to obtain financial compensation or injunctive relief due to a breach or inadvertent infringement of IP rights. For example, the licensee will want the licensor to warrant that the data does not infringe any third-party rights. In turn, the licensor will want to protect his/her position and ensure that the licensee will use the data for the purpose as defined in the licence and will not cause any third-party unauthorised use of the data to occur. This is particularly important where the data include personal data, for which a breach can have serious consequences.

Conclusion—Data Licensing

With the central importance that data play in a variety of NTs, ensuring data are adequately protected under a licence is key to commercial success for both parties. Intellectual property rights may be present in certain databases; however, this will only provide limited protection. Generally speaking there is no IP in data, which is why data need to be considered distinctly and protected through contractual means.

DLT/Blockchain

Distributed Ledger Technologies (DLT/blockchain) can come in many forms with varying levels of accessibility and have a multitude of applications in a variety of sectors, the full extent of which has arguably not been fully realised. Different considerations can be required, depending on the technology itself and its application. As with AI, a "one size fits all" approach to regulation is unlikely, so considerations as to the nature and use of the technology is important when licensing.

Intellectual Property Rights

As with other NTs, certain intellectual property rights may be applicable to DLT/blockchain and need to be covered by the terms of a licence. For example, despite the perception of DLT being open-source, there may be patent rights over certain applications of the technology, copyright in the code being used, or database rights subsisting in the application of the technology. Again, it is important for those licensing such technology to understand the underlying technology and its application to ensure that any relevant rights are both protected and adequately licenced. The relevant warranties, for example, that the technology does not infringe any third-party intellectual property rights, will need to be raised. The licensee will also wish to ensure that it has the necessary consents and/or sub-licensing permissions if the technology is intended to be used by third parties.

As with other NTs, it is also important that the licence address the issue of ownership of any intellectual property rights arising from developments in the technology, particularly where the licence may cover use of or development of the underlying software.

Consideration should also be given where open-source software (OSS) is used to develop a DLT/blockchain solution. Open source software licence terms can take many different forms. For example, they may require the user to make any developments based on the OSS freely available. Some OSS licences might actually be highly restrictive, and an implementation using incorporated software or libraries should be aware of these restrictions before commercializing their own solution.

Liability

As DLT/blockchain is decentralized, one obstacle is the difficulty in determining liability in the event that something goes wrong, particularly where there are multiple parties in the DLT/blockchain and it is unclear who may be in breach. It is not clear how liability would be determined under law (and legislative intervention specific to DLT/blockchain may be beneficial), but parties may be able to protect their positions to a certain extent by determining how liability will be determined under the licence.

Such provisions may depend upon which party could be deemed to have the most control over the DLT at the time of the circumstances giving rise to potential liability, or which party's omission or action gave rise to the liability, but as with other NTs, a mechanism that can take account of unforeseeable circumstances may be useful.

Data Protection

Depending on the application of the DLT/blockchain, where personal data are used, additional considerations will be required. Legislation prescribes who are considered data controllers and data processors; however, this may be less clear in the case of DLT/blockchain, particularly as the technology is decentralized. It is therefore important that the licence sets out the role of the licensee and licensor (if applicable), and how data protection issues will be handled. The licence will not be able to override legislative provisions, but it can be used to provide contractual safeguards to the parties.

Jurisdiction

Due to the decentralized nature of DLT/blockchain, one issue which may arise is in the case of cross-border technology. This may also have an impact on the obstacles discussed above. For example, regulatory compliance, data protection compliance and liability may differ depending on the jurisdiction in which actions take place. Given the technical and the jurisdictional complexities, it may be beneficial for the parties to opt for arbitration proceedings to settle any disputes that may arise.

Conclusion—DLT/Blockchain Licensing

As with other NTs, it is important that the parties understand the technology being licenced and its foreseen applications in order to ensure that the licence can provide adequate safeguards.

4.6. Enforcement

Enforcement of IP rights is a powerful tool in the hands of IP rights holders, providing them with the means to protect their brands and products. This is also true where IP rights protect NTs, although due to the nature of certain NTs, specific considerations can arise when determining how best to enforce IP rights to ensure the most effective protection. Other challenges will depend on the IP right at hand. Many of the challenges relating to enforcement of IP rights in the NT world apply regardless of which NT is at hand; however, where challenges relate to or are especially relevant to a specific NT, this is identified below.

Jurisdiction

IP rights are, by their nature, national rights. This means that any enforcement actions will be required to be brought nationally. The challenge that this poses to those seeking to enforce IP rights in the NT context arises due to the fact that many NTs have a cross-border element to them. For example, the decentralized nature of DLT/blockchain means that the networks involved in the technology could be based in different jurisdictions. Similarly, with regards to AI, it may be that a company uses a data center in another jurisdiction. For all NTs, manufacture may take place in a separate jurisdiction to where the NT is ultimately used or sold.

First, this means that a company looking to enforce IP rights in relation to their NT needs to ensure that it has adequate protection in its key markets, including in all of the jurisdictions where the NT is operating. Here a distinction needs to be made between registered and unregistered IP rights. In relation to the former, it is important for businesses to ensure that they have applied for those rights that can be registered in key jurisdictions. Unregistered rights, on the other hand, will arise automatically, provided the requirements for subsistence are satisfied. However, in both cases we discuss elsewhere in this paper the possible difficulties around the subsistence and/or ownership of IP rights in relation to NTs, which may differ depending on jurisdiction. This in turn could have ramifications for enforcement if it leaves companies without any IP rights to enforce in key markets.

Second, as NTs have a cross-border element, any infringement of those NTs may also involve a cross-bor-

der element, meaning that multiple actions may need to be brought in different jurisdictions. This is particularly true where the infringer manufactures the underlying technology in a different jurisdiction to where the NT is ultimately used. This greatly increases the cost of enforcement for rights holders. In addition, depending on the IP right at issue and the jurisdiction concerned, there could be a risk that if different parts of what would be considered the "infringing act" take place in different jurisdictions, a rights holder could be prevented from bringing an infringement action and recovering any applicable damages if all elements of the infringement do not take place in that jurisdiction.

Liability and Evidence of Infringement

A key determining factor in the success of enforcement of IP rights is identifying who is liable for infringement and obtaining evidence of acts of infringement. The first question to determine is what the IP rights in issue actually cover. For example, a business may be able to patent its online payments process. However, if the invention resides in the backend of the underlying technology, obtaining evidence of infringement will be challenging (in that case, trade secrets may be a more suitable means of protection). We discuss elsewhere in this paper the challenges that arise in relation to each IP right, and such challenges will be relevant when it comes to enforcement.

In terms of identifying who is liable for infringement, as discussed elsewhere in this paper, NTs seek to produce machine-to-machine communications with little or no human intervention, which creates challenges when it comes to determining against whom enforcement measures should be taken (and conversely, for users of NTs, challenges in determining when they may be liable in the event of inadvertent infringement of third-party IP rights, for example by an AI). It is likely that as NTs advance even further, these issues will be exacerbated.

A further challenge is the complex multi-party ecosystem in which many NTs operate. For example, in AI, the system relies heavily on the quality of the data input into the system, which may come from multiple sources. In addition, other parties will be involved in developing the algorithm used by the AI for processing and developing the outputs required. The law is currently unclear against whom enforcement could take place in the event of an infringement of third-party IP rights by the AI. It is likely that it may be against the party deemed to have most control over the system, but as detailed elsewhere, as AI systems become more advanced and have less human intervention, this question will become more difficult to answer. Change to the legal framework around liability for use of AI is expected in the EU and is welcomed to provide more certainty for businesses and users of AI.

IP rights holders need prima facie evidence of infringement in order to bring a claim and producing the necessary evidence can be a challenge in the context of NTs. For many NTs, this requires reverse engineering the technology, which can be time-consuming and costly. Notwithstanding time and cost, for some NTs, it may not even be technologically possible to reverse engineer the technology. For example, as mentioned elsewhere in this paper, even now, the nature of AI technology means the decision making of some AI systems cannot be reverse engineered to determine how or why circumstances gave rise to liability or possible infringement of third-party IP rights. Without the required evidence, it may be difficult for rights holders to commence infringement proceedings. In order to ensure that NTs continue to be developed and that those who invest in NTs can obtain protection that can be adequately enforced, a new approach to the evidential requirements of infringement for NTs should be considered. Also, existing processes for obtaining evidence via court proceedings should be instated in jurisdictions where this is missing and made to be more efficient in those where it is a reality.

In a similar way to AI, DLT/blockchain gives rise to liability and evidential issues due to the fact that no central body or individual has control of the process. Therefore, where something goes wrong or third-party IP rights are infringed, it may be unclear how and where it went wrong and who should be liable. In these circumstances, it is not clear how the law would address liability. As with AI, and particularly given the wide range of industries in which DLT/blockchain may be deployed, legislative intervention specific to DLT/blockchain would be welcome.

Standard Essential Patents and NTs

Standard essential patents ("SEPs") are those patents that protect technology believed to be essential to implementing a standard. Previously considered to be the domain of telecoms, as NTs become more reliant on standardized communication technologies, many companies involved in NTs will find themselves grappling with the concept of SEPs and the enforcement challenges that come with them.

One such challenge is the fact that national courts may be willing to determine the royalty rates and terms of a 'FRAND' (Fair, Reasonable and Non-Discriminatory) licence, however on a global basis, as was seen in the *Unwired Planet v. Huawei* decision before the UK Supreme Court. This poses a challenge to multi-jurisdictional court proceedings. Also, for companies that may not be used to operating within the ambit of FRAND licensing, this may require a change in business practices.

Indeed, how the concept of FRAND will apply to NT industries is something that will inevitably be de-

veloped through the courts as SEP licensing disputes arise. Guidance advanced by the industries themselves may assist in shaping how questions of law around SEPs and their licensing will be decided.

Trademarks

A particular consideration for the enforcement of trademarks in relation to NTs arises where the infringement relates to similar marks used in relation to identical goods or services, or similar marks used in relation to identical or similar goods or services where there is the additional requirement of a likelihood of confusion on the part of the public.

NTs engage consumers in new ways. For example, trademarks may be presented to consumers through an algorithmic formula so that the public may take a more passive role in product selection. This raises the question of whether the current test of likelihood of confusion is adequate or whether a different or additional layer to the test is required to account for the new approach of public engagement.

In addition, where human intervention is lessened and trademarks are presented purely through algorithmic formulas, the question arises whether that can be said to be use of the trademark in the course of trade. Again, whether a different test is required for NTs should be considered.

Relief

Enforcement of IP rights is only as useful as the relief that one can obtain through such enforcement. Although this is true of all technologies and industries, there are particular considerations in relation to NTs.

The cross-border element of NTs referred to above could give rise to challenges where it comes to obtaining and enforcing injunctions, a relief which is traditionally a national right. The ability of, for example, servers to be located anywhere in the world could lead to ease of circumventing injunctions. Whether a similar mechanism to the website blocking injunctions seen in relation to piracy could be developed, and whether it would be effective in the context of NTs remains to be seen.

In relation to damages, we discuss elsewhere in this paper the difficulties in valuing some NTs, for example with data. This could be problematic when it comes to claiming damages for infringement as the true damage may be difficult to ascertain. A further challenge arises in the context of the multi-party ecosystem that comes with many NTs. For IP rights holders, it is important to start an infringement action against a party that has the ability to compensate you for lost damages. Where various parties may be involved in the development and use of infringing NTs, it could be difficult to determine: (1) who would be considered to be the infringer under law; and (2) who the most profitable 'infringer' is for the purposes of claiming damages. If the law does not provide rights holders with the ability to recover damages, the utility of IP rights could be called into question (although injunctions may, in some cases, be an adequate remedy in and of themselves).

Conclusion—Enforcement

Enforcement of IP rights is of fundamental importance to give companies protection. It is clear that in the context of NTs, specific challenges can arise when it comes to enforcement. Those involved in developing NTs will need to ensure that they have adequate protection across all jurisdictions in which the NT operates or where it is manufactured. However, there is only so much that rights holders themselves can do to protect their position. From our discussion above, it is clear that guidance, developments in case law, and/or legislative intervention may be required in order to ensure that IP rights can be adequately enforced in the context of NTs.

5. Conclusions

NTs are indeed changing the pace at which human beings inter-relate in society, generating a huge impact as new products and services are rolled out, offering capabilities not possible or even foreseen before.

The natural evolution in integrated circuit processing, unlimited memory storage, and ever-increasing communication speeds provides possibilities to collect and analyse data in an immense quantity. This natural evolution has allowed other technologies to finally come to fruition, such as AI, permitting AI to be implemented in a multitude of real-life applications, providing solutions which, otherwise, human beings would not be capable of delivering. Another example is automatization, where routine repetitive activities can be better performed not only by robots, but by computer algorithms. Finally, the appearance of DLTs/blockchain promises to facilitate the convergence of many of these implementations, as it enables the programming and running of machine-to-machine interactions and communications in the IOT.

We do not know yet how these NTs will change our society in the coming decades. However, it is sure that a plurality of solutions, extremely useful for society, have been and are being developed. The developers, always the main motivators of technological change worldwide, need the adequate support for bringing these products and services to market. In this context, adequate means, in particular, updated.

From the existing instruments offered by the IP framework, as discussed in this paper, it seems that patents and licensing are the ones most affected by the intrinsic properties of NT-based developments.

The usefulness of patents, as the IP right that is directed to the technological content of an NT-develop-

ment, is, at present, being tested. If the various global patent frameworks do not take into consideration the differences between NT developments and traditional ICT inventions and internalize these differences somehow into their framework (if not by adapting the law, then by adapting their regulations, or even practice and procedures), it might very well be possible that patents will stop being an interesting support for the NT developers to depend on for furthering the implementation of their products and services.

Although the trade secrets framework, as such, does not seem to be heavily impacted by the intrinsic properties of NT-developments, it does seem to be the immediate alternative for those NT developers who see difficulties in patenting their NT-developments. Although it is commonly known that keeping a secret from spreading is extremely hard, it is a readily available solution in the short/medium term to proceed with product development without worrying about the short-term implications of an IP strategy. The downside: keeping progress as a secret does not benefit society as a whole.

Copyrights, being automatically recognized IP rights, are commonly used, in particular, for software developments underlying all of the above-mentioned NTs. Within the open source community, the "Copyleft" variants are also highly popular tools. Although these variants do permit the fast propagation of the software, it is not clear how useful they are to NT developers who need a return on their investment, in case their particular NT development has required considerable investment in resources (time, people, and money). Most longstanding products and services have historically required such considerable investment and a corresponding monetization strategy. Similar to copyright, the trademarks framework does not seem to be impacted by the intrinsic properties of NT developments.

On the other hand, the licensing framework definitely needs to take into account several aspects mainly related to the collecting, ownership, and contracting of data, and of data generated by a machine, or input to a machine and output from a machine. Personal data are being regulated worldwide, however, ongoing discussions exist on the need for a new type of IP right that would cover non-personal data, the type generated by sensors or algorithms. The fact is that an innovative device or method can generate readily identifiable data, which in the digital economy will have an economic value. The transfer or licensing of industrial (non-personal) data will be part of interactions between entities forming different parts of a value chain based on the processing of data and information it contains. Furthermore, there is a grey zone when it comes to dealing with machine-generated products and services, such as liability. This grey zone seems to worsen when considering a typical NT system, wherein the whole system is made up from a plurality of sub-systems from different NT developers. The legal implications will need to eventually be ascertained in order for these contracts to be functional.

LESI, as a world-leading association of experts in technology transfer, is continuously monitoring the health of the IP framework. Whereas we acknowledge the aspects of the IP framework that are working well and catering adequately for the creative community, it is also our task to identify aspects where the current IP framework is falling short in its function to support bringing the best of development to market, and therefore, eventually, to positively impact society. The job of bringing implementations to society is tough, and the developers need the corresponding support in this journey, not further hindrances. Hopefully this overview has shed some light as to possible potential areas where the IP framework is lagging behind, and probably should keep up to pace with the specific areas of technology that will govern our lives in the not-so-far-away future. ■

Available at Social Science Research Network (SSRN): *https://ssrn.com/abstract=3946536*