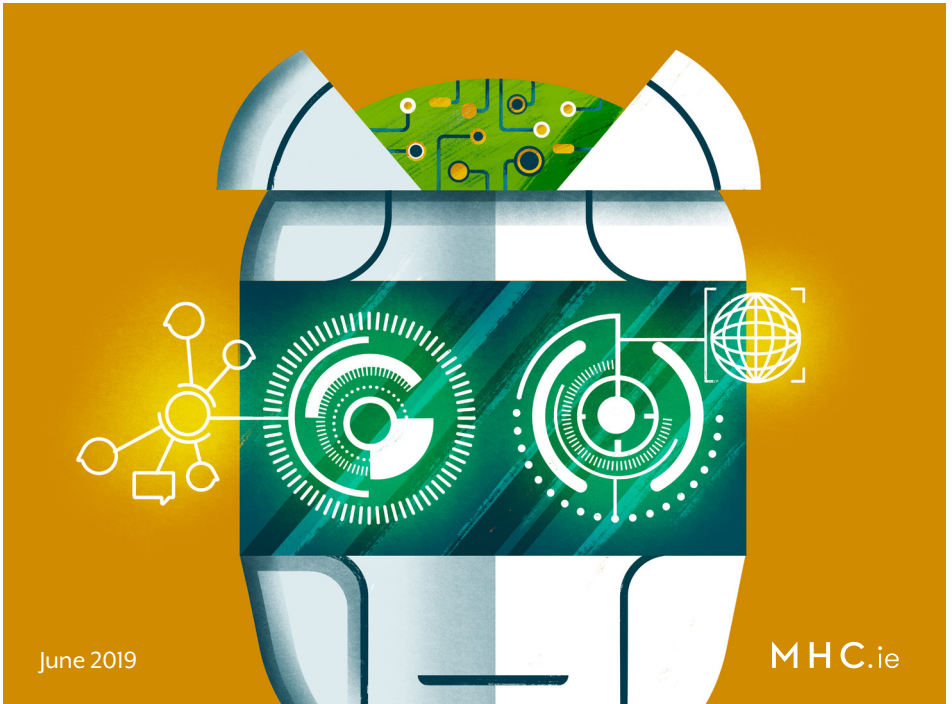


MASON  
HAYES &  
CURRAN

# Artificial Intelligence

Overview



June 2019

MHC.ie

## What we do

Our team is recognised as a world leader for technology law. Our lawyers provide cutting-edge advice on a range of complex matters to the world's leading tech and data driven companies.

We regularly advise social media and financial organisations along with high potential startups and multinationals. From first round funding to strategic outsourcing partnerships, intellectual property management or global privacy protocols, we give the smart advice our clients need.

We specialise in solving complex problems and foresee the challenges that clients experience in this fast moving sector.

## Our expertise

- Information technology
- Cloud computing and data hosting
- Outsourcing and shared services
- Intellectual property and licensing
- Service level agreements
- T&Cs of website use and online sales
- Product licensing
- Data privacy
- Irish and European regulations
- Consumer protection
- Confidentiality agreements
- Software licensing agreements
- Procurement

# Contents

---

Can Machines Own Copyright in Their Creations?	4
Liability Arising from the Use of AI in Healthcare	7
Artificial Intelligence in FinTech	12
GDPR, Part II? EU Organisations to Face New Rules on Non-Personal Data	17
AI in Commercial Contracts – What You Need to Know	21
The EU Approach – Human Centric Artificial Intelligence	24
How AI is Changing Your Life Every Day	29
Artificial Intelligence and the Irish Approach – AI Island	32
AI Jargon Buster	36

---

# Can Machines Own Copyright in Their Creations?

22 May 2019



The 2017 EU Parliament Civil Law Rules on Robotics concluded with a prompt to the Commission to consider in the future:

*“Creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently”*

Is this open prompt to the Commission in any way grounded in reality? More importantly, how do we now treat those narrow AI machines that are creating masterpieces and writing books? Are they authors or, indeed, can they be authors?

## The expert view

A good place to begin is to check in with some experts in this area. A group of signatories representing AI and robotics researchers, industry leaders, law and ethics experts, health specialists and political leaders have written an open letter to the European Commission urging it to rethink this approach to advancements in AI and robotics. They reasonably maintain that a legal status for a robot cannot be derived from the natural person model. The robot would then hold human rights such as the right to dignity, the right to its integrity, the right to remuneration or the right to citizenship. Neither should it derive from the legal entity model, since it implies the existence of human persons behind the legal person to represent and direct it. And this is not the case for a robot.

The main thrust of views on this topic appears to be as follows:

- To seek to grant some form of “entity” or “agency” status to the narrow scope of AI on offer at present is foolhardy considering the very limited general intellectual capacity of the technology.
- It is misconceived to seek to shoehorn the round peg of general artificial intelligence into the square holes of a “natural person” or a “legal entity” because of the very specific make up of those legal terms.

By this logic current iterations of AI do not have the capacity to own or have rights to work output. Given that true general artificial intelligence is not expected to be with us for decades, or longer, we may comfortably set this argument aside for the short to medium term.

## The author?

So, if a machine can create a masterpiece but there are no reasonable grounds to attribute the work to the machine, who shall be the owner? For this we can look to Sections 2 and 21 of the Copyright and Related Rights Act 2000 (CRRA) where such a scenario was anticipated when the legislation was enacted almost 20 years ago.

Under Section 2 of the CRRA, a “computer-generated” work is one that is generated by a computer in circumstances where the author of the work is not an individual. The author of this type of work according to Section 21(f) of the CRRA is the person by whom the arrangements necessary for the creation of the work are undertaken.

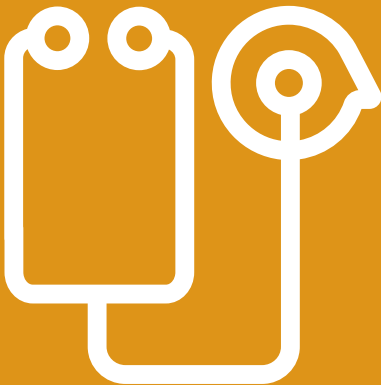
In the absence of significant case law in this area, we shall have to wait to understand how terms like *the arrangements necessary for the creation of the work* will be interpreted. In the meantime, we may reasonably assume that the data scientists and software engineers putting together the models and software are individually and collectively the authors and first owners. As with all software projects that outcome is not workable for the developing entity. As a result, AI projects need to be very clearly scoped when it comes to an understanding of who shall own the outputs from both a data and IP perspective. Attention will need to be paid to local law approaches to IP created by the employee and contractors, similar to the manner in which traditional software is developed.

## Conclusion

By all accounts the scope of intelligence of current AI systems is quite limited although apparently very impressive for dedicated tasks. In most cases this narrow AI provides far superior results to human counterparts. However, it is far too early to speak about these systems in terms of it or them. As a consequence it is also far too early to contemplate machine ownership of IP in AI created works. The issue is further complicated when we consider how even a truly intelligent machine might be able to take on rights and obligations when current legal concepts of a person/entity are at odds with this new technology. We can be sure, however, that this issue will not go away and we should expect significant debate in the coming years.

# Liability Arising from the Use of AI in Healthcare

21 May 2019



From health apps to software medical devices to 3D printing, AI technology is currently on its way to becoming an integral part of our health system. In the UK, the NHS has already partnered with a number of AI companies and has started to test and utilise their products throughout the healthcare system.

Not all AI technology used in healthcare will be classified as a software medical device, and subject to the medical devices framework. Whether a particular AI technology is deemed to be a software medical device will require careful consideration under the Medical Devices Directive[1] and from May 2020, under the Medical Devices Regulation[2]. While this regime seeks to reduce the risks posed by software medical devices as much as possible, there will inevitably be occasions when things go wrong and injury is sustained as a result.

## Is AI a product or a service?

Whether a software medical device or not, one of the key considerations in establishing which liability (rather than regulatory) framework is going to be applicable is whether the AI technology used is considered a product or a service. This classification will depend very much on:

- The precise AI that is used;
- The manner in which it is used; and
- Whether it is used with or without hardware.

If the AI used is ultimately deemed to be a product, then it will be subject to the product liability framework.

## EU Product Liability Directive

The EU Product Liability Directive[3] (PLD) relates to “products” which are defined in Article 2 as “...all movables...even though incorporated into another movable or into an immovable.” “Movable” is not defined in the PLD which has led to uncertainty around whether it can apply to intangible things such as software[4].



If the PLD is applicable, then the AI developers or manufacturers - and in some circumstances, the suppliers/distributors - will be subject to the strict liability regime. Although fault is not a requirement, consumers (patients) must still prove defect, injury and a causal link.

## Determining defect

In determining whether the AI technology is defective, the court will consider the level of safety a consumer is entitled to expect. Complex issues arise when determining what the defect is in the AI technology. Identifying the actual failure may be particularly difficult given the potential sources of defect. Sources might include:

- Fault(s) in the underlying algorithm
- Corrupted training data
- Insufficient training data in the algorithm
- Misuse of the AI machine
- Hacking of the data or the machine
- Faulty hardware
- Clinician error

## Patient protection and safety

Determining what level of safety a consumer is entitled to expect from AI technologies is going to be very challenging in reality. This is because in many cases, all aspects of its operation are not fully understood by the majority of developers, users or consumers. Further, if the AI is replacing the decision making of a doctor, is the level of safety one is entitled to expect safer than, or equivalent to, that expected from a doctor? Do we need to look at how a reasonable AI machine operates? Are AI machines allowed to “have a bad day”? These are all issues which will ultimately need to be played out in court.

The statutory defence which we are most likely to see relied upon in these claims is the development risks defence. This defence relates to instances in which the risk was not reasonably foreseeable at the time of development of the AI technology and/or that the AI technology was developed in line with the relevant industry standards at the time of development. This, however, does raise the question of whether industry standards can keep up with technology developments to the extent they need to, in order to protect the public.

## Negligence

Manufacturers, as well as repairers, installers, suppliers and others may be sued in tort for reasonably foreseeable damage caused to those to whom they owe a duty of care. In negligence claims, the reasonableness of the conduct of the AI manufacturer will be under scrutiny rather than the level of safety a consumer/patient is entitled to expect. However, claims based in negligence are not without their difficulties either. Given the pace of change, trying to determine what might be “reasonable” at a particular point in time, may be exceedingly challenging.

In the event of a defect causing injury, the extent to which the manufacturers of the AI technology warned of the risks will likely also be heavily scrutinised. Whether these warnings will ultimately feed into consent processes undertaken by clinicians to patients remains to be seen.

In addition, clinical negligence claims against doctors could arise in the context of their use of an AI product or software medical devices for myriad reasons. For example, consider an instance in which an app employed by a doctor gave an apparently incorrect dosage calculation. Perhaps the doctor should have noticed the error and failed to address it. Perhaps the doctor forgot to implement a critical software update; or maybe the doctor inputted erroneous information into the software which then led to an incorrect calculation. Alternatively, perhaps the doctor was responsible for a clinical error unconnected to the AI or software. This may have broken the chain of causation arising from the AI software failure, meaning that ultimately it was their actions that caused the harm rather than the AI.

## Contract

Contractual liability will inevitably arise given the various contractual relationships entered into around the use of AI in healthcare. Contractual provisions will need very careful consideration to ensure that warranties, liability, indemnity and limitation clauses are appropriately in place. For example, these may be between the AI software manufacturer, the hardware manufacturer, the hospital authorising its supply, etc.

## Conclusion

Manufacturers and users of AI in healthcare need to be aware of the potential liability frameworks they could be exposed to. Whether the existing product liability framework remains fit for purpose in its application to AI remains very much under review.

# Artificial Intelligence in FinTech

21 May 2019



The EU has been focusing on AI regulation development. The European Commission's High-Level Expert Group on Artificial Intelligence delivered its Ethics Guidelines for Trustworthy AI in April 2019. The guidelines build a horizontal foundation for AI, applying to all sectors, but it is recognised that a sectorial approach may be needed.

Domestically, the Central Bank of Ireland has recognised that regulated financial service providers (RFSPs) are considering the introduction of further technological innovations, including AI, but have not yet provided any standalone guidance for its use in the financial services industry.

## The use of AI

With the capabilities of AI constantly evolving, it is predicted that AI will revolutionise the financial services industry in the coming years. Financial decisions which were previously made by human beings will be capable of being made through the use of AI. Examples might include decisions as to whether to grant credit to consumers, and under what terms, or decisions as to what products should be offered to certain consumers.

AI is also becoming increasingly relevant in the area of robo-advice. This is where investment advice or portfolio management services are provided through an automated or semi-automated system. Essentially, this automated system can use AI to produce its advice and services.

## Regulation

The EU and UK have been taking steps towards standalone regulation for AI, so we may see Ireland follow suit in future.

There is no prohibition on the use of AI by RFSPs. However, they must comply with their general obligations, including the GDPR's rules on automated processing in Article 22, and have the necessary systems and controls in place to ensure appropriate oversight.

## MiFID II

Robo-advice qualifies as “investment services” within the meaning of MiFID II, so RFSPs providing these services will need to make sure that their use satisfies the suitability requirements set out in the Directive.

MiFID II also imposes prescriptive rules on “know your client and know your product”. As part of this, RFSPs may design questionnaires to be completed by clients to assist in a suitability assessment. While the extent of the information gathered must be proportionate, it is important that they gather all the necessary information from the client.

Clients must be given information about the suitability assessment to help them understand the purpose of the requirements. As robo-advice and AI are new technologies, additional information needs to be given to clients to satisfy the RFSPs’ obligations. These include:

- Explanations of the degree and extent of human involvement
- The fact that their answers will have an impact on determining the suitability of investment decisions, and
- A description of the sources of information used to generate investment advice or to provide the portfolio management service

## Questionnaire design

In the context of robo-advice and AI, where there is limited human interaction, the design of the questionnaire is of particular relevance. RFSPs must ensure that the information gathered allows for advice which is suitable for clients on the basis of their knowledge and experience, financial situation and investment objectives and needs. The questions should be sufficiently clear and the questionnaire should be designed to require additional clarification where necessary. RFSPs should also consider whether they need to make human interaction available for clients when responding to the questionnaire, or whether additional steps need to be taken to address inconsistent responses.

## Consumer Protection Code

Similarly, where a RFSP is subject to the Consumer Protection Code in its dealing with customers, it will need to make sure that its use of AI satisfies the “knowing the consumer and suitability” rules.

Before offering, recommending, arranging or providing a product or service to a consumer, RFSPs must have sufficient information gathered to ensure that the product or service is suitable for the consumer. The type of information they must have gathered relates to consumers’ needs and objectives, personal circumstances, financial situation and their attitude to risk.

Therefore, in the context of AI, RFSPs will need to make sure they have sufficient human oversight of the process to make sure that the necessary information is being gathered and considered in the decision making process. Adequate systems and controls will be needed to demonstrate compliance.

## Outsourcing

As fintech and regtech firms are typically more advanced in their understanding and development of innovative solutions, the Central Bank has recognised that it is expected that RFSPs will likely outsource to them when it comes to innovations like AI.

To comply with their regulatory obligations when it comes to these outsourcing arrangements, RFSPs need to ensure that they have the appropriate level of oversight and risk management in place with robust outsourcing obligations applying.

## Innovation Hub

The CBI has responded to the increasing focus on FinTech and recognised the need to engage with innovators and experts in the field. An Innovation Hub has been established for RFSPs to share information and engage directly with the Central Bank outside of the existing formal regulatory engagement process.

The Central Bank has reported a steady flow of engagement with the Innovation Hub, which is facilitating a more complete view of how innovation is unfolding and likely to impact the financial services industry. The Innovation Hub is supported by an internal FinTech Network drawing on expertise from over 20 divisions across the CBI, helping to disseminate the information across the organisation. The Central Bank has also been hosting regular FinTech and innovation events, including an Innovation Hub event focusing on RegTech, with presentations by a number of RFSPs on their business models and use of technology.

The Innovation Hub is being used by the Central Bank to gain a full understanding of the relevant technological developments and innovations, including the use of AI, so that regulation and supervision can respond accordingly.

## Conclusion

The EU is pursuing a comprehensive action plan for the development of AI.

In the meantime, it is important for RFSPs to ensure that they have adequate systems and controls in place to ensure their use of AI complies with their existing regulatory obligations. Existing policies and procedures should be reviewed to ensure they are consistent with AI use. It is important also that management responsibility is clearly outlined, with management being capable of understanding AI capabilities and how to challenge its operation.



# GDPR, Part II? EU Organisations to Face New Rules on Non-Personal Data

21 May 2019



The near supersonic growth and expansion of digital technologies – particularly artificial intelligence, machine learning, the Internet-of-Things (IoT) and 5G-enabled services – has resulted in considerable quantities of non-personal data being amassed throughout the EU. In order to retain a strong competitive edge in the expanding international digital ecosystem, the European Commission has introduced a new Regulation governing the free-flow of non-personal data within the EU. It is hoped that this framework, by blocking data localisation techniques implemented by EU Member States, will help secure competition and ensure the growth of technological innovation within the EU, marking another major step in the Commission's European Digital Single Market strategy.

## What is non-personal data?

The Regulation itself avoids a definition for non-personal data. It instead piggybacks on the GDPR by defining non-personal data as any data not falling within the definition of personal data under the GDPR. Given this definition's considerable breadth, the Regulation gives examples of non-personal data as including:

- Anonymised or aggregate datasets for big data analytics; or
- Industry-specific data.

Industry specific data, for example, can be data on precision farming used to monitor and optimise agricultural practices. It could also describe machine-generated data which is non-personal in nature. This would include data on equipment maintenance needs for industrial machinery.

By blocking EU Member State localisation restrictions on the storage and processing of non-personal data, the Regulation will have a major impact on a number of industries that operate in the AI and machine learning sector, including businesses in construction, financial services, healthcare, agriculture and technology industries.

## Main changes

The Regulation prohibits Member States from running mandatory data localisation requirements in relation to non-personal data throughout the EU.

For example, a legislative measure requiring that health data generated in Ireland or relating to Irish citizens be processed and stored in Ireland would be prohibited under the Regulation.

The new Regulation is set to have a wide-ranging impact on a number of EU organisations, and often, data localisation restrictions are viewed in parallel with data security issues. For instance, customers of an IT service provider might indicate a preference towards locally stored data and show mistrust in its cross-border storage. However, the Commission's view was that the legal uncertainty in this area would only stifle both the modernisation of EU data services and the competitive strength of European businesses.

In creating a more enhanced mobility framework for non-personal data, the Regulation will:

- Safeguard the free movement of non-personal data throughout the EU
- Secure data availability for regulatory purposes
- Encourage self-regulation for the porting of data

## How will the Regulation impact my organisation?

The Regulation comes hot on the heels of the GDPR and introduces a new layer of regulatory compliance of which organisations must be aware.

For both organisations and customers, the Regulation is set to better facilitate the competitive operation of the EU Digital Single Market and ensure the availability of secure, reliable and affordable cloud services for users. It will improve cross-border commercial activities for organisations that process non-personal data and increase business stability, particularly for start-ups and SMEs, who already face existing challenges in establishing themselves within the digital market.

Interestingly, unlike the GDPR which is enforcement-centric, the Regulation affords Member States manoeuvrability in terms of imposing penalties on organisations for failure to comply with access requests from competent authorities.

## Challenges ahead

There are a number of interpretative and practical challenges ahead of the Regulation's implementation. For example, the Regulation does not make it clear how it is set to interact with the GDPR and many organisations may find that certain datasets in their control often contain a complex mix of personal and non-personal data. For those organisations, compliance with both the new Regulation and the GDPR may be a challenge. It is expected that the Commission will publish guidance for organisations shortly which will address this issue as well as other areas of concern.

## Conclusions

The new Regulation, in bringing down existing barriers to the mobility of non-personal data, has re-iterated the Commission's strong drive towards Digital Single Market reform which will continue over the coming years. While the legislation is welcomed as it looks to ensure legal certainty, greater market integration and a level playing-field around the processing of non-personal data, its implementation over the coming months will not be without its practical challenges.

# AI in Commercial Contracts – What You Need to Know

21 May 2019



Significant attention has been drawn to AI in the context of headline areas such as data protection and cyber security. However, one of its most practical applications to date in the legal industry has been for commercial contracting. In particular, the drafting and negotiating of commercial contracts for AI-based products and/or services has given rise to specific consideration given the nature of the technology and its potential impact within the business. We focus on the areas of disclaimers/ insurance, confidentiality and audit rights and AI and the legal liability problem.

## Disclaimers and insurance policies

This issue should be considered carefully in any contract for an AI service. An AI supplier will generally seek to provide the AI service with limited guarantees related to the standard of service and care should be taken to ensure that the supplier does not exclude any warranties relating to the quality of the AI or its service availability. As AI evolves, there is greater potential for service outages; and the general impact this might have on the wider business should be taken into account, particularly around support services, etc. Customers receiving AI services should also review and negotiate liability clauses with caution, as it is likely that a supplier will have capped or excluded liability for the unavailability of the AI service.

It is also prudent for customers to explore both their own existing insurance policies and also the insurance coverage which their supplier has in place. We have seen a number of instances over recent years where new technologies or risks around the use of AI technology are not automatically captured within existing policies. This is an important consideration and should be explored with the company's insurance brokers.

## Confidentiality or auditing rights

The standard auditing clause in commercial contracts will take on a new dimension in light of AI. This is because the work typically carried out by personnel will be carried out through AI systems instead. Many suppliers will be hesitant of permitting wide audit rights around their AI technology and will usually resist anything that might impact upon their proprietary technology.

As a result, it will be important to ensure that existing audit clauses and mechanics used in standard supplier agreements are examined to ensure they are flexible enough to cover verification of AI-produced results where this is required for internal audit purposes.

Confidentiality issues are another area worth exploring, particularly during the input of business sensitive information within the system. Difficulties can arise for customers to ensure that once an AI agreement has been terminated the information will be deleted from AI systems which are generally, by their nature, built to use and learn from the information which it is processing. In addition, the issue of migration to new service providers can also be potentially problematic. This is because of the proprietary nature of many AI systems and the reluctance of many suppliers to provide any information which might compromise their 'black-box' technology.

## AI and the legal liability problem

AI is not responsible for its own actions because it is not a legal person. As a result, the question then arises as to who bears legal responsibility? Similarly, under the laws of negligence, questions arise around duty of care and other related concepts. This is still somewhat unknown territory and is one of the most debated legal aspects of AI as a whole. Accordingly, it is likely that we will begin to see a new approach to liability clauses and how they are constructed over the coming years in order to address these difficult issues.

## Conclusion

AI is still evolving and we are likely to see a continued diversity in terms of how businesses use and implement the technology into their existing business models. While AI specific commercial contracts are still very much a work in progress, it is clear that contracts being entered into for AI-based products and/or services will require additional consideration prior to drafting. Otherwise there is the potential for contracts to be impractical, not fit for purpose and overall being disruptive to the operations of the business. It is, therefore, possible that these negative factors could negate much of the benefit of moving to AI.

# The EU Approach – Human Centric Artificial Intelligence

22 May 2019





As part of its Digital Single Market initiative the European Commission is putting forward a European approach to artificial intelligence and robotics. It deals with technological, ethical, legal and socio-economic aspects to boost the EU's research and industrial capacity and to put AI at the service of European citizens and economy.

In this article we take a look at the details of a recent Communication from the EU Commission to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Building Trust in Human Centric Artificial Intelligence.

## Background

The EU wants to build an AI regulatory environment in its own image - one based on a set of fundamental values complemented by a strong and balanced regulatory framework. The ground work was completed in December last year when the AI High Level Expert Group delivered its draft Ethics Guidelines for Trustworthy AI. The guidelines focus on human centric and trustworthy AI that produces products that operate in a traceable and accountable manner and are based on a principle of ethics by design.

With the latest Communication, the EU is now moving to the next stage – a targeted piloting phase to ensure that the ethical guidelines for AI development and use can be implemented in practice.

## EU AI strategy

AI can benefit the whole of society and the economy. It is a strategic technology that is now being developed and used at a rapid pace across the world. Nevertheless, AI also brings with it new challenges for the future of work, and raises legal and ethical questions. To address these challenges and make the most of the opportunities which AI offers, the Commission published a European strategy in April 2018. The strategy places people at the centre of the development of AI – human-centric AI.

It is a three-pronged approach to:

- Boost the EU's technological and industrial capacity and AI uptake across the economy
- Prepare for socio-economic changes, and
- Ensure an appropriate ethical and legal framework

## AI and ethics

The EU's view is that the ethical dimension of AI is not a luxury feature or an add-on:

*"...it needs to be an integral part of AI development. By striving towards human-centric AI based on trust, we safeguard the respect for our core societal values and carve out a distinctive trademark for Europe and its industry as a leader in cutting-edge AI that can be trusted throughout the world."*

The Commission explains that trustworthy AI is based on the following key requirements:

**Human agency and oversight** – AI systems should support human agency and fundamental rights and contain appropriate degrees of control measures including adaptability, accuracy and explainability.

**Technical robustness and safety** – AI systems need to be reliable, secure and resilient and have a fall back plan in case of problems. Their decisions should be accurate and reproducible.

**Privacy and data governance** – Privacy and data protection must be guaranteed at all stages of the AI system's life cycle.

**Transparency** – The decisions of AI systems should be traceable and it should be possible to log and document those decisions. Explainability mechanisms should be pursued. Explanations of the degree to which an AI system influences and shapes the organisational decision-making process, design choices of the system, as well as the rationale for deploying it, should be available.

**Diversity, non-discrimination and fairness** – AI systems should be set up so as to avoid harm that will flow from inherent bias, incompleteness and bad governance models.

**Societal and environmental well-being** – The impact of AI systems should be considered not only from an individual perspective, but also from the perspective of society as a whole.

**Accountability** – Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes, both before and after their implementation.

## Pilot and next steps

To ensure the ethical development of AI in Europe in its wider context, the Commission is pursuing a comprehensive approach with its pilot including in particular the following lines of action to be implemented by the third quarter of 2019:

- Launch a set of networks of AI research excellence centres through Horizon 2020.
- Set up networks of digital innovation hubs focussing on AI in manufacturing and on big data.
- With Member States and stakeholders, the Commission will start preparatory discussions to develop and implement a model for data sharing and making best use of common data spaces, with a focus notably on transport, healthcare and industrial manufacturing.

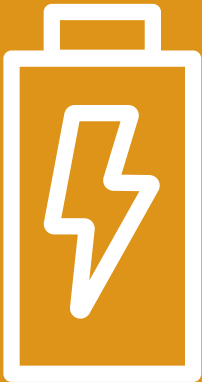
Further the Commission doubled its investments in AI in Horizon 2020 and plans to invest EUR 1 billion annually from Horizon Europe and the Digital Europe Programme.

## Conclusion

The EU's AI plan is ambitious and rigorous in approach. No doubt it will be attacked by critics for being too slow and cumbersome. It could also be criticised for potentially widening the existing gap between the advances in the field of AI being made in the EU and other jurisdictions. However, one could reasonably argue that the long game being played by the EU is a canny approach. In fact, it could trump its US and Chinese competitors in the long run, particularly in a world of consumers that are becoming increasingly privacy-savvy and are conscious of the downsides of owning and using products that require to be fed large amounts of data including personal data. In such a world, trust and not speed is likely to be the ultimate driver of innovation.

# How AI is Changing Your Life Every Day

22 May 2019



The online experience is becoming more and more tailored to suit our everyday needs. Google's AI search engine software can analyse details about you – like your age, location and other personal details – in trying to provide you with the best possible results for your query. We look at four examples below of how AI is changing your life every day.

## Smart travel

AI has dramatically changed both where we go, and how we get there. Apps like Google Maps, for instance, use AI software to tell us how to get from A to B in the fastest time, even if not always in the safest way. Daily travel apps – like Uber, DublinBus or MyTaxi – use AI software and real time information to determine how long it will take your taxi, ride-share, bus or even food delivery to get to you to, and how long it will take to get you to your destination.

AI is also powering many parts of the travel experience, managing things like routes, capacity and dynamic pricing on a real-time basis with minimal human input. Once you get to your holiday destination, travel recommendation apps and technologies, like the Hilton's famous robotic concierge "Connie", embedded with AI software will then provide recommendations for restaurants, hotels, and information on local attractions, making your travel experience as smart and as tailored as possible.

## Intelligent connectivity

Thanks to AI, the way we connect with others online has dramatically changed. For example, algorithmic software can now be used to recognise patterns in your images to offer tagging suggestions. Some apps, for instance, will now even recognise your pets. If you are job-hunting, platforms will use dedicated software to match you with suitable employers, based on your listed skills, experiences and education.

Meanwhile, image-sharing apps are using AI-based tools to identify objects in the images you search or upload so you can easily find more ideas about interior design or home gardening.

Finally, e-mails services will use AI software to detect spam, suggest smart replies like, “Thank you, John, that’s great!”. They can even offer a useful, if not sometimes self-shaming, “nudging” feature that will remind you to follow up on emails from those you’ve ignored or forgotten.

## Enhanced customer experiences

AI software is being increasingly developed to improve your customer experiences. For example, online retailers like Amazon and eBay use intelligent software to collect information about your shopping preferences and buying habits, in order to personalise your online retail experience by providing recommendations and suggesting new products suited to you. Chatbots have become increasingly popular on a wide variety of websites, such as financial services and mobile network provider sites. In ways that often accurately simulate human contact, chatbots are able to analyse words and phrases you use when “chatting” to them in order to deliver you helpful results when in search of answers.

## Music and video streaming

Our everyday video and music streaming services like Spotify, YouTube and Apple Music are each embedded with cutting-edge AI software dedicated to tailoring the online streaming service. Spotify, for instance, offers suggestions for new music discoveries, fresh releases, and even old favourites, based on your listening habits. Netflix will show you its “Top Picks for You” based on the viewing habits you have indicated to your very own digital butler. YouTube analyses data from your search and watch history to recommend videos it “thinks” you will be interested in watching (with almost terrifying – and often unexpected – accuracy).

## Comment

The world of AI and machine learning is a fascinating one but to an extent daunting from a legal and risk perspective.

# Artificial Intelligence and the Irish Approach – AI Island

21 May 2019





There are a number of factors which have neatly converged on Ireland's journey to becoming an AI Island and which point to strong future growth and development of its AI ecosystem. Local economic and education initiatives are complimented by the legal framework being developed by the EU Commission.

## Existing AI island ecosystem

The time and effort of agencies such as ICTSkillsnet, IDA, EI and SFI, and many invested experts, has led to the creation of a burgeoning AI ecosystem. This in turn is beginning to churn out a number of successful Irish AI companies such as Nuritas, Soapbox Labs, Opening and LogoGrab. These efforts are supported by many corporations in Ireland who have established centres for data analytics, cloud computing, big data and future internet. Google, for example, launched a support hub for AI startups in Dublin last year.

The AI agenda is also being driven by a number of key individuals in Ireland and EU. Prof. Barry O'Sullivan of University College Cork is one such individual. He is President of the European Artificial Intelligence Association and a representative on the EU's AI Expert Group which is spearheading the EU's strategy regarding AI. The Group makes recommendations on future policy development and on ethical, legal and societal issues, including socio-economic challenges.

## AI island legal framework

Irish AI specific legislation is likely to almost exclusively derive from future EU ethical and legal developments. AI products and services already on the market are regulated by legislation such as the GDPR, the Data Protection Act 2018, the Copyright and Related Rights Act 2000 and the European Union (Protection of Trade Secrets) Regulations 2018. However, there is a lot more to come from the EU. The EU wants to build an AI regulatory environment in its own image - one based on a set of fundamental values complemented by a strong and balanced regulatory framework. The ground work was completed in December last year when the AI High Level Expert Group delivered its draft Ethics Guidelines for Trustworthy AI. The guidelines focus on human centric and trustworthy AI that produces products that operate in a traceable and accountable manner and are based on a principle of ethics by design.

The EU is now moving to the next stage - a targeted piloting phase to ensure that the ethical guidelines for AI development and use can be implemented in practice. The EU's view is that the ethical dimension of AI is not a luxury feature or an add-on but that:

*"...it needs to be an integral part of AI development. By striving towards human-centric AI based on trust, we safeguard the respect for our core societal values and carve out a distinctive trademark for Europe and its industry as a leader in cutting-edge AI that can be trusted throughout the world."*

Critics will argue that this process is too slow and cumbersome and that it could lead to widening of the existing gap between the advances in the field of AI being made in the EU and in the US and China. In another light one could reasonably argue that the long game being played by the EU is a canny approach which could see it trump its US and Chinese competitors in the long run, particularly in a world of consumers that are becoming very privacy savvy and are conscious of the downsides of owning and using products and apps that require to be fed large amounts of data including personal data. In such a world trust and not speed could be the ultimate driver of innovation. We delve further into these issues in our article exploring the EU's current approach to AI.

## Impact of Brexit and other factors

The instability brought about by Brexit casts Ireland in a very favourable light when it comes to our country's burgeoning AI sector. Ireland's status as the only other English speaking common law jurisdiction in the EU, and possibly the remaining one by the end of 2019, is of great benefit in the context of forging new business relationships. From a technology contracting perspective, our legal concepts are recognised and understood by most foreign investors, including US multi-nationals. The stability offered by Ireland being intrinsically tied into the future of the EU AI legal regime is another positive.

In addition to our 12.5% rate of corporation tax on trading profits which applies to companies that actively exploit IP through Ireland, the Irish tax regime also offers a knowledge development box regime. This regime provides a highly attractive tax rate of 6.25% for income generated from commercialising patents and copyrighted software. This is particularly helpful for AI entities seeking to qualify for relief.

## Investment in Education

The investment in promoting AI in our third level institutions is further a boost. Ireland's first masters degree in AI was recently launched in response to a growing demand by industry for related skills in Ireland. The programme runs in the University of Limerick and includes a fast-track introductory course developed in collaboration with the Irish Centre for High-End Computing. The design of the entire programme is led by ICT companies under the aegis of Technology Ireland ICT Skillnet and the University of Limerick. Companies that have been involved in developing the programme to date include Accenture, Advanced Metadata, Analog, Arvato, Citibank, Ericsson, Fujitsu, GM, Google, IBM, Microsoft, and many more. The speed with which this course was designed and developed on foot of that industry demand is impressive and sends a strong signal to international partners that the Ireland is willing to take specific action to support the AI sector.

## Conclusion

Recent analysis shows that AI will boost Ireland's GDP in 2030 by 11.6% to €48 billion. This presents a substantial commercial and economic opportunity for the country. The Irish AI ecosystem is strong and growing from a collaboration, research, education and economic perspective. So far all the signs are positive that we can live up to the projected growth rates and our growing reputation as the AI Island.

# AI Jargon Buster

23 May 2019

As with all new and emerging themes affecting our future daily lives, manufacturers and consumers are often bombarded with a large amount of unfamiliar buzz words and acronyms. We provide a helpful guide on commonly used AI terms.



## Glossary of terms

**Artificial Intelligence (AI):** broadly refers to the ability of computing technologies and software to simulate human cognition and learning. AI enables machines to perform tasks normally requiring human intelligence, allowing software to learn, reason, interact, and engage in sensory perception and understanding. While there is no universal definition, AI technologies have become ubiquitous in modern life – from Siri, to tailored Spotify or YouTube recommendations, to driverless cars.

**Algorithm:** An algorithm is an unambiguous set of mathematical rules to solve a class of problems which is the key to enabling AI software to problem-solve. For example, if you need to get from A to B on Google Maps, an algorithm exists within the software that will help you work out the fastest route taking into account things like congestion etc.

**Artificial Neural Network:** refers to a network of “neural” layers that are used to allow software to mimic the processes of the human brain. For example, when Google Images needs to tailor its search results to decide whether or not a dog is in an image, the neural network will consider (in nanoseconds) various elements and characteristics of the image (including for example, the arrangement of pixels, instances of light and shadow, notable shapes and even whether or not s/he will have pointy or floppy ears) before making a final decision.

**Autonomous Mode:** refers to the capability of AI software to operate independently without direct human input. Examples of autonomous AI include robots covering deep sea and space exploration, deep learning in medical diagnosis and of course driverless cars.

**Big Data:** refers to unique datasets which are so large or complex that traditional data processing applications are inadequate to deal with them. Examples include financial services using big data analytics software to detect suspicious transactions in the prevention of money laundering, or cutting-edge meteorological models (like IBM Deep Thunder) forecasting weather patterns through high performance computing of big data.

**Blockchain:** refers to a system of secure data storage in which digital transactions made using a cryptocurrency (e.g. Bitcoin) are stored as encrypted “blocks” of data in a secure linear “chain” which is maintained across several computers within a network.

**Chatbots:** these are “chat robots” that converse with human users through text or voice commands, commonly used by websites and online services to mimic human contact for customers.

**Deep Learning:** refers to the ability of AI algorithmic software to recognise patterns within a neural network by extracting features from large datasets, thereby allowing it to closely resemble human intelligence.

**Internet of Things (IoT):** refers generally to the interconnectivity of devices via the Internet which enables them to freely send and receive data between them (e.g. physical health sensors and activity trackers in the healthcare sphere).

**Machine Learning:** refers to the processes by which machines and AI algorithmic software “learn” by example and/or teach themselves to recognise patterns or reach set goals without being explicitly programmed to do so.[1]

**Robotics:** refers generally to the branch of scientific technology focused on the manufacture and design of “robots” which simulate human intelligence and actions. Think C-3PO, but bear in mind that robotic sentience is still a long-way off and most robotics in use today are focused on repetitive tasks such as welding and assembly.

**Virtual Reality (VR):** refers to technologies often using VR headsets which simulate physical, real-world environments by generating realistic images, sounds and other sensations resembling a user’s physical presence in a virtual or imaginary environment.

MASON  
HAYES &  
CURRAN



Ensure you get the legal updates & event invites that matter most to you by joining MHC Brief

**Your Insights &  
Events Community**

Join now at [MHC.ie/BRIEF](https://MHC.ie/BRIEF)

# Key Contacts



---

**Philip Nolan**  
*Partner, Head of Technology*  
+353 1 614 5078  
pnolan@mhc.ie



---

**Mark Adair**  
*Partner, Co-Head of FinTech*  
+353 1 614 2345  
madair@mhc.ie



---

**John Farrell**  
*Partner, Technology*  
+353 1 614 2323  
jfarrell@mhc.ie



---

**Rowena Fitzgerald**  
*Partner, Co-Head of FinTech*  
+353 1 614 5891  
rfitzgerald@mhc.ie



---

**Michaela Herron**  
*Partner, Product Regulatory*  
+353 1 614 5878  
mherron@mhc.ie



---

**Brian Johnston**  
*Partner, Privacy & Data Security*  
+353 1 614 7746  
bjohnston@mhc.ie



---

**Brian McElligott**  
*Partner, Intellectual Property*  
+353 1 614 2199  
bmcelligott@mhc.ie



---

**Oisín Tobin**  
*Partner, Technology*  
+1 415 655 6841  
otobin@mhc.ie

Dublin

London

New York

San Francisco

