Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Robotics and law: Key legal and regulatory implications of the robotics age (Part I of II)

Chris Holder *, *Vikram Khurana*, *Faye Harrison*, *Louisa Jacobs*

Bristows LLP, London, United Kingdom

Keywords:
Robots and law
Autonomous vehicles and law
Healthcare robots and law
Data protection issues in robotics
Intellectual property issues in robotics
Consumer protection issues in robotics
Robotics and commercial contracting

A B S T R A C T

In this edition, we explore some of the legal, regulatory and ethical implications of robots and robotic systems and applications. We begin by giving our view of why this emerging technology will become increasingly prevalent and why it is important that lawyers and regulators play an important role in its development. We go on to address the key legal, regulatory and ethical issues in respect of specific types of robotics, including automated vehicles and healthcare robots. We also focus on the impact that robotics will have on core legal practice areas, including data protection, intellectual property, consumer protection and commercial contracting. Our objective is to identify the key legal and regulatory implications of robotics, and to start a dialogue about how our existing legal framework might need to adapt and change to meet the demands of the robotics age. In the next edition, we will continue our focus on key legal issues in respect of different types of robotics and core legal practice areas relevant to the discussion.

Guest Editorial – David Bisset, Founder of Itechnic LTD**

Robotics and autonomous systems is being hailed as the fourth industrial revolution. Its impact will be felt more widely than either the computer or communications revolutions that preceded it. This special edition explores this impact in the context of the law and the role the law will have in shaping products and services that employ robots and deliver autonomy.

While the computerisation and widespread communication of data has transformed and disrupted various industries, the addition of systems able to make autonomous decisions, build knowledge from unstructured data and act physically in the world has the potential to be highly disruptive, both of existing value chains and through the creation of novel and innovative products and services. Mixing this technical disruption with economic and demographic pressures and changes to the global flow of trade the effect of autonomy and robotics will be far reaching: in the home, at work and in our cities, hospitals, farms, supermarkets and in the infrastructure we rely on.

There are indications that people are becoming less trusting of technology, more wary of its long term impact and particularly so of "AI"-based technologies that appear, or are portrayed as, intrusive and controlling. They are beginning to understand that their personal data is valuable and that it can be used profitably by others. Robots will be able to collect data

* *Corresponding author.* Bristows LLP, 100 Victoria Embankment, London, EC4Y 0DH, United Kingdom.
E-mail address: chris.holder@bristows.com (C. Holder).

** David Bisset has worked in robotics for 24 years. The founder of iTechnic Ltd, he is currently responsible for the Strategic Research Agenda, the Multi-Annual Roadmap and the work programme focus for robotics in Horizon 2020 for euRobotics aisbl, the private side of the Robotics Public Private Partnership, SPARC, within the RockEU coordination action. He currently chairs the Robotics and Autonomous Systems Advisory Board (RAS-SIG-AB) under the KTN/Innovate UK, contributed extensively to the recently published UK robotics strategy (July 2014) and was responsible for the UK robotics landscape document.

http://dx.doi.org/10.1016/j.clsr.2016.03.001

and more importantly contextualise it, on a scale never before possible. In return we will be offered new kinds of services that filter choices, interact sympathetically and reduce complexity. Robots will become the tools that we use to increase productivity, utility and efficiency; robot vacuum cleaners have already saved millions of hours of time. But within this there will be a digital divide, work patterns will favour flexibility and those that can retrain, products will persuade, perhaps unethically, and autonomy will replace human centred services based on cost alone. User acceptance will be critical to uptake and acceptance will be based on trust.

Effective law and regulation create trust, and for robotics to grow and develop trust will be an important commodity: trust in brands, trust in functions, trust in privacy, trust in a fair market. While current legal frameworks are robust enough to handle some of the challenges that autonomous and robotic products and services will bring, they will need to adapt and develop to respond both to new areas of commerce, government action and personal choice.

Robotics and autonomous systems are at very early stages of development and it will be at least a decade before the full extent of this impact is felt. Yet we can see now the first stages of this revolution; how it will change travel, how we are cared for and how we work. The technical impact cannot be treated in isolation; there will be an accompanying socio-economic impact: on value chains and on people. With these changes comes an expectation that the law will protect and regulate. This special edition begins to set out how that might happen and where the focal points of change might be.

1. Introduction

Like all new technologies, robotics will go through a series of stages before it eventually becomes mainstream.

As of now, 2016, this new technology is in the midst of rapid growth, rapid advancement, huge public interest, spurious reporting and a general lack of appreciation as to its capabilities.

From the sensational headlines of 'Killer Robots will destroy Humanity' to more mundane matters of software programmes which replicate previous human tasks and thus replace a person inputting data, the robotics industry is at a nascent stage of development and understanding.

This is precisely why it is now that legislators, regulators, scientists, philosophers and anyone else who is interested need to understand the importance to the future development of society of such technologies and the inherent dangers associated with some of the disciplines that contribute to the general definition of 'robotics'.

It is not very long ago that computers were seen as machines that boffins played with in the basements of big government buildings and therefore were of little, if any, relevance to the way people lived their daily lives.

Spring forward to the mid-1990s and you have the development of the home PC, networked computing, the internet and e-commerce. These, coupled with later developments around mobile technologies and social media, have completely changed the way we communicate, the way we do business and the way we access information.

Traditional industries – publishing, advertising, banking – have all been affected to a greater or lesser degree and some been changed forever, for example the music industry. New industries have been created and giant companies established in less than a decade (Google and Facebook, for example).

Robotics will have a similar impact. No longer will robots just sit in fixed positions and build cars – they will interact with humans in the workplace, at home and generally. It is the ambitious aim of our special publication on robotics and law – spread across two editions – to set out some thoughts and guidance as to where such developments will have the greatest impact and deal with how the legal system will need to adjust.

Let us not forget that law has traditionally been quite slow to deal with technological developments – which is hardly surprising given the time it takes to develop good 'law' as opposed to the ever increasing speed with which the digital world is changing. This is not to say that English law, for example, does not have the capacity to deal with new technologies from their inception, because the laws of contract and tort have been developed over hundreds of years to deal with new concepts very easily. This capacity will remain but, of course, where case law cannot develop quickly enough to deal with new situations, then statute and regulation will be required.

The debate has just started and our hope is that it continues and expands in order that the undoubted advantages that robotics technologies will deliver will not be outweighed by the challenges and dangers that will present themselves.

1.1. *What is a robot?*

The definition of a 'robot' as set out in Oxforddictionaries.com is as follows:

> *"A machine capable of carrying out a complex series of actions automatically, especially one programmable by a computer".*

This definition makes it clear that we are talking about a 'machine', which could be anything from a software program to a fully humanoid shaped 'device', just so long as it performs a task or series of tasks automatically without the need for human control or guidance.

There is another definition, however:

> *"A machine resembling a human being and being able to replicate certain human movements and functions automatically".*

This is the more popular understanding of what a 'robot' is but, with reference to the above, it does not tell the complete picture.

Some financial services functions are now performed by robotic software programs without a human being in sight. This function is no less 'robotic' than a humanoid shaped robot answering the telephone with a standard set of responses – all it requires is for the robot to act automatically time and again within its given parameters and in response to external events.

Robots, therefore, have been around for years. The recent raft of publicity, however, is centred not on robots *per se* but on the way that we, as humans, will begin to interact with them. The more technologically advanced the robot is, the more

functionality it has and the greater its ability to do more tasks automatically.

Add this to a greater mobility, the continued development of sensors and the increase in wireless network technology and then, all of a sudden, you have a machine that can move, sense, react and perform tasks. Again, looking back in time, the move of computing away from the standalone mainframe in the basement of a building to a mobile, network enabled computer utilising easy-to-use applications created its own challenges and opportunities. Society had to learn to adapt and understand the impact that such changes would have then and it should be no different now with robotics.

It goes without saying that some robots are more complicated than others. A robot fulfilling one function only on an automatic basis may have less functionality than a driverless car which is travelling the length and breadth of California – but it is still a robot. Much the same as a game of 'brick bat' is a computer game, so is 'Call of Duty' – but one bears little resemblance to the other.

The point being, technology develops. It starts off in a monochrome, 2-dimensional form and develops into an all-singing, all-dancing, 3D, multi-player Hollywood scripted production.

A robot that welds panels to a steel core to make a car is not very exotic. A robot drone that decides when, where and at whom it will send its rockets paints an altogether more dramatic picture.

It is the advance of robotic technology, aligned with the increasing power and miniaturisation of computing, the development of broadband wireless technology and convergence of life sciences and technology that has brought to life a new industry which has the capacity to have a profound impact upon society at large. This new technology is what this edition is concerned with – and the discussion has already started in Europe via the trailblazing Robolaw Project.

1.2. *The Robolaw Project ("the Project")*

The Robolaw Project[1] was started in March 2012, completed in September 2014 and was funded by the European Commission under the 7th Framework Programme for Research and Technological Development ("**FP7**").

The importance of the Project can be seen by the very fact that it was funded under FP7, because this fund, some €50 billion made available between 2007 and 2013, is regarded as one of the key investment initiatives within Europe designed to foster job and business growth and increase Europe's competitiveness in the world.

This is not unlike the strategy[2] adopted more recently by Innovate UK and the UK Government, which has earmarked robotics technologies and manufacturing as being a key area for growth in the coming years.

The Project was commissioned to look at the way that robots and robotics should be regulated in the future and to provide some suggestions and guidelines that might be helpful for legislators and regulators moving forward.

The 215-page report was divided up into four main sections, which looked at the development of robotic technologies in certain areas, namely self-driving cars, surgical robots, robotic prostheses and care robots.

Interestingly, the participants in the Project were very clear that they were not going to concentrate on developing a definition of 'robot' themselves, because of the extremely diverse nature of how robotics is developing – driverless cars, softbots, prosthetic limbs, orthotic exoskeletons, manufacturing robots, lawn mowers, vacuum cleaners etc. – but instead they looked at the peculiarities and differences between each robot group and tried to categorise them by the main features that were common across all forms of robotics. The Project concluded that these features were:

- Use or task of the robot – Robots are used to perform certain tasks and so what is the main purpose or application that the robot is used for? The Project considered there to be two major categories, namely service or industrial use.
- The environment – outside of the robot, where it operates, is this environment physical or non-physical? For example, is it a softbot carrying out functions in cyberspace or is it operating in the physical environment as a machine? Or within biological systems (the human body) as a nanorobot?
- Nature – how does the robot manifest itself? Is it embodied (machines, hybrid bionic systems or biological robots) or disembodied (virtual agents or softbots)?
- Human–robot interaction – this category focuses on the relationship between humans and robots and how one interacts with the other. This would include the proximity of human and robot when in operation and also the interface between the two.
- Autonomy – looks to the level of independence that a robot has during its operation and can be described as full autonomy, semi-autonomous or as part of a tele-operation. This would include a discussion of such diverse items as driverless cars (fully autonomous/semi-autonomous) and the da Vinci surgical robot system, which is operated remotely by surgeons (tele-operation). It would also look at the autonomy of drones, whether fully autonomous attack vehicles or subject to human guidance – although this area was not specifically covered by the Project's remit.

Through a mixture of research and consultation, the Project's aim was to look at the developing technology, understand whether the existing laws in Europe could deal with this technology and whether or not regulations would have to be developed instead.

The requirement for regulation is driven by a number of factors, including: (i) the need for manufacturers to understand the legal framework within which they will operate so as not to develop products that do not sell or which create unacceptable product liability issues; (ii) the need for consumers and society at large to be protected from devices that cause harm or adversely affect commonly accepted rights; and (iii) the need to promote technological advancement and create business opportunities.

[1] Regulating Emerging Robotics Technologies in Europe: Robotics facing Law and Ethics (http://www.robolaw.eu/).

[2] RAS 2020 Robotics and Autonomous Systems – A national strategy to capture value in cross-sector UK RAS innovation pipeline through co-ordinated development of assets, challenges, clusters and skills. July 2014.

All three of the examples given above have obvious merits and the Project attempted to balance the aims of each of these in its research and conclusions. It also had to take into account the many and varied ethical issues that surround robotic technology and attempt to provide some view as to what these are and how best to deal with them.

Each of the core areas that the Project focused on had its own set of ethical issues but certainly those related to healthcare (prosthetic limbs, surgical robots and care robots) contained the most eye-catching, from 'what is it to be human?' to 'should we consign our elderly to be looked after by machines?'

The importance of such debates comes through in the conclusions that the Project drew. Undoubtedly this sector is seen as an important industrial sector for future growth and prosperity, but at what cost?

The Project's view was that regulators have to weigh up many factors but at the heart of their thinking must come a few core principles. These included:

- Robotic applications have to be designed in such a way as to protect the values of human dignity, health, safety and privacy;
- Research and innovation has to be responsibly led and the application of technologies aimed at overcoming human vulnerabilities may require legislators to review their applicability for other uses, for example in enhancing the abilities of the already enabled; and
- Liability: Who is responsible for loss or damage caused by the acts or omissions of a robot? And should robots be treated differently from other machines?

These were by no means the only conclusions but they do provide a flavour of what the Project thought were the major issues coming out of its studies.

This edition will look at different aspects of robotics and so we start with an area which, arguably, has attracted the most media attention – autonomous vehicles, aka the driverless car.

2. Autonomous vehicles

2.1. *Introduction*

In recent years, autonomous (or driverless) cars have moved from the realm of science fiction into the public consciousness. Initiatives for the trial, rollout and integration of driverless cars have been launched in a number of cities and states around the world, including California, the Netherlands, Japan and now four UK cities. The societal advantages of removing humans from the driving seat – such as increased safety, reduced traffic and lower energy use – have been widely written about.

However, such advantages do not mean that driverless cars are necessarily less problematic from a legal perspective. Volvo's announcement in October 2015 that it would assume full liability for any damage caused by its autonomous vehicles does set a very interesting precedent, but further thinking on how such vehicles will affect existing laws is required and so regulators around the world are beginning to grapple with the potential legal, regulatory and ethical issues that are presented by autonomous vehicles.

This section will set out our view of those key issues and some thoughts and suggestions for the approach authorities might take in regulating this emerging technology.

2.2. *Civil liability – who is at fault and who pays for damage?*

One of the biggest legal and ethical issues that arise in any discussion of driverless cars concern liability, in particular, who is liable for damage caused by a driverless car. This discussion largely focuses on vehicles of full automation that are capable of operating on the road network without human intervention. Such vehicles store and use information, make decisions independently and physically act upon those decisions. This means that, as tangible physical objects navigating public spaces, fully automated vehicles are capable of causing real-world damage independently of their manufacturers, owners or occupants. This raises an important legal question: who is liable for such damage? As the technology becomes more widespread over the coming years, the possibility of driverless cars causing damage to property and humans will increase. It may become more difficult to apply traditional legal doctrines, such as product liability and torts such as negligence, to apportion liability in such circumstances.

How well equipped is the existing legal framework to deal with these issues? One line of thought is that our current legal systems and practices are broad enough to adapt to deal with damage caused by driverless cars. This suggests the driverless car is not radically different to other technologies designed to improve automotive safety that have been implemented without requiring a radical reshaping of our liability systems, such as the seatbelt, the airbag, or anti-lock braking. So a driverless car causing personal injury due to a defect would be a product liability issue,[3] imposing strict liability on the manufacturer if the car was not as safe as people are generally entitled to expect.[4] However, this perhaps ignores the fact that the more complex the technology, the greater the gap between people's expectations and its true performance. People using driverless cars may, at least during the initial stages, have unrealistic expectations, or claim they did not (or could not) fully appreciate their safety features. Equally, manufacturers may claim driver-operators could (and should) intervene to avoid damage more than they do so. There are likely to be 'grey areas' where the contributing causes of damage will be unclear. Indeed, the safety expectations are predicated on there being a high take up of the technology (spatially aware driverless cars will be spatially aware of other driverless cars, but cannot anticipate the unexpected). Pedestrians may take more risks and drivers of traditional cars may act more aggressively if they

[3] Council Directive 85/974/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[4] The UK Department for Transport (DfT) seems to agree. As part of its recent review of laws and regulations relating to driverless cars, it said: *"for cars with high automation, we consider that the situation would not be significantly different to the current situation with technologies such as ABS [anti-lock braking] and ACC [adaptive cruise control], where malfunctioning can cause collisions and injuries. It is anticipated that the regime of strict manufacturer liability would continue to apply."*

know that the driverless car is programmed to act within the rules. This problem is usually most acute when a new technology is most nascent; the risks to manufacturers would reduce as people become more familiar with it, but at the start we can expect a lack of clarity and, accordingly, the potential for dispute as to the cause of accidents.

Another possibility that has been posited is to assign some form of legal personality to automated vehicles; a recognition that they can cause damage and loss in their own right. This potentially avoids difficulties around how the legal test for negligence in road traffic accidents would be interpreted, such as whether a vehicle that is programmed to follow the law and Highway Code would be incapable of liability for an accident, or proving which of potentially numerous contributory factors which arise due to the nature of the driverless car product (e.g. defects could be caused by any of several parties including the manufacturer, software developers and the network operator). Allocating legal status to the driverless car itself for the damage it causes also obviates any need to "blame" an owner or manufacturer who may not in any way be guilty for the actions of its driverless car, while at the same time protecting the rights of the equally blameless victim.

How liability for damage caused by driverless cars will be treated has potentially significant consequences for the current insurance system. New insurance products and structures would be needed to cater for the increased responsibility on manufacturers, owners, software developers, network operators, occupants and the other players involved in building and keeping driverless cars on the road. Manufacturers would need cover for liability arising from defects in the technology, while vehicle owners are likely to need "no fault" insurance to cover any injury or damage caused by any other accidents. A possible solution lies in Sweden's current model whereby the compensation and accident prevention functions of insurance are separated, entitling victims to be compensated by insurers and allowing insurers to decide whether to pursue product liability claims against manufacturers based on objective methods (including black box devices fixed in vehicles). The Swedish system is not without drawbacks and is heavily reliant on state funding, meaning that transporting the concept to other jurisdictions may prove challenging.

2.3. *Criminal liability and corporate manslaughter*

In the same way as occupants of vehicles are unlikely to have civil liability for damage caused by a driverless car, they are also unlikely to have criminal responsibility other than in extreme circumstances. Existing criminal offences relating to driving (e.g. speeding, reckless driving) would probably be no longer relevant; however the prospect of criminal responsibility for manufacturers and operators that do not comply with their responsibilities gains more prominence.

Corporate offences would apply to deter wilful flouting of the safety rules – imagine a scenario whereby companies insert software to defeat certain safety standards. Something that is certainly not that far-fetched these days.

Legislators will also need to define appropriate criminal liability for interference with both the systems within the vehicles and the systems in the external environment on which the vehicles depend for safe operation.

2.4. *Driving and road traffic laws*

The current legal requirements governing drivers of traditional cars would not seem appropriate in the age of the driverless car and new requirements would have to be considered if they are to be rolled out to the general public. What type of licence (if any) would be required to operate a driverless car? Should a licence be required for high automation cars in which the human would (in theory at least) never need to take control? If a licence is required, would it be permissible for newly-qualified drivers to operate a driverless car, or should a certain number of years of experience driving a traditional car be a prerequisite? What training should users have to undertake before operating a driverless car and who should provide such training? Would over-regulation in this area negate one of the key benefits autonomous vehicles could bring, the independence it could provide to those who would not be able to operate a normal car (such as the young and the disabled)? Equally, some of the existing driving rules would no longer seem relevant, such as the ban on using a mobile phone while driving[5].

More generally, the basis of current road traffic laws in many countries[6] is that a driver is always needed to be in control of a vehicle. Recent moves to soften this requirement to allow for the evolution of autonomous vehicles have not gone far enough. An international agreement on the best way forward would be the best approach. The UK and the US are signatories to the less strict Geneva Convention, and so may be able to satisfy the requirements with the concept of a 'driver' remote from the vehicle. Regulators will need to clarify the question of what constitutes 'driver' control.

2.5. *Data protection and cyber security*

As with most other connected technologies, driverless cars will collect and analyse personal data, for example to ensure safety and analyse accidents. Also, the integrated set of systems required for a driverless car to work will be vulnerable to malicious attacks by hackers to disrupt, or take over control of, its functioning. Accordingly, many (if not all) of the data protection and cyber security issues discussed elsewhere in this edition that apply to robotics (see section 4 and edition II) will apply equally to driverless cars.

2.6. *Ethical issues*

Much of the discussion around the ethics of driverless cars concerns the inherent absence of a human making moral decisions in extreme situations. Should a driver swerve to avoid a pedestrian at the risk of hitting a car on the other side of the road? Does it make any difference that the pedestrian is a child, adult or elderly person? Many argue that an autonomous car, preprogrammed to behave in a certain way in a given situation, should not be allowed to itself make these ethical choices and that a human driver should always be present to take over the vehicle in extreme situations.

[5] s110 Road Vehicles (Construction and Use) Regulations 1986/1078.

[6] Vienna Convention on Road Traffic of 1968 and its predecessor the Geneva Convention on Road Traffic of 1949.

Driverless car technology is already prominent in the public consciousness. This will only increase as the testing of driverless cars on the roads increases and the first commercial driverless cars become available. Any kind of accident involving a driverless car, no matter how minor, will generate a lot of publicity (certainly if the coverage of incidents involving Google's trial cars is anything to go by). Those which involve serious injury or death in the early stages of the adoption of the technology will generate intense scrutiny and generate concern. A coherent, strategic approach to regulation – preferably at the international level – would stand the best change of striking the right balance between promoting innovation, dealing with liability issues and protecting the public.

In the interim between now and full adoption, perhaps the greatest challenge to regulators is to look forward to full autonomy while partially-autonomous test vehicles are being trialled. As control is slowly removed from the driver, the driver is encouraged to give more control to the vehicle. Perhaps the most dangerous prospect is a failure to address the points on the sliding scale between full control and full autonomy without dealing with all of the potential regulatory and safety consequences presented by the rise of the autonomous vehicle.

3. Surgical robots, care robots and robotic prosthetics

3.1. *Introduction*

The exploitation of robotic technology in the healthcare setting has a great deal of potential and is an exciting area of development. The industry has already experienced the successful implementation of robotic technology, the da Vinci surgical robot being a notable example, and appears to be heading towards a time when robots could play a much larger role in helping to care for and treat a significant portion of the population. This section focuses on three main areas: care robots, surgical robots and robotic prostheses, and gives an overview of some of the legal, regulatory and ethical issues that will become increasingly relevant as robotic technologies play an increasingly bigger role in healthcare.

3.2. *Robots in healthcare*

One of the consequences of the many medical advances in modern society is an ageing population. Care robots have been suggested as a way to help address the growing issue of how to care for the elderly, but the use of care robots is not confined to assisting the elderly – they can also be used to help disabled people or people recovering from injury.

A host of uses for care robots can be imagined, from providing help with everyday tasks within the home, to dispensing medication, bringing food, serving as a memory aid and giving physical assistance[7], helping those in need of permanent care and people undergoing rehabilitation.

Indeed, many such robots have already been developed, and projects are underway to test their use in real-life scenarios. The Giraff[8], for example, essentially a videoconferencing screen attached to a pole on wheels, can move about the home and allow a care giver to see and talk to the patient in their home. The Care-O-bot[9] can move around the home, open doors, and undertake 'fetch and carry' tasks such as bringing the user a drink. Robear[10], an experimental nursing care robot which looks like a human-sized teddy bear, can lift patients from a bed into a wheelchair.

Care robots have obvious potential for assistance with physical tasks but they can also be used in a psychological way. There was widespread news coverage of Paro, the robot designed in Japan which looks like a toy seal, and which a small number of NHS trusts have experimented with to help care for the elderly[11]. It is designed for people with dementia and learning disabilities, intended, among other things, to decrease stress and anxiety and promote wellbeing.

Robotic technology can also be physically integrated into the human body in the form of a prosthesis. Prostheses are already frequently used but the introduction of robotic technology has hugely expanded their potential. The ultimate aim of robotic prosthetics is the replacement of a missing or functionally impaired body part with a robotic body part that entirely replicates (or even surpasses) the natural function of the lost body part. Further, with the aid of exoskeletons, new brain–computer interface technology may allow for individuals with severe spinal code injuries to walk again[12].

While care robots and robotic prostheses are not currently widely used, surgical robots are already fairly widespread in surgery, having been introduced mainly to improve the quality of surgical procedures and the precision with which surgery is carried out. The development of surgical robots is strongly related to the pioneering of minimally invasive surgery in the 1980s[13], where surgery is carried out through one or more tiny incisions, using long instruments and often a camera (laparoscope) to aid the surgeon.

Probably the most well-known surgical robot is the da Vinci system, made by Intuitive Surgical, Inc[14]. Sitting at a console while operating the machine, the surgeon can see a high definition 3D image of the patient and has control over the movement of four robotic arms, three of which are surgical tools and the fourth an endoscopic camera. Some of the advantages over traditional laparoscopy are (i) the 3D image from the endoscopic camera as opposed to a traditional 2D picture, (ii) automatic correction of natural hand tremors, and (iii) a larger number of degrees of freedom of movement.

[7] Robotic technologies and fundamental rights, Koops BJ, Di Carlo A, Nocco L, Cassamassima V, Stradella E, International Journal of Technoethics, 2013.

[8] http://www.giraff.org/

[9] http://www.care-o-bot.de/content/dam/careobot/en/documents/Download/PB_300_309e.pdf

[10] http://www.riken.jp/en/pr/press/2015/20150223_2/

[11] http://www.bbc.co.uk/news/health-34271927

[12] See for example: Demonstration of a Semi-Autonomous Hybrid Brain–Machine Interface Using Human Intracranial EEG, Eye Tracking, and Computer Vision to Control a Robotic Upper Limb Prosthetic, McMullen DP, Hotson G, Katyal KD, Wester BA.

[13] Discussed in Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics.

[14] http://www.intuitivesurgical.com/

In common with most new technologies, however, there are naturally some drawbacks with the da Vinci system. Operating such a sophisticated machine requires training and takes time for surgeons to master. The operation of the robot, and changing and configuring its tools during surgery could make certain procedures longer with the patient needing to spend longer under anaesthetic. Finally, although the 3D image is of good quality, this is very different from the surgeon being able to feel and directly see the body he or she is operating on.

3.3. *Safety and regulatory issues*

In common with the regulation of robots in other areas, there is already legislation in place that applies to robotics in healthcare (see edition II of this publication which will deal with medical devices and the law) to greater or lesser extents depending on the type of robot in question. Two of the most important pieces of legislation in this area are:

- Council Directive 93/42/EEC concerning medical devices (as amended by Directive 2007/47/EC) ("Medical Device Directive"); and
- Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices ("AIMDD")

Robotic prostheses, for example, would be subject to the AIMDD. The AIMDD is aimed at medical devices that rely on a source of electrical energy (or any source of power) for their functioning[15] and that are intended to be totally or partially introduced, surgically or medically, into the human body and which are intended to remain after the procedure[16]. However, the AIMDD does not identify any specific requirements for robotic prostheses and there are no specific safety standards for robotic prostheses that have been developed by standards organisations.

The categorisation and regulation of care robots are slightly more problematic. The definition of 'medical device' in the Medical Device Directive is "*any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:*

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,*
- *investigation, replacement or modification of the anatomy or of a physiological process,*
- *control of conception,*

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means."

Some care robots, such as those which remind users to take medicine, might fall under this definition, but care robots with other functions, such as fetching items from around the home, might not be captured and these types of robots will therefore not be subject to the requirements of the Medical Device Directive.

In the absence of specific legislation, the usual point of reference is the International Organization for Standardisation's ISO 13482:2014[17] standard which has been developed to specify safety requirements for personal care robots. ISO 13482:2014 describes potential hazards associated with care robots and provides requirements to deal with these. By virtue of the fact that they are using a care robot, users will be vulnerable in some way. The automatic nature of a robot, its close (and often physical) contact with a user, and the unpredictability of the user's interaction with the robot are all factors that could increase the risk of the user being harmed by the robot, despite the fact that one of the primary purposes of care robots is to increase safety in the home. It is therefore imperative that, in addition to safety standards, these robots are appropriately regulated.

Surgical robots clearly fall under the regulation of the Medical Device Directive. The da Vinci robot is a Class IIb medical device[18], with corresponding strict controls on their safety. However, there is currently no European legislation governing the training or requirements of surgeons operating surgical robots like the da Vinci. The da Vinci's use is unrestricted and every surgeon is able to use it as he or she sees fit. The Guidelines on Regulating Robotics, a project co-funded by the European Commission within the Seventh Framework Programme ("RoboLaw Guidelines")[19], suggest that a licence should be required for surgeons to operate the da Vinci surgical robot, which would require them to undergo specific training[20]. Indeed, the RoboLaw Guidelines reported that even the surgeons interviewed during that project stressed the need for such regulation. In the meantime, it is up to individual hospitals to ensure their surgeons are property trained. The Royal Marsden hospital, for example, has put in place a Robotic Fellowship for surgeons which could train up to 30 multi-disciplinary surgeons in robotic surgery over the next 10 years[21].

3.4. *Liability issues*

The issue of liability when a robot causes damage or injury is, in common with most robotic applications, an important issue relevant to robots in healthcare.

Using a care robot as an illustration, it is not beyond imagination that a robot lifting a person from a bed into a wheelchair, for example, may injure that person if it malfunctions. If this happened, which party would be liable for compensating the injured person? The party responsible for the harm could theoretically be the manufacturer of the robot, the designers, the party that provided the use of, or sold, the robot to the user,

[15] Article 1(b) AIMDD.
[16] Article 1(c) AIMDD.
[17] http://www.iso.org/iso/catalogue_detail.htm?csnumber=53820
[18] Annex IX of Medical Device Directive.
[19] http://www.robolaw.eu/RoboLaw_files/documents/robolaw_d6.2_guidelinesregulatingrobotics_20140922.pdf
[20] RoboLaw Guidelines, Chapter 3, Paragraph 4.3.
[21] http://www.royalmarsden.org/da-vinci-xi

the people who maintain the robot or even the user themselves, for interacting with the robot in a way that is prohibited by the manufacturer.

The same considerations arise in relation to robotic prostheses. The risks associated with the use of robotic prostheses may be especially high given the fact that they are extremely technologically complex; they are used in a high number of everyday activities and may well be used in ways that were not originally contemplated by the manufacturer.

The introduction of robots into surgery also gives rise to a new risk: the potential that a patient could be harmed by the robot independently of the actions of the surgeon. Between January 2000 and December 2013 there were 144 deaths and 1391 patient injuries and 8061 device malfunctions reported to the FDA's MAUDE database related to robotic systems and instruments used in minimally invasive surgery[22].

The existing product liability framework governed by Directive 85/374/EEC ("Defective Product Directive"), a strict liability regime, is likely to apply to a defective care robot, a defective prosthesis or a defective surgical robot (as well as traditional actions in negligence). A manufacturer is able to avoid liability for a defective product under the Defective Product Directive if the state of scientific and technical knowledge at the time when the manufacturer put the product into circulation was not such as to enable the existence of the defect to be discovered[23] and it is possible we could see an increased application of this defence. There may also be occasions where a user has been injured through their misuse of a care robot or prosthesis, rather than due to a defect in the robot, and in these cases there is an important role for insurance.

In addition to traditional product liability, there are many factors to consider in any actions for negligence. Taking robotic surgery as an example, the surgeons, the hospital, the maintenance teams, the software developers and the networks could all have a possible claim made against them in negligence.

Whether a claim is made under the product liability framework or by actions for negligence, proving the defective nature of complex robotic technology may be difficult.

It has been suggested that surgical robots should contain a 'black box' that would record data relating to the movements of the robot, environmental data detected by the robot, the commands given by the operator and so on. An obvious application of this would be to help to resolve legal disputes if, for example, someone was injured by the robot. However, it could also enable manufacturers to understand how the robot's learning algorithm causes changes in the robot's behaviour. Due regard would need to be had to the data protection issues associated with such recordings and these issues are more fully explored in section 4 below.

The idea of black box recorders is not limited to surgical robots and they could also play a role in many other robotic technologies. In relation to prosthetics, it has been suggested that a black box recorder in a prosthesis would help to investigate the cause of an accident or injury, possibly allowing investigators to detect mechanical or electrical malfunctioning as the cause. However, unlike in a surgical robot, where a relatively large black box, attached to a main power supply would not pose such a problem, any black box in a prosthesis would have to be small, not affect movement, and power supply would be more of a challenge. It is also questionable how easy it would be to detect where the cause of an accident was the user's own actions, or the interpretation of the user's intention by the robot.

It is pertinent at this stage not just to evaluate how we would apply existing liability schemes to robots, but to consider if we need to adapt existing liability schemes, or develop new ones. Under a 'no-fault' scheme, for example, the producer is exempt from all liability, and if somebody is injured by the defective technology, there is an automatic compensation mechanism which could be funded by contributions from all producers of the technology. The advantage of such a scheme would be that it enables the injured party to avoid very complex and lengthy litigation, and provides more certainty.

There are also certain liability questions raised by robotics that we have not encountered before. For example, one of the more intriguing possibilities of robotic surgery is that surgeons may be able to operate on a patient who is in a different room, a different hospital and even a different country to the surgeon. This would be especially beneficial where there are a small number of surgeons in a particular specialist area who could, in theory, operate on patients all around the world. In the event that a surgeon does perform an operation on a patient in a different country via such 'telemedicine', this raises the question of which liability laws apply if something goes wrong, and also raises issues of the adequacy of the surgeon's insurance cover.

3.5. *Privacy*

As mentioned above and in section 4 below, it is likely that robots used in healthcare will store large amounts of sensitive personal data. Details of a person's health and illnesses, medication and other health related data may have to be stored in order to enable the robot to carry out its function. In the case of care robots, there is also the potential for large amounts of personal data collected by these robots to be stored on the cloud, and for care robots to interact with other devices in the home, with data being passed between them.

3.6. *Ethical issues*

The use of robots in the home, either to replace (or supplement) care that would otherwise have been provided by humans naturally gives rise to ethical debate.

Care robots have the promise of giving people independence. Someone who may have been reliant on a human caregiver for daily tasks may be able to carry those out without human assistance. This may free up human carers to care for people whose needs cannot be met by a robot but, at the same time, may deprive people of the human contact they would have benefited from if they had a human carer. This is a serious consideration, with loneliness a recognised problem among older people. It has even been suggested that the increased use

[22] Adverse Events in Robotic Surgery: A Retrospective Study of 14 Years of FDA Data, H Alemzadeh, RK Iyer, Z Kalbarczyk, N Leveson, J Raman, J, Maxwell Chamberlain Memorial Paper for adult cardiac surgery at the annual meeting of The Society of Thoracic Surgeons (STS).

[23] Article 7(e) Defective Product Directive.

of robots as caregivers could weaken the moral obligation of society as a whole to care for the vulnerable[24].

Robotic prosthetics too raise interesting questions. Prostheses are currently used to replace lost function but where should the line be drawn between replacing 'normal' human functions and giving 'super human' ability? Should prosthetic legs, for example, give people the ability to run faster, and jump higher than they otherwise could have done? There is a grey area, because of the vast difference in abilities between different human beings, so it is difficult to define what a 'normal' human ability would be. However, there are clearly some abilities that go beyond what any human being could otherwise achieve. Would it be right to permit such enhancement?

Wider questions about how a robotic prosthesis is viewed by the law and by society can be asked: should a robotic prosthesis be seen as part of the body in some circumstances, or should it always be treated as a product? It would seem sensible that, should it malfunction, the wearer would have the full protection of product liability law. However, if a prosthetic leg was lost in an accident, for example, should this be treated as a natural limb for the purposes of compensation for non-pecuniary losses?

3.7. *Conclusion*

Healthcare is one of the areas in which robotic technology is already flourishing and there is great potential for the future. It is likely that issues of regulation and liability will be dealt with partly prospectively and partly by reaction to problems as they become apparent down the line. Much of our existing regulatory and legal framework is sufficient to deal with robotic technology in healthcare. However, as with technologies in other areas, the pace of development is fast and is likely to outpace our capacity to legislate for all aspects of it.

4. Data protection

4.1. *Introduction*

As we have seen in previous sections, the functionality and capabilities of current and emerging robotics technologies vary greatly. However, one key feature that all of these technologies tend to have in common is an ability to collect data, and in many cases, lots of it. The mass volumes of data collected by a driverless car or a drone, for example, present wide-ranging opportunities and benefits for those that process this data. If a driverless car were to be involved in a collision, the data collected could be used to provide the emergency services with the exact location of the car, speed of impact, maybe even the sex and ages of those on board, greatly improving the efficiency of their response and increasing the survival chances of those involved. Likewise, the extensive surveillance capabilities of a drone may allow the police force to prevent and detect crimes that previously went under the radar.

Of course the flipside of these perceived benefits is that the collection and processing by robots of extensive datasets have a potentially significant impact upon the privacy of individuals, whose personal data is among such datasets. Where robots process personal data, data protection legislation will apply to this processing, including the Data Protection Act 1998 (**DPA**). A balance must therefore be struck between deriving maximum benefit from these large datasets and ensuring a good level of compliance with the DPA. This section looks at some of the privacy issues associated with the data processing abilities of current and emerging robotics technologies and ways to achieve a better level of compliance.

4.2. *Application of the DPA and key terminology*

The DPA applies only to the processing of personal data. "Personal data" is essentially any information from which an individual person can be identified, whether from that data alone or in combination with other readily available data. "Processing" means any operation that can be carried out in relation to data, from collecting, obtaining or recording data, to using, storing, disclosing, transmitting or even deleting data.

Whether or not the DPA applies to an entity that processes personal data will depend on whether or not that entity can be considered a "data controller". A data controller is essentially an entity that decides why the personal data is processed (i.e. for what purpose) and how the personal data is processed (i.e. in what manner). However, note that the DPA is to be replaced by new legislation some time in 2018, which will have wider application beyond just data controllers (see sub-section on 'The Future and the GDPR' below).

In order to identify the data controller in relation to a robot, it is essential to establish who (or what) is deciding what data is collected, and how and why the data is being processed. However, this may not be an entirely straightforward task. Consider, for example, a care robot in an individual's home, which processes data in relation to an individual's medication requirements. Perhaps the robot is capable of monitoring simple vital signs such as blood pressure and temperature, in order to make decisions on when medication should be taken and in what dosage. In such a scenario, we will need to consider who is making such decisions and therefore taking on the role of data controller.

Potential candidates could include the patient's GP, if given access to the data collected by the robot in order to make decisions about the patient's care. If the robot links to online applications in order to process data and make decisions, potentially the app provider could be the controller. Perhaps there is more than one controller. Another entity worth considering is the robot itself. Is the robot sufficiently autonomous to make its own decisions about how the data is used to give care, thereby rendering the robot the data controller? And if this is the case, how can a robot be compelled to comply with legislation, or punished for not doing so?

These are just a few of the questions that spring to mind when considering how the current legislative regime under the DPA may apply to robotics technologies and the associated challenges that may arise. Of course as a 20 year old piece of legislation, it is hardly surprising that robots were not at the forefront of the legislators' contemplation when enacting the DPA.

[24] RoboLaw Guidelines, Chapter 5, Paragraph 3.6.

In order to delve deeper into the application of the DPA to robots, it is important to consider the principles which make up the foundations of the DPA and question how these may be interpreted in respect of technologies that may not have been envisaged at the time of enactment. The DPA is made up of 8 data protection principles, a number of which are addressed in the following subsections.

4.3. *First principle: process data "fairly and lawfully"*

In order for data processing to be "fair" under the DPA, an individual whose personal data is collected (a "data subject") must be informed of the identity of the data controller and the purpose(s) for which their personal data will be processed. Fair and lawful processing also requires one of a number of specified conditions to have been met, including that the data subject has consented to the processing, that the processing is necessary under a contract to which the data subject is party, or that the processing is necessary for compliance with a legal obligation to which the data controller is subject.

As identified above, identifying the data controller in respect of personal data collected by a robot may be a tricky task. Even if the data controller is readily identifiable, will the data subject always be informed of who the data controller is? Consider, for example, a civil drone surveying a large landscape. Will data subjects on the ground know who the data controller is or even be aware that their personal data (e.g. photographic images) is being collected? How can a data subject be aware of the purposes of this processing, if they aren't even aware of the processing itself or of who is carrying it out?

Similar issues may arise if we take the example of a home robot. While the user may, in choosing to interact with the robot, have implicitly consented to the collection of its personal data, it may not have fully understood the purposes for which this data is being processed, or in fact who is conducting the processing.

Some general recommendations on how to address these issues are set out in the 'Best Practice Recommendations' subsection below. Taking the example of a drone specifically, the WP29 (defined below) has come up with a number of suggestions on how to notify the public of their use[25], including who is the controller, what data they are collecting and for what purpose. For example signposts could be used for drones in fixed locations, along with information sheets for specific events. Additionally social media is a great way of getting a message out to the public, and of course there is the option of making the drone highly visible, enabling individuals to be better informed about when they may wish to exercise their data protection rights. Ideally a multi-tiered approach would be taken, using a number of different mediums to ensure that individuals are fully informed to ensure compliance with the first principle.

4.4. *Second principle: purpose limitation*

The second principle under the DPA requires that data controllers process personal data for a specified purpose or purposes only and that all processing of the data is compatible with that purpose(s).

Consider the example of a rented driverless car, which constantly collects data about the location of the vehicle (and the passengers within it) for the "purpose" of escorting the passengers from A to B. Having been informed that their location data would be used in this manner when hiring the car, the passengers may have consented to their data being used for this purpose. However, there is potential for the owner of the car to process this location data for additional purposes. For example, the owner could collate location data relating to its regular customers, in order to plot their regular journeys and discover further information about their lifestyle choices (for example, passenger X visits a drive-through restaurant three times a week, passenger Y always goes to the gym on the way to work).

This could enable the owner to create profiles of its regular users in order to provide them with targeted marketing next time they use the car – perhaps a voucher for a new drive-through restaurant which will require the passenger to incur further mileage, thus increasing the owner's revenue, or maybe even targeted radio marketing within the vehicle. Clearly this additional processing is not compatible with the original purpose of escorting the passengers from A to B. If the passengers have not been informed about (and, in the case of marketing activities, consented to) this additional purpose, there is a clear violation of the second principle.

4.5. *Third principle: data minimisation*

A data controller is required to process the minimum personal data necessary to fulfil its intended purpose. As mentioned in the introduction to this section, current and emerging robotics technologies often have the capability to collect mass volumes of data and wide-ranging datasets. Robots have the distinct ability to go places that humans cannot go and see things that humans cannot see, using a range of highly sophisticated sensors and processors, which significantly increases their capacity to collect and process data[26].

One way to help achieve data minimisation is the concept of "blurring". For example, a drone or similar technology which takes indiscriminate photos of identifiable individuals could use blurring functionality or similar graphic capabilities to de-identify these people where their identification is not necessary for the purpose for which the image is being collected.

The idea of "blurring" can similarly be applied to other types of personal data, for example location data. The data controller should consider how detailed it needs location data to be for the purpose in connection with which the data is being processed. For example, would the location of "North London" be sufficient, as opposed to an exact street name or number? Equally is it sufficient to know that an individual is within a

[25] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, Adopted on 16 June 2015.

[26] M. Ryan Calo, "Robots and Privacy," *in Robot Ethics: The Ethical and Social Implications of Robotics* (Patrick Lin, George Bekey and Keith Abney, eds.) (Cambridge: MIT Press, forthcoming).

particular building, without needing to know in what room and on what floor?

4.6. *Seventh principle: data security*

The seventh principle requires the data controller to take appropriate technical and organisational security measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

What may be appropriate in any given circumstance is likely to depend upon the type of data that is being processed and the likelihood of this data being compromised. For example, a care robot managing the affairs of an elderly individual may process highly sensitive information ranging from the individual's daily medical needs to their bank account details. Clearly this type of information is susceptible to hackers and requires robust protection. On the other hand, a drone used to monitor crops, which inadvertently takes the odd photo of recognisable individuals, may not need such stringent security measures.

Security also ties in with a further principle under the DPA, which requires that personal data is not retained for longer than needed for the purpose for which it is processed. Security measures should therefore include strict data storage and deletion schedule to ensure that any personal data that is no longer required is securely deleted.

Some of the current and developing robotics technologies present significant security concerns which will need to be carefully managed if these technologies are to operate in compliance with the DPA. Take the example of a surgical robot, which communicates with a surgeon-operated console over a network, which in some cases may be an insecure, wireless network[27]. Without appropriate security being implemented, there is a risk of extremely sensitive health data being compromised and interfered with, with potentially dire consequences for the patient.

4.7. *Sensitive personal data*

Sensitive personal data is a subset of personal data under the DPA and includes data relating to an individual's race, ethnic origins, political opinions, religious or similar beliefs, physical and mental health, sexual life and criminal records.

Sensitive personal data is afforded additional protection under the DPA and in particular, the individual's explicit consent is generally required for any processing.

It can be seen that robots used in a healthcare setting, such as surgical robots and care robots, are likely to collect a range of health data. A future healthcare robot could potentially monitor a patient at all hours, reporting back to other technologies and perhaps also to humans[28]. This could result in the collection of large volumes of wide-ranging sensitive personal data, which is potentially made available to a variety of third parties. Of course, with such sensitive data being processed at mass-volume, there are also greater security risks. Indeed there is evidence that healthcare data is a target for data theft and blackmail[29].

Consider the case where an individual is rushed into A&E and subsequently cared for by a healthcare robot for many months, having never interacted with or even been aware of the robot. It is difficult to see how explicit consent could be given to the processing of large volumes of sensitive personal data in such a scenario. Of course it is likely in practice that a form of doctor–patient confidentiality would exist for a health robot, although such confidential information may be a lot more difficult to safeguard, when outside of human hands.

Another viable scenario could be a driverless car, which keeps a record of locations visited. Imagine a scenario where a passenger uses the car to visit a religious place of worship on a regular basis? This information informs the data controller about the passenger's likely religious beliefs, thereby constituting sensitive personal data. But could the passenger really be said to have consented to this?

4.8. *Right to private life*

One of the key capabilities of robots that set them apart from earlier technologies is their ability to access the most private and "historically protected"[30] of spaces. Take the example of a robot in the home, which has the ability to interact with humans in their home environment and to collect images, recordings and other data relating to their private life within the four walls of their home. Perhaps in their most human-like form, so-called "social" robots may be uniquely placed to extract information from humans in the home, which would otherwise remain private[31].

Equally, the ability of technologies such as drones to enter private premises and collect vast amounts of data not previously accessible to the outside world can be seen as a clear intrusion into the private lives of individuals, and as a possible form of covert surveillance.

These unique capabilities mean that robots may be processing extremely sensitive data, which has not previously been readily available, and may be of great interest to certain third parties, such as hackers or even government authorities with appropriate legal rights to access the data. Clearly, the collection and processing of such intimate data do not sit very comfortably with the human right to respect for private life and to the protection of personal data under Article 8 of the European Convention of Human Rights.

There is, of course, an argument that the intrusive capabilities of certain technologies and any access that they may provide to certain third parties, for example the police, to the data they collect, may be justified as falling within exemptions under the DPA (for example, compliance with certain provisions of the DPA may be exempted where personal data

[27] "*Surgical robots – smart but insecure*", Taylor Armerding, CSO, June 2, 2015.

[28] Regulating Healthcare Robots in the Hospital and the Home: Considerations for Maximizing Opportunities and Minimizing Risks, Drew Simshaw, Nicolas Terry, Dr Kris Hauser and Dr ML Cummings.

[29] Eric Cowperthwaite, vice president, advanced security and strategy at Core Security, quoted in "*Surgical robots – smart but insecure*", Taylor Armerding, CSO, June 2, 2015.

[30] M. Ryan Calo, "Robots and Privacy," *in Robot Ethics: The Ethical and Social Implications of Robotics* (Patrick Lin, George Bekey and Keith Abney, eds.) (Cambridge: MIT Press, forthcoming).

[31] Ian Kerr, 204, "Bots, Babes and Californication of Commerce," *University of Ottawa Law and Technology Journal* 1:285.

is processed for journalistic purposes, for household use only, or for the purposes of preventing or detecting crime).

However, the WP29 (as defined below) has been very clear in its guidance[32] that any exemptions such as those listed above should be interpreted narrowly and that where reliance upon such an exemption may impact upon the fundamental right to private life, this should be limited to circumstances where such reliance is strictly necessary and where to do so will genuinely meet the objectives of the general interest of the EU or the need to protect the equivalent rights and freedoms of others. Data controllers utilising intrusive and covert technologies will therefore need to be mindful of this limitation when seeking to rely on an exemption under the DPA.

4.9. *Best practice recommendations*

The Article 29 Working Party (**WP29**) adopted an opinion in June 2015 on privacy issues relating to drones[33]. While the guidance is specifically aimed at the capabilities of drones, it provides a useful baseline for how to address privacy issues presented by robots more generally.

Much of the guidance centres on steps that should take place in the design and development stages of a new technology in order to ensure privacy compliance from the outset. This includes employing the principle of 'privacy by design', i.e. a robotic technology should be designed with privacy in mind, ensuring compliance with the DPA from day one with data protection "embedded within the entire life cycle of the technology"[34], rather than attempting to establish privacy compliance further down the line, when a technology is already founded upon capabilities that are inherently unfriendly from a privacy perspective. In this regard it should also go without saying that developing robotics technologies should incorporate 'security by design', particularly where a technology is intended to handle very sensitive data and/or large volumes of personal data.

Another key principle to follow is 'privacy by default', which essentially means that, by default, the capabilities of a new data processing technology should be limited such that personal data is only processed to the minimum extent necessary for each specific purpose of the processing and further, that such data is not retained beyond the maximum time period necessary for those purposes.

The WP29 also recommends that privacy impact assessments are carried out in the early stages of development in order to assess the impact of a new technology on the rights of individuals to privacy and data protection.

Another key recommendation in the WP29's guidance, which is clearly relevant to other types of developing robotics technologies, is that users should be provided with sufficient information within the packaging and operating instructions for the robot, explaining the potential intrusiveness of the robot and, in the case of drones as specifically addressed in the guidance, where their use is allowed.

It can be seen that this recommendation to provide information could be a useful means of addressing a number of the principles under the DPA. A clear privacy policy, whether provided in hard-copy in the robotics packaging, or in soft-copy as part of the technical set-up process, could address a number of key requirements, including notification of: (i) the identity of the data controller; (ii) the types of personal data that the robot collects; (iii) the purposes for which the data is processed and any third parties with whom it is shared; (iv) the security measures that the data controller has put in place etc.

Beyond pure notification, a robot should, as part of its set-up process and as part of its ongoing functionality, enable the user to access and change its privacy settings in order to put the user in control of what personal data is collected, how this is used and with whom it is shared. For example, a user might be happy for a robot to collect images, but not to record location data in relation to where this data was collected. Similarly, a user of a "social" robot may be happy for its data to be shared with other users of social robots, but may not be happy for its data to be shared with third parties.

Data minimisation should also be a key feature of any new robotics technology, including in terms of the preference settings made available to the user. For example, in order to function correctly and safely, a driverless car needs to collect current geo-location data. However, it does not need to keep historic location data of all journeys taken by a particular passenger (which could potentially be used for profiling purposes), in order to function correctly and safely. As a privacy-friendly default therefore, this type of "not strictly necessary" data collection should be switched off, with the user having the option to switch it on, if preferred.

Other recommendations touched upon in the WP29's guidance on drones[35] include: (i) involving a data protection officer in the creation and implementation of policies related to the use of the new technology; (ii) implementing codes of conduct for the responsible (and privacy compliant) use of robots within specific industries; (iii) ensuring that data processed by a robot is further reviewed by a human operator before it is used to make any decision which may adversely affect an individual; and (iv) implementing policies and guidelines to ensure that the DPA principles are always met.

4.10. *The future and the GDPR*

Looking to the future, the DPA is ultimately to be replaced by the General Data Protection Regulation (**GDPR**). The text of the GDPR has now been agreed by the EU Legislative Bodies and it is anticipated to come into force in the first half of 2018. The GDPR is intended to update data protection legislation in light of current and emerging technologies and, once implemented, is likely to give individuals greater control over their personal data than ever before. Of course, the law faces challenges in trying to keep up with the pace at which technology is

[32] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, Adopted on 16 June 2015.

[33] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, Adopted on 16 June 2015.

[34] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, Adopted on 16 June 2015.

[35] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, Adopted on 16 June 2015.

developing and it is likely that there is already a vast array of developing robotics technologies that have not been anticipated by the GDPR.

However, some of the WP29's guidance referred to above will be enshrined into law in the GDPR, including the principle of privacy by design and the requirement for privacy impact assessments to be conducted.

One of the biggest changes under the GDPR in contrast to the DPA is that it will place direct obligations on data processors, i.e. entities that process personal data on behalf of data controllers. With this in mind, providers of robotics technologies which only provide data processing capabilities on behalf of a data controller making use of the technology will have their own compliance obligations under this new legislation.

The requirement to identify a clear purpose for processing personal data and the threshold for obtaining 'consent' are to become more onerous under the GDPR, increasing the compliance burden on data controllers. Individuals will also have the right to withdraw their consent and request the erasure of their personal data in certain circumstances. This could prove tricky for data controllers using robotics technologies to process mass volumes of centralised data. Mechanisms will therefore need to be in place from the outset to address such requests.

Another key feature of the GDPR is that it imposes significantly increased fines for non-compliance which are based on worldwide revenue. Serious breaches of the GDPR such as processing data without a valid purpose will attract fines (applicable to both controllers and processors) of up to €20 million, or 4% of annual worldwide turnover, whichever is greater. Currently, the maximum fine available in the UK is £500,000 and the largest single fine issued to date is £325,000. It will therefore be more important than ever that data controllers (and now processors) operating robotics technologies with vast data processing capabilities ensure that this is done in a manner that is sufficiently compliant with applicable data protection legislation.

4.11. *Conclusion: are we robot ready?*

It is evident that robots present a number of privacy and data protection concerns and there is clearly some question over whether a 20+ year old piece of legislation is up to the challenge of meeting these concerns. However, existing WP29 guidance provides a useful starting point for considering data privacy issues with robots and looking at ways to address these.

As robots continue to become more main-stream, it is likely that further guidance will be issued to help with appropriate interpretation of the DPA and equivalent legislation around Europe.

The introduction of the GDPR in 2018 will serve to update current, dated legislation, so that it is more 'robot ready', enshrining some of the guidance and recommendations we have seen above into law. Of course, the process of adopting new European legislation is inherently slow and technology is likely to continue to move at a far greater pace for the foreseeable future, making it very difficult for the legislators to keep up.

In reality of course, the same problem has arisen with a number of new technologies over the last decade or so – at the time of enactment of the DPA, its application to cloud computing, social media or apps was not envisaged. Ultimately, therefore, there will always be a need to carefully interpret legislation and to rely upon relevant guidance and commentary, in seeking to achieve an appropriate level of data protection and privacy compliance in relation to new technologies. Robots and their extensive data processing capabilities are no exception to this rule.

That said, if robots achieve autonomy to the point that they themselves become the data controller and responsible for compliance with data privacy legislation, concerns over how that legislation can be applied and enforced may become significantly more complex to address.

5. Consumer protection

5.1. *Introduction*

Many of the robotic and related technologies discussed in this edition are already in the hands of consumers, and in other cases are at least designed with the future consumer use in mind. The public has, or will soon have access to a range of consumer robotics, from driverless cars to personal drones and care robots. These types of robots will, most likely, collect people's data, attempt to gain their trust, control their medical supplies, disclose their information, make purchases on their behalf, display advertising to them and generally socially interact with people.

Consequently, these robots have the potential to deceive and mislead people, threaten and cause them physical harm, and breach their privacy. This dynamic raises some traditional consumer protection issues and perhaps some additional consumer protection concerns that are specific to robot–human interaction.

This section will examine some of the key consumer protection issues, the ways in which existing regulatory regimes would deal with them, and whether further legal consideration is needed if robots are to have a permanent place in the human sphere.

5.2. *Overview of UK legal framework*

Firstly, it is useful to give a very brief overview of the key aspects of the UK legal framework that would cover (as we will see, to varying degrees) the consumer protection issues raised by robotics and the way we interact with them.

Consumer protection law in the UK is divided into the following categories:

- unfair trade and commercial practices (primarily covered by the Consumer Protection from Unfair Trading Regulations 2008[36] (the "**CPRs**") and in relation to advertising,

[36] The CPRs implemented into UK law the EU Unfair Commercial Practices Directive.

self-regulation under the Committee of Advertising Practice's ("**CAP**") codes of practice[37]);
- unfair terms in consumer contracts (primarily covered by the Consumer Rights Act 2015[38] (the "**CRA**")); and
- consumer rights and remedies for goods and services (also primarily covered by the CRA).

For each of the specific consumer protection issues discussed in this section, at least one of these categories of consumer protection law is likely to be directly relevant. In the discussion of the key consumer protection issues below, we will attempt to offer some analysis on whether the existing law in these areas is sufficient to protect consumers, whether they give rise to any broad principles or standards which can usefully be applied by manufacturers and retailers into the design and sale of consumer robots, and what further legal protections might be considered in the future.

5.3. *Trust and confidence*

It is often argued that robots are not so different to existing technologies and appliances we are used to dealing with in the course of our daily lives. In many ways this is true. A robot car is a tool for getting from one place to another just as a normal, driver-operated car. A way in which it is not true, however, is in how we view and interact with them.

Studies show humans tend to trust and confide in robots[39] (and it is not as if anyone would reveal dark secrets to their toaster or vacuum cleaner). This gives them a unique place in technology appliances as they are often both useful and social at the same time, marking consumer robots out from the power drill and the word processor.

The trust and confidence we tend to place in robots, and the good reputation many types of robot enjoy among the public, represent the reasons why robots can harm and deceive us in a way other technology appliances usually cannot.

There is evidence that people trust and confide in robots even where they do not believe the robot to be conscious or have emotions, particularly where it takes on an anthropomorphic form or closely resembles human emotions[40]. We can conceive of circumstances in which that trust could be abused or confidence breached via deception. This is not a new problem in relation to technology products, as shown by the example of the Spinvox speech recognition software, which users were led to believe converted their speech to text via sophisticated software but in fact was operated by human employees in a call centre in the Philippines who translated the speech manually and were therefore privy to people's audio messages[41].

In relation to robotics, consider the so-called 'Wizard-of-Oz' arrangement where a human interacting with a robot believes the robot is acting autonomously but in fact it is being remote-operated by another human[42]. In these examples, people could be deceived into disclosing sensitive or confidential information they would not knowingly wish to disclose to another human.

It is this trust factor which means that the issue of deception is perhaps more relevant to robots than other technology appliances where trust in the appliance itself (as opposed to, say, the brand or manufacturer of the appliance) is a less significant factor. Driven by their representation in science-fiction, as well as our own imaginations, we are all too ready to believe that robots can actually match or exceed our high expectations of them, and over time we will be less and less surprised and enthused by their promised functionality[43].

Taken together, these factors make it more likely that we will expect a robotic product to be safe, trustworthy and that our communications and interactions with them will be safe, secure and confidential. However, when the state of the art does not meet such expectations, consumers are prone to over-trusting (and over-sharing) putting their sensitive and confidential information at risk, and it is this dichotomy that presents clear consumer protection risks.

The main regulatory tools available to deal with the types of practices described above are likely to be the prohibitions on unfair and misleading commercial practices under the CPRs, a criminal offence the punishment for which is usually a fine. The general prohibition simply states that unfair commercial practices are prohibited[44] ("**General Prohibition**").

The wording of the General Prohibition is deliberately wide to catch any unfair practices that may be developed in the future. A practice is unfair if it fails to meet the standard of "professional diligence" (the standard of skill and care that would reasonably be expected of a trader in its field of activity) and it materially impairs an average consumer's ability to make an informed decision, causing him to make a decision he would not otherwise have made.

In most cases, the average consumer will be taken to be reasonably well-informed, reasonably observant and circumspect. However, where a trading practice is specifically targeted at a particular consumer group, the average consumer will be the average member of that group. Given the potentially broad applicability of robots to people's everyday lives it might not always be possible to identify a specific consumer group, but it is possible to argue that specific types of robot are targeted at certain markets or demographics (e.g. a care robot or a

[37] The key ones being the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing ("**CAP Code**") and the UK Code of Broadcast Advertising ("**BCAP Code**"), each enforced by the Advertising Standards Authority.

[38] The Consumer Rights Act 2015, the majority of which came into force on October 2015, simplified and consolidated key parts of the UK's consumer protection law.

[39] A Wagner, The Role of Trust and Relationships in Human-Robot Social Interaction, Georgia Institute of Technology, December 2009.

[40] J Michael and A Salice, (How) Can Robots Make Commitments? A Pragmatic Approach, pp. 128–129.

[41] http://www.theregister.co.uk/2009/07/29/spinvox_mechanical_turk/

[42] Jacqueline Kory Westlund & Cynthia Breazeal, Deception, Secrets, Children, and Robots: What's Acceptable?

[43] We see this currently in the realm of current consumer electronics, such as smartphones and tablets, where the rapid pace of improvement has led to increasingly high consumer expectation which each set of new iterations seems destined to fall short of, leading to a form of 'technology fatigue' when those expectations are not met.

[44] Regulation 3(3), CPRs.

brain–computer interface) which form an identifiable group of consumers the decisions of which the unfair practice is likely to distort.

Given what we have said about the gap between people's expectations and reality, it may be that the average member of that consumer group would make a purchasing decision based on the unfair practice being undertaken (the misleading performance video, the misstated functionality, or the 'Wizard-of-Oz' setup). In these cases, which might seem isolated but which might grow over time as robots are developed to suit specific consumer needs, it is likely that a local Trading Standards office or the Competition and Markets Authority[45], the enforcers of the CPRs, would take a keen interest.

The General Prohibition is a safety net and is intended to be future proof. Depending on the nature of any given unfair practice by a robotics company it might be that their action amounts to a more specific breach of the CPRs. In the robotics context (and in light of the examples given above) the most relevant specific prohibition appears to be that against giving false information or an overall impression that deceives (or is likely to deceive), even if the information is factually correct, about the nature or main characteristics of a product (**"Specific Prohibition"**)[46]. Again, where that deception affects (or is likely to affect) an average consumer's ability to make an informed decision, causing him to make a decision he would not otherwise have made, then it is likely to be a breach of the CPRs[47].

Whether or not the impression of a robot given by a robotics manufacturer would amount to a breach of the Specific Prohibition will of course depend on the facts. But we can speculate that regulators may consider certain practices, such as the 'Wizard-of-Oz' setup, to give a misleading impression of the characteristics of the robot in question – in this case, that the robot is fully autonomous and what you do or say to it is between you and it, and not a human operator controlling it.

The General Prohibition and the Specific Prohibition are supplemented, of course, by action that might be taken by other regulators who are not directly concerned with consumer protection. An example is the Information Commissioner's Office who might consider any personal data of the consumer to have been collected by a 'Wizard-of-Oz' robot to have been collected without the requisite consent of the consumer if the consumer was not made properly aware of the way in which its information would be used (and by whom).

While the existing protections offered by the CPRs, coupled with interrelated laws and regulations such as data protection legislation and information security standards, are likely to continue to protect consumers from deceptive information about and misleading impressions of robots given by robotics companies, it is important that trade practices in this nascent market will need to be carefully policed and the rules carefully enforced to ensure consumers continue to be protected in an age when the gap between expectation and reality continues to widen.

5.4. *Misleading advertising and marketing*

We have seen that the public expectation of how robots will perform can often outstrip the functionality of the state-of-the-art. Another factor that potentially broadens this gap is the way in which robots are marketed and advertised. It is not inconceivable that robotics companies or other malicious operators could seek to deceive people by exploiting the trust and positive brand image enjoyed by many consumer robots.

Already, there are a number of ways in which robotics manufacturers have attempted to deceive in this way. 'Performance videos' showing off robot functionality may speed up the motion of robots to make them appear faster than they are[48]. Robots might be advertised to simulate features that are planned but which might not yet exist. These practices try to play on our tendency to over-estimate the functionality and effectiveness of robots and presents clear opportunities for malicious companies to attempt to scam consumers.

The practice of deceptive or misleading advertising is not new. The Advertising Standards Authority (the **"ASA"**) enforces the CAP Code and the BCAP Code which set down rules for advertisers, agencies and media owners to follow. Non-broadcast advertising is governed by the CAP Code and broadcast advertising is governed by the BCAP Code. The codes contain generally similar rules to be observed. The rules require advertising to be responsible, not misleading or offensive, and set down specific rules that cover advertising to children and advertising for specific sectors like alcohol, gambling, motoring, health and financial products. It is to be expected that robotics companies would likely rely on highlighting the capabilities and functionality of their robots as a key part of their marketing armour – so of particular relevance here are the rules that marketing communications must not materially mislead or be likely to do so[49] and claims that consumers would regard as objective must be capable of objective substantiation[50].

The enforcement powers of the ASA are relatively limited, extending to the power to force an entity to withdraw or amend an advertisement which does not comply, and to publish the ruling on the ASA's website ('name and shame'). The ASA considers the compliance of an advertisement on a complaints basis, responding to complaints made by consumers or business competitors alike. In extreme cases, the ASA may refer an enforcement matter to the CMA/Trading Standards, who may take action under the CPRs (for example, for breach of the General Prohibition or the Specific Prohibition under the CPRs outlined above).

The ASA's powers may seem limited, but the impact of 'naming and shaming' an advertiser's deception has a reputational impact that a fine or other penalty may not and the ASA has ruled against advertisers where the goods or services were advertised in a misleading way.

There is a clear trend involving technology products/services which misstated or oversold technological capability.

[45] The previous enforcement body was the Office of Fair Trading which was closed in 2014 with its powers passed to various bodies including Citizens Advice, the Financial Conduct Authority and, in relation to consumer protection, the Competition and Markets Authority.

[46] Regulation 5(2), CPRs.

[47] Regulation 5(4), CPRs.

[48] W Hartzog, *Unfair and Deceptive Robots*, 74 Md. L. Rev. 785 (2015).

[49] Rule 3.1, CAP Code.

[50] Rule 3.7, CAP Code.

A recent BT advertisement relating to the speed and upload times of its BT Infinity broadband service was ruled to be misleading, exaggerating as it did the speed of photo transfer and upload, and the process of buying a ticket online, as depicted in the advertisement.

Dyson complained about Vax's claims in its advertisement for its Vax cordless vacuum cleaner that it had the same functionality as a corded vacuum cleaner; the ASA upheld the complaint on the basis that the advert misled consumers and exaggerated the functionality of the product.

Rulings such as these can often get traction in the media, doubling the reputational impact of misleading or exaggerated advertising. The nature of robots – being in most cases advanced pieces of technology with new or unusual functions – means that there may be a strong temptation for advertisers to overstate, exaggerate or mislead people about what they can do. The ASA's regulatory powers, as demonstrated in recent examples of misleading technology advertising, suggest the ASA is well placed to provide effective oversight of such advertising practices going forward.

5.5. *Influence, persuasion and manipulation*

The potential for robots to influence, persuade and manipulate people also presents a consumer protection issue. It is well known that humans are highly persuadable and vulnerable to manipulation of differing degrees[51]. This phenomenon has attracted the attention of advertisers and marketers for a long time and has more recently been grasped by governments (including the UK government which part-setup the 'Nudge Unit', so-called because its purpose is to apply psychological insights to influence people's behaviour[52]).

Robots could "nudge" people into buying or using them, or into disclosing sensitive information to them, using the personal information that people give to them or exploiting the trust and confidence people place in them. This is not to say that "nudging" itself is never legally or ethically acceptable, or that it is not commonplace in today's consumer market. However, there is a blurred line between "nudging", in the sense of steering someone in a certain direction while preserving their decision-making power, and wrongful manipulation, involving high-pressure techniques and misleading tactics.

While manipulative trade practices by one salesperson or within one company can be dealt with (internally or externally) on a case-by-case basis, the ability of such practices to be designed into robots which can reach out to a much broader section of the public has a higher potential impact and may be harder to identify and eradicate. Robots that are seen as cute or cuddly, or that come to be seen as part of the family (think of a driverless car with a name and a voice, or an anthropomorphic care robot in a nurse's uniform), that elicit emotional responses from its user could clearly cajole or manipulate that user into doing things it otherwise would not do. This could include persuading a user to buy an expensive upgrade pack or an additional maintenance service, or a care robot influencing an elderly person to buy a particular brand of medication.

Aggressive or manipulative sales practices are of course nothing new. These types of practices typically range from harassing, threatening or demanding behaviour in the most extreme cases, to high-pressure (or "hard-sell") approaches designed to force a consumer's hand ("if you don't buy it now, the offer is off the table"). There is a thin dividing line between assertive and aggressive practices which sales-focused businesses are used to treading lightly. The CPRs prohibit aggressive commercial practices that, by means of harassment, coercion or undue influence, significantly impairs (or is significantly likely to impair) the average consumer's freedom of choice or conduct and so causes (or is likely to cause) the average consumer to take a transactional decision that they would not otherwise have made[53].

Whether or not a pushy robot exerting undue influence over a user or buyer to make a purchasing decision would breach this prohibition will be a question of fact in each case. A consideration which must be factored in to any decision as to whether such a tactic is unlawfully aggressive is the nature of the relationship between the relevant robot and consumer. This reflects the difference between aggressive tactics deployed by human shop assistants or traditional advertising on the one hand, and those deployed by robots (usually at the behest of their manufacturers or retailers) on the other.

People are used to being given the "hard sell" by sales assistants. However, they will have less experience of spotting a hard sell by a robot they may rely on and trust in. It is clear that an attempted sale by a care robot to its human owner/patient is different to that by a telesales operator. The patient's familiarity with and possible reliance on its robot creates a closer more trusting relationship then the typical seller–buyer relationship, and the exploitation of that close relationship is a factor which makes such a sale more likely to be viewed as an aggressive practice depending on how it takes place. Accordingly, while it is likely that the existing prohibition would be sufficient to protect the typical consumer, in determining whether a robot's sales technique is aggressive and whether a robot influenced a consumer's decision, it will be important to take into account the trust and confidence people may place in their robots, as it is more likely someone will listen to and be influenced (or manipulated) by their personal robot.

5.6. *Robot–consumer contracts*

Various types of consumer robotics will (and indeed currently do) require users to agree and sign up to legal contracts. In the vast majority of cases these will not be negotiated and will be presented to users on their first use of the robot in the form of standard user or licence terms which they will be required to accept (e.g. via a tick box or 'accept' button) before they are able to actually use the robot. Fundamentally, this is no different to the click-through (or click-wrap) terms you are required to accept before being able to use a software product, the website terms of service that govern your surfing of a website, or hardware terms of use, each of which will apply

[51] See, for example: Can you be persuaded? Individual differences in susceptibility to persuasion, M Kaptein, P Markopoulos, B de Ruyter, E Aarts, Human-Computer Interaction – INTERACT 2009.

[52] https://www.gov.uk/government/organisations/behavioural-insights-team

[53] Regulation 7, CPRs.

to an array of technologies that are currently widely used by consumers. However, a factor that distinguishes robot contract terms is the potential difference between the ways in which people may wish to use robots, and the use the relevant legal terms might envisage or permit. This issue may arise more commonly with robots then with typical software, hardware and other devices and technologies, because of (as highlighted above) people's higher expectations of the functionality and effectiveness of robots compared to more traditional appliances.

The difference between people's potential planned use of their robots and the intention of their creators can play out in the robot user agreement. In September 2015 it came to light that SoftBank, the company behind Japan's most famous humanoid robot, 'Pepper', stated in its user agreement that "The policy owner must not perform any sexual act" on the robot or engage in "other indecent behaviour"[54]. This might seem like a somewhat bizarre warning (and one unlikely to be seen in the typical office printer lease), but it serves to highlight the type of interactions people may wish to have with consumer robots that blur ethical, moral and (in the case of this user agreement, at least) legal boundaries.

In terms of consumer protection, these real-life examples of actual public use (or misuse) of robots points to broader issues that robotics companies will need to consider when establishing their standard terms of use. For example, it is common for technology manufacturers to try to limit their liability to users to the greatest extent possible. However, existing unfair contract terms legislation sets down clear examples of liabilities that cannot be excluded or limited. As well as the usual liabilities that cannot be excluded by contract (i.e. fraud, death and personal injury), the CRA provides a range of circumstances in which a trader cannot limit or exclude its liability to its customers.

Where liability cannot be excluded, to what extent will robotics companies be liable for the uses to which users put their robots?

If the killers of Hitchbot (the hitch-hiking robot who was pronounced "dead" after it was attacked by vandals while crossing America) used him to cause harm to others, it would be an evidential issue as to how much of that liability could be ascribed to his manufacturer, particularly if the way in which they deployed him meant the harm was more likely to occur. Perhaps more pertinently for commercial robotics firms, the inability to exclude liability for key characteristics of their goods, for example as to satisfactory quality and fitness for purpose, may present challenges where there is a significant gap between user expectation, marketing and advertising representation, and actual robotic performance. Where a consumer believes a robot should perform a particular function or behave in a certain way, and if this belief has been encouraged by the robotics firm, then any mismatch between that and real-life functionality could potentially be actionable by the consumer, with the firm taking on potentially significant liability from a potentially broad consumer base.

So far in this section we have assumed robots are goods provided by traders and have analysed the law on unfair consumer contract terms on this basis. This need not be so. It is conceivable that a robot provided by a robotics company to a consumer would not be provided as a one-off transaction, but as an ongoing service. The robot might be leased/or licensed to the consumer under a set of lease or licence terms, with a service 'wrapper' provided regarding ongoing repair and maintenance, patching, and upgrades to improved functionality, perhaps for an ongoing monthly fee.

In this scenario the robot is not sold by the trader nor owned by the consumer. Instead the benefits provided by the robot to the consumer are provided as a service. This has implications for how the law on unfair consumer contract terms applies since the law differs depending on whether it is a good or service that is provided. For example, a service provider cannot limit or exclude its liability to a consumer for its obligation to provide the service with reasonable skill and care. It is clear that operators will need to consider how they structure their offering (e.g. a product or a service?) to ensure they design user terms that are compliant with consumer contract law and so they understand the risks they are taking on when they design, market and sell exciting new robotic technologies to an awaiting public.

5.7. *Conclusion*

In many ways, robots are not so different to the traditional consumer technology appliances we have been familiar with for a long time. However, in certain key respects they are very different: the social as well as the functional use of robots; how we view and interact with them; the familiarity, trust and confidence we might place in them; and our high expectations of how they will work fed by media, film and our own imagination.

These factors mean that robotics warrants special consideration when considering how best to protect consumers from aggressive and malicious operators. At the same time, we need to ensure that any fears and risks applicable to the design, advertising and sale of consumer robots are seen in context, and balanced with the need to ensure innovators feel on safe ground in developing and marketing the new and exciting robotic applications that the world is waiting for.

The implication of all this for regulators is to analyse and test whether existing consumer protection laws remain fit for purpose in the robot age, whether they have the tools they need at their disposal to strike this balance between protection and innovation through effective regulation, policing and enforcement, and, if not, whether special consideration (whether in the shape of new laws or new enforcement policies) should be applied in certain instances.

6. Robotics and commercial contracting

6.1. *Introduction*

The use of robotics in existing IT delivery models is fast becoming a whole new sector within the IT services industry. Known as Robotic Process Automation or RPA, this new

[54] http://www.theguardian.com/world/2015/sep/28/no-sex-with-robots-says-japanese-android-firm-softbank

technology is being seen as the next wave of innovation and improvement across many existing IT service areas.

This has come to recent prominence in relation to application development, off shoring, outsourcing and systems integration whereby robotic processes (or digital workers) are being used to replace human involvement and full time equivalents or FTEs (the unit of measurement commonly used to calculate cost for the use of individuals in providing services).

The effect of this is that robotic processes are being seen as a new way within which cost can be driven out of some of these IT service delivery models. It makes sense that, given the removal of FTEs, costs should decrease and delivery change to be 'product' based rather than service based.

Indeed, in a study in 2013, McKinsey & Company estimated that if the use of robotic processes grows at the rate expected, then by 2025, as many as 110–140 million FTEs will be replaced by automated tools and software.[55]

This has obvious advantages for suppliers and customers alike – but the impact for the off-shoring industry, where its growth has been underpinned by the wage arbitrage effect, could be vast. No longer cheaper, it will have to adapt.

This section will look at the impact that robotic processes will have on contracting models for the future.

6.2. *What types of services will be affected and how?*

Services which are most likely to reap the benefits that RPA promises to deliver are those that are based upon repetitive, rules based processes which are high frequency in nature.

There are many examples of these across a wide variety of industry sectors but most commentators believe that the banking and insurance industries, healthcare and logistics will be the areas where uptake is likely to be at its greatest.

Specific examples within the banking sector would include:

- Account analysis;
- Payment processing;
- Credit checking;
- New product marketing campaigns; and
- Client detail updates.

For insurance, examples would include:

- Payment protections claims;
- Automation of administration;
- Reinsurance processes; and
- Data collection, cleansing and analysis.

For healthcare, one could look at:

- Patient database changes;
- Appointment changes;
- Drug administration; and
- Facilities management administration.

[55] McKinsey Global Institute. "Disruptive technologies: Advances that will transform life, business and the global economy." May 2013. Print July 2014.

Every customer that adopts RPA as a new technology would look to obtain certain benefits from doing so. Cost savings would certainly be one – if not the most important – of the considerations but there are others.

As RPA integrates with existing legacy systems, one of its advantages is its ability to obtain data and feed it into related applications. This ability also allows it to provide better data collection, cleansing and analysis which, in turn, allow an enterprise to make better decisions based upon this data.

Technology in this area is advancing rapidly and the use of cognitive computers and augmented systems (more commonly, and incorrectly in the author's view, termed Artificial Intelligence or "AI") allows for unstructured data to be collected and analysed far faster than humans are capable of. This is adding to the list of advantages that RPA is presenting organisations because they now have access to data within a time frame and in a form that is far more useful than previously imagined.

Further, RPA promises to provide systems which are more efficient and which reduce the level of mistakes that their human counterparts make. It is not all bad news for the FTE, however, as increased productivity; higher levels of customer satisfaction and removing repetitive tasks from the human workforce should increase levels of worker satisfaction as well as release them to perform higher value tasks.

6.3. *What will be the impact on commercial contracts in the IT services industry and beyond?*

6.3.1. *Pricing*

As RPA is providing a different solution to end user customers and is delivered differently by suppliers, existing contract models may have to be adapted to provide for this change.

If we take the example of an insurance applications and premium administration service, which is currently outsourced by a customer to an off shore based company, this service will traditionally be provided by the supplier subject to the terms of a service agreement and priced, mainly, with reference to FTEs.

The software and support that sit behind the process are usually invisible to the customer but the scope of the services, the level of services and the cost of the same are transparent and are managed via the terms of the agreement between the parties. Therefore, any required interaction between applications will form part of the services scope and will be performed by FTEs and priced accordingly.

An RPA solution which replaces the provision of certain services may not necessarily be required to be spelt out via a contract change as the end result because the service that is to be provided may remain exactly the same.

However, if there are specific reasons why a customer would need to understand *how* the service is provided, for example because of regulatory compliance reasons or because the customer has a risk/reward agreement with the supplier for any cost savings, then the nature of the RPA may need to be fully described and added as a variation to the existing agreement.

6.3.2. *Intellectual property*

There may be intellectual property ("**IP**") considerations to be taken into account when looking at the nature of the delivery

model. Suppliers tend to contract on the basis that they will own their own IP that is used to provide the services and any other IP is either licensed from a third party or provided by the customer. The ownership of any IP developed during the course of the agreement is usually the subject of debate between the parties but more often than not, if it is bespoke development for the customer, then the customer will own the IP in such development.

Such IP is usually generated by the FTEs and assigned to the customer via the agreement – but what happens with any IP or database created by the robotic process software/hardware itself?

Most likely, such generated work will take the form of a software program and would therefore be copyrightable under English law and made subject to the terms of the Copyright, Designs and Patents Act 1988 (the "**CDPA**").

The CDPA already makes provision for works created by machines and defines 'computer generated' works as works generated by a computer in circumstances such that there is no human author of the work.[56] It is not sufficient for a work to be carried out via a computer – that would not satisfy this definition – but rather the computer itself must create the work according to a programme without a human having been involved in the creation.

Regarding ownership of copyright, the normal rule is that the author who creates the work is the owner.[57]

Where a work is seen as being computer generated, the author is the person *by whom* the arrangements necessary for the creation of the work are undertaken.[58]

In *Nova Productions v Mazooma Games*[59], the question was who owned the individual frames that were shown on the screen when playing a computer game. Was it the player or someone else? The Court held that the player of the game was not the author of the copyrightable work because they had not contributed any artistic skill or labour. Rather, the author was the person who had devised the rules and the logic used to create the frames.

It should be noted, however, that between computer assisted creations (where the author uses a computer to assist the creation of the work, for example using a word processor application to write a book) and computer generated works (discussed above) there is a third category termed 'intermediate works' that may be applicable where a person becomes the author as a result of that persons skill and effort using a computer.

For RPA generated works, it would seem that the Section 9(3) CDPA position, as more fully explained in the Nova Productions case, would appear to be the most likely position from which to start when determining who the author is – namely the author of the RPA algorithm software itself. However, as robotic software and hardware becomes more 'cognitive' and learns and adapts from data inputs, the works created may have no relationship to the original author's software and so other factors may well come into play.

[56] Section 178 CDPA.
[57] Section 9(1) CDPA.
[58] Section 9(3) CDPA.
[59] Nova Productions Ltd v Mazooma Games Ltd [2006] EWHC 24 (Ch).

6.3.3. *Contract formation*

Robotic processes that feed into information loops – for example whereby the RPA will gather data from one application and apply its 'learning' to update inventory procurement from suppliers to an enterprise – create additional contractual issues to be dealt with.

Can a software program bind one company into an effective contractual relationship with another for the purchase of goods and/or services?

It is universally accepted that a robotic system does not have a legal personality and therefore is a 'mere tool' the legal responsibility for which lies with its human/corporate controller.[60] Further, in relation to products, it is the producer of the product who bears liability for it pursuant to the terms of the Product Liability Directive 85/374/EEC of July 1985.

However, this is a debate that may well change as RPA and the Internet of Things develop and cognitive computing becomes the norm. With machines talking to machines and learning from each other and the experiences shared across networks, the likelihood is that the contracting framework will need to be developed to take into account commercial dealings that take place without human involvement.

Inasmuch as the current law states that the 'owner' of computer programs (and in all likelihood the licensee who uses such programs in an automated procurement system) will be bound by the agreements that such systems enter into, it is when the machines themselves start to decide who to contract with rather than with pre-programmed suppliers, that such issues of robotic legal personalities will become more important.

6.3.4. *Representations and warranties*

When dealing with representations and warranties from customers and suppliers alike, do they take into account the activities of an RPA? Do suppliers really want to warrant that an RPA will use skill and care when performing the services – or is this merely a functionality issue that can be dealt with by warranting that software and RPA software in particular, will meet its level of functional specification and that is it?

Similarly, is a supplier happy to enter into agreements on the basis that the output of the RPA will meet a customer's specific business purpose? If the process is sold as 'being automatic, without the need for human intervention and thus it will increase productivity by 25%' – is this something that customers will expect to see reflected in their bottom line, or will suppliers point to the functionality point again and say that the software 'just does this' and no further warranties will be made?

The approach to be taken by suppliers is particularly interesting because while they may be trumpeting the advantages of new systems and processes, what will they actually take responsibility to provide? Making fraudulent representations under English law relieves the supplier of the benefit of certain

[60] 'Regulating Emerging Robotic Technologies in Europe: Robotics facing law and ethics', Robolaw http://www.robolaw.eu/Robolaw

contractual exclusions that suppliers like to maintain and so salespeople will have to be careful when making exaggerated claims about benefits knowing that such benefits are not going to, or are very unlikely to, happen.

6.4. *Summary and conclusion*

The above represents an overview of the major contractual issues that RPA is creating at the present time and it does not purport to be a non-exhaustive list.

Certainly, RPA will have a large impact upon those areas of IT services performed by humans who are engaged in low value, repetitive, high frequency tasks and businesses that have grown up based upon such activities being performed by low paid workers may well see these being replacement by softbots or digital workers.

It is certainly not outside the realms of possibility to expect customers of this technology to be asking for contracts to be priced according to their own increases in profitability or revenue as a result of being sold 'intelligent and cognitive' systems that learn on the job and replace FTEs.

Price is but one element of the equation, however, and so increased efficiency, fewer (if any) mistakes, 24/7 availability, speed, data analysis and being part of an end-to-end IT system will undoubtedly also appeal to customers.

The above represents some of the intriguing questions which will have to be answered as the technology becomes more widespread and used within IT services and contracting models have to take these issues into account.