Analysis and insight for the industry - lawyers, regulators, manufacturers and users

THE ROBOTICS LAW JOURNAL

Volume 1, No. 6 May/June 2016

RAVN SYSTEMS
Law firms are starting to look closer at the organisation and editing of data in their search for more efficient ways of providing legal services
Page 4

LIFELONG LEARNING
Technology is taking hold of the workplace and the education system needs to adapt
Page 7

CYBER TERRORISM
Professor Connelly discusses the ethics of cyber counter-terrorism and the implications for legal systems
Page 10

COMPLIANCE
Financial services organisations are struggling to keep pace with regulatory demands and looking to AI for help
Page 15

Euro 2016 No Fly Zones

The ten host stadiums have been declared no-fly zones at this year's European football championship, starting in France on 10th June. This security move comes following the attacks in Paris last November, which included three explosions outside the city's Stade de France while France played Germany in a football friendly. Head of security for Euro 2016, Ziad Khoury, has noticed how proliferate drone use has become and has decided a blanket ban of the technology is in order to ensure safety, saying that the technology is a 'dissuasive measure that didn't exist at previous sports events'.

What are the potential threats?
Drones can be bought and used by anyone, so the likelihood is that a drone appearing near a stadium is likely to be holding only a camera so that an interested spectator can film the match from above. There has already been an arrest in the UK last year for nine breaches of the Air Navigation Order by a man taking video over football grounds, up and down the country. Clearly, with Premier League matches there are commercial as well as safety and security issues.

> There is already quite a range of deterrence options to choose from and the French gendarmerie has already begun employing GPS jammers to steer away drones from the stadiums

French security forces for Euro 2016 are also preparing for the possibility of a drone being used to disperse chemical agents over the crowd of a stadium. No specific threat has been identified, nor have drones been marked out as a particular threat by any intelligence. This is a case of vigilance using the technology as a deterrent, as well as ensuring all possible avenues of attack are covered. Given the current proliferation of drones in general society, it is not inconceivable to think that a threat could hide in plain sight.

How will they deter drones?
There has still been no official announcement on the exact nature of the anti-drone technology that will be employed, but Mr Khoury has said that it is intended to interfere with as well as even take control of drones. There is already quite a range of deterrence options to choose from and the French gendarmerie has already begun employing GPS jammers to steer away drones from the stadiums. The downside to this method is that GPS signals for civil use might be affected, aircraft use being of particular importance.

> There has already been an arrest in the UK last year for nine breaches of the Air Navigation Order by a man taking video over football grounds

Destruction of drones runs the risk of collateral damage, so deterring them from flying near the stadium is more preferable, as well as tracking the signal to identify the pilot. Expanded security perimeters around the stadiums will be put in place to help ensure that drone pilots are kept at a considerable distance to limit their influence.

The announcement of the zero-tolerance policy to drones is itself a useful deterrent, likely to put off most private drone owners due to fear of damage to their possession.

Contents


Alessandro Maiano

Incubating AI

Artificial Intelligence ("AI") is a very fast growing part of the technology sector. To get an idea of the processes involved in helping these types of start-ups to grow, Robotics Law Journal talked to Alessandro Maiano, the Managing Partner of Wilbe, a London based advisory and investment firm for founders of early-stage innovative ventures.

Wilbe supports ventures that are looking to change the way that society functions through the application of exponential technologies including blockchain, virtual reality and artificial intelligence.

History

Wilbe started in 2011 as a shared work space founded by Alessandro Philip Maiano (current Managing Partner) and Benjamin Radomski (Strategy Partner). Coming from, respectively, a corporate law and marketing background through Wilbe they soon started offering tenants integrated services and advice around corporate structuring, funding, international expansion and recruitment. A team of senior professionals from across some diverse sectors was gradually formed, constituting Wilbe's current Board of Advisors, adding industry expertise to the range of services offered.

Keen to be able to support promising ventures that had not yet accessed funding resources, a 6-month acceleration programme on a 'sweat-for-equity' basis was developed and by the end of 2012 tenants started referring to Wilbe as an 'incubator' for start-ups.

Members of the Board of Advisors started taking a vested interest in the ventures that were incubated by investing their own funds. Over the last couple of years, Wilbe has invited other potential investors from within its network that would share the mission to consider investment opportunities and eventually formed a private group of angel investors.

Sectors

According to Maiano, there is no shortage of ventures looking for help. "A lot of ventures come to us originally through word-of-mouth", he said. "They pay a fixed fee for services like rent and broadband and if we are interested in taking our involvement further, we invest for an equity interest. We have just exited from one such arrangement in the last couple of weeks."

As a former solicitor, Maiano knows that there is a great opportunity for AI in helping run law firms. Some of the new legal entities are much more involved in breaking new ground in this way. "Riverview, for example, is a machine-led law firm", he said. Wilbe is currently looking at a venture in the compliance space at the moment involving the development of a rules engine.

Timeline

Global timeline: what to expect on drone regulation

Mid-June — US

FAA regs expected - drone flying to be permitted

By early 2016 — Bahamas

Drone regs expected to take effect - being brought forward by Bahamas Civil Aviation

2016

Amazon Prime Air delivery service in '30 minutes or less using small unmanned aerial vehicles' due to start - so putting focus on practical application of drone regs on deliveries.

2016 — Australia

Lighter regs for commercial drones under 2kg - from Civil Aviation Safety Authority

2016 — Europe

RPAS framework - to implement March 2015 Riga accord

2018 — Global

ICAO standards - international standards for use to develop national guidelines

2016-20 — US

FAA - airborne sense & avoid systems - initial certification

Global timeline: What has happened so far on drone regulation

2016

May, 2016 — US

FAA clarifies educational carve-out for drone usage.

2015

December, 2015 — Global

Geo-fencing starts on products from market-leading manufacturer DJI - easing the way for enforcement of restrictions on flying near airports, prisons and other areas.

December 21, 2015 — Ireland

Irish Aviation Authority requires that 'all drones over 1kg must be registered' with them by this date

December, 2015 — US

Department of Transportation hopes to launch its drone register for UAV-users, to meet rising public concern about near misses

November — US

Chicago City Council passed drone regs which are a 'draconian ordinance all but banning drones in most cases', according to Professor Greg McNeal of Pepperdine University Law School

November — US

2,500th exemption licence (s333) given for drone flying

November — US

Registration by pilot (rather than individual drone) recommended by task force advising the Federal Aviation Administration

October — Ireland

Irish Aviation Authority published first draft of proposed Small Unmanned Aircraft (Drones) and Rocket Order

October — EU

MEPs voted to revise and develop rules for the safe use of drones

October — Finland

Finnish Transport Agency introduced what it is says is 'one of the most liberal aviation regulations in the world' for UAVs

September — Taiwan

Cabinet began process to regulate use of civilian UAVs

September — Japan

Amendments to Civil Aeronautics Act regarding drones: Regs include bans on UAV use over residential areas

September — Indonesia

Regulation 90/2015 from the Transportation Ministry took official effect: Indonesian Press Council says that the rules could restrict use of drones in journalism

September — EU

End of European Aviation Safety Agency consultation on drones - Key part of moves towards EU regulatory framework

August — US

National Telecommunication and Information Administration started work on drone privacy voluntary standards

August — New Zealand

Updated drone rules - risk-based

July — South Africa

CAA regs take effect: drone flying became legal

June — EU

Privacy rule recommendations from Article 29 Working Party

FAA Clarifies Educational Use of Unmanned Aircraft Systems

Anne Swanson

The FAA has carved out a useful exemption from drone regulation using the hobbyist definition

Anne Swanson, a partner in Cooley's Regulatory Communications practice and based in the Washington office, welcomes the new guidance issued by The Federal Aviation Administration ("FAA") on the use of unmanned aircraft systems ("UAS") at accredited educational institutions by students and faculty during instruction. In a clarification to guidance originally issued in June 2014, the FAA indicates that there are some situations when student and faculty use of UAS may qualify as "hobbyist" or model aircraft operations that do not require prior FAA authorization.

According to Swanson, "This guidance on the hobbyist exemption extending to educational establishments is a very welcome addition to a more liberal regulatory regime and will free up essential training as part of broader classes on UAVs."

Students

In this latest memo, the FAA reviewed the principles of Section 336 of the agency's 2012 reauthorization legislation (the FMRA), which provides special regulatory treatment for UAS operated as "hobbyist" aircraft. To qualify as a "hobbyist," a UAV operator must meet several criteria, noted below, but most importantly, must have a non-commercial purpose, and the operation may not be indirectly incidental to any business or compensated activity.

In its latest clarification, the FAA said that students at accredited educational institutions may operate unmanned aircraft in accordance with the hobbyist exception as a component of their coursework, as long as UAS operation and flight training are not the sole purposes of the course, that is, the course is not solely related to UAS flight training, and as long as the students do not receive compensation directly or indirectly from the activity. The FAA notes that students operating UAS as one component of a curriculum pertaining to broader principles of flight, aerodynamics, and airplane design and construction actually promotes UAS safe use and advances UAS-related knowledge, understanding, and skills.

> "This guidance on the hobbyist exemption extending to educational establishments is a very welcome addition to a more liberal regulatory regime and will free up essential training as part of broader classes on UAVs."

Faculty

As a part of this coursework, the FAA also indicated that faculty may provide limited assistance to students operating unmanned aircraft under the same hobbyist exception, but only if UAS operation is a secondary component of the curriculum. A student must maintain operational control of the unmanned aircraft, although the faculty member is allowed to help regain control or to terminate the flight.

The FAA also said that a faculty member conducting research may not rely on Section 336's concept of "hobby or recreational use" to operate a UAS or direct student UAS operations in connection with research. Likewise, a student operating UAS for research on behalf of a faculty member is associated with that faculty member's professional duties and compensation, and, thus, the activity is not hobby or recreational use by the student pursuant to Section 336. Student operation of the UAS for the professional research objectives of faculty renders the operation non-hobby or non-recreational.

Section 336 definition of "hobbyist"

As a reminder, to qualify as "hobbyist" use, a UAS must meet the following criteria, which also must be met to qualify for the benefits of this new guidance:

1 Flown strictly for hobby or recreational use;
2 Operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;
3 Limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;
4 Operated in a manner that does not interfere with and gives way to any manned aircraft; and
5 When flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic control facility is located at the airport) with prior notice of the operations (model aircraft operators flying from a permanent location within 5 miles of an airport should establish a mutually-agreed upon operating procedure with the airport operator and the airport air traffic control tower).

FAA authorization required for non-hobby or non-recreational use

When UAS operations do not qualify for the hobbyist exception, the operator must seek approval through one of the following avenues:
1 As public aircraft operations pursuant to the requirements of the public aircraft statute and under a Certificate of Waiver or Authorization (COA) from the FAA;
2 As limited commercial operations by type certificated UAS, provided the operator obtains a COA from the FAA; or
3 Pursuant to a Section 333 of the FMRA grant of exemption based on the Secretary of Transportation's determination that a certificate of airworthiness is not required, and provided the operator obtains a COA from the FAA.

The Big Picture

The industry is waiting with baited breath for the FAA to produce the full regulatory landscape. "The codified regulations, promised in late June, will bring a lot of confidence to the markets but it would be really optimistic to say they would be done by the end of June as meetings were still being scheduled in the office of regulatory review until the end of May," said Swanson.

There is an ongoing conflict between Federal and local jurisdictions which does not seem to be going away anytime soon. In the last edition of Robotics Law Journal, we highlighted the regulatory landscape in California where different cities looked at drone regulation in quite different ways.

"Although, in a very broad brush, you could say that once a plane gets off the ground then the FAA takes over, there is a lot of tension between federal and state and local authorities over the regulation of UAS since state and local leaders are interested in meeting their constituents' concerns related to UAVs, particularly in the privacy area," added Swanson.

New Work, New Tools

Law firms are starting to look closer at the organisation and editing of data in their search for more efficient ways of providing legal services

Artificial Intelligence (AI) software is revolutionising the ways in which lawyers work. After a lifetime of 'sorting and sifting' being a junior lawyer's basic skillset, computer algorithms are faster and more economical. RAVN Systems, an AI consultancy and software developer, has started winning contracts from law firms to help them perform repetitive tasks in a much more efficient way. Robotics Law Journal spoke to their CEO Peter Wallqvist.

"We have a lot to thank the regulators for", says Wallqvist. In the UK, the new regulatory regime around Alternative Business Structures and the competitive landscape of client fee pressure has led to a more encouraging approach to process efficiency models. The practice of hourly billing is under more pressure in the UK than in the US where the process efficiency argument is only working with the firms at the very top end. "There needs to be a culture at law firms of not charging by the hour", says Wallqvist.

> "originally engineers would work with slide rules and equations but now they have calculators and computers

Starting in 2010, RAVN was founded by ex-Autonomy engineers and without any investors. In the early years they funded the business with consultancy work while developing the software. It took 3 years to develop the Applied Cognitive Engine (ACE) application. Working at Autonomy, the founders thought they were spending too much time on the search element but not enough on the understanding element.

As part of their consultancy work they discovered that in law firms in particular there were a huge number of processes that were just about finding and highlighting important data from ever growing piles of unstructured data. Their consultancy background also meant that they could spend time working with pricing teams at law firms and to make the software "part of the mission at that firm".

RAVN Systems CEO, Peter Wallqvist

RAVN is riding a wave of interest in AI by professional services firms made possible by a number of recent developments. "The convergence of AI and unstructured data is made possible by a massive increase in computing power and the inter-connectiveness of data" says Wallqvist. "Extranets have helped immensely because all the data is collated and ready. Cloud computing has made a lot of things easier."

> "The convergence of AI and unstructured data is made possible by a massive increase in computing power and the inter-connectiveness of data"

Although the recent trend among some law firms is to reduce transaction costs by employing lower paid workers in lower cost locations to conduct repetitive tasks, the use of AI would seem to be a much more efficient and scalable solution. It could also give smaller firms more muscle to conduct different kinds of work for which they would normally need an army of junior lawyers or paralegals. "When we are in a room with a partner, the coin really drops when the conversation moves on from how much money they could save to how they could get to do work they would not otherwise get to do".

> "There needs to be a culture at law firms of not charging by the hour"

RAVN, whose current client list includes Linklaters, BLP and Taylor Wessing, thinks the law firms are responding to client demand for different and more efficient ways of working. There are always better tools being developed. As Wallqvist says "originally engineers would work with slide rules and equations but now they have calculators and computers".


AUDS set up


Chess Dynamics

Anti-Drone Collaboration

The flipside of the rapidly increasing Drone market is another market devoted to thwarting them

The Anti-UAV Defence System (AUDS) is the product of three different British companies: Blighter Surveillance Systems, Chess Dynamics, and Enterprise Control Systems. The capability is designed to detect, track and interfere with UAVs that are engaged in potentially malicious activity. Robotics Law Journal spoke to Chess Dynamics about AUDS and what it will mean for the future of drone use.

The malicious use of drones has been rising, with high profile breaches of security at the White House and the high number of incursions over nuclear power stations, especially in France. Equally, there has also been a rise in announcements of anti-drone technology being implemented, such as at Euro 2016, reflecting the newly emerging potential threat. The necessity for a specific technology like this came about due to airspace violations over the DMZ between North and South Korea, whereby North Korean drones, whilst being detected, could not be combatted. This was the genesis of AUDS.

There are three parts to this system. First, the Blighter radars will detect a UAV in a designated target area, regardless of weather conditions. Once acquired, the target is handed over to the Chess Dynamics Hawkeye Deployable System, which uses both thermal and daylight cameras. The UAV is tracked, identified and classified. The human operator will then able to make the decision early, using all the information gathered from the radar and the EO tracker, to use the Enterprise Control Systems inhibitors to interfere with the C2 channels on the UAV in order to disrupt it, keeping collateral damage to a minimum.

Collaboration

None of the three companies could have created this technology on their own, they were all able to identify and recognise their skill sets and how they could complement each other. Collaboration has brought about this unparalleled success and in the quickest possible time – it took just a few months to create a prototype from the three CEOs originally putting their heads together. As with a lot of technologies, getting in early counts for a lot and the speed this collaboration has afforded them has been a real advantage.

Regulations

With AUDS, the interference stage involves radiating electronically, which requires the operator to have a licence. For all types of electronic radiation, particularly in controlled bands, the operator needs a licence. This is a pre-existing regulation that applies to those who would wish to operate AUDS, and helps to ensure that it can't be used by just anyone wanting to survey the area around their house, for instance. The prevention of intentional malicious use or accidental misuse of both drones and any countermeasure, that could cause collateral damage in some way, is the main aim of such regulation.

Unsurprisingly therefore, the client base is restricted, at present, to national and international government departments. The UK has some of the strictest export control legislation in the world. With technology like this it is important that the Ministry of Defence and the other government departments that are part of the Export Control Organisation (ECO) know who the potential customers and users are, and they need to be shown to be responsible upstanding people. Most applications to international government departments from friendly countries have been successful and no warning flags have been raised within ECO.

If an unscrupulous company or person was interested in acquiring this technology to enhance their own security, they would have to go through a very stringent vetting process. It is a test of the individuals' or organisations' trustworthiness and character that determine whether or not the UK Government will licence the sale. This is both necessary to avoid the danger of the technology getting into the wrong hands (3rd party exploitation), but also to protect IP.

Could it be sold commercially in the future? Technically it could, but there would have to be close oversight by governmental departments. If an energy company wanted to protect its power stations and could make a strong case for acquiring this technology (the protection of critical national infrastructure), they would charge their security contractor for updating the security perimeters who would then become a buyer of the AUDS. That contractor would naturally be licensed themselves by the government to buy and operate it.

The future will undoubtedly hold some commercial aspect for this technology. Much like UAVs themselves, it began life as a military technology, became miniaturised and moved to being developed commercially. Future regulation would have to deal with a greater potential for misuse, the same way that drone regulation is hitting those same barriers at present. For the moment, the regulation complements the use of this technology on the governmental level and doesn't hold any serious barriers because it is not yet being sold commercially.

So the regulation rests primarily with the licensing structure and presently this is very much restricted to government departments. Should commercial operators be delegated the responsibility for using this technology, they would have to ensure that only approved people are the ones that are using it. Great care has to be given on who it is demonstrated to and who it is likely to be sold to.

US interest

The US is the single biggest technology market in the world. While they like to protect their own industries, they are equally happy to go abroad if they lack an ability to produce a particular capability on their own. The wide range of scenarios that AUDS can be used in is its major selling point. The threat from drones is global in this regard, and is the same regardless of whether an operation is military or civilian. AUDS and its parent companies were looked at closely by US authorities before being invited for trials. AUDS' US distributor, Liteye Systems, has been successful in promoting the capability in the US which has led to the FAA shortlisting the technology for evaluation at a number of US airports within its Pathfinder system.

THE IAA USES A RISK-BASED APPROACH TO THE SAFETY REGULATION OF DRONES. A SPECIAL OPERATING PERMISSION (SOP) ALLOWS USERS TO OPERATE THEIR DRONES BEYOND THE LIMITS THAT ARE DEFINED IN LEGISLATION IN CERTAIN CIRCUMSTANCES AND SUBJECT TO CERTAIN CONDITIONS

Irish respond to Drone increase

Ireland is another country which is responding to an increase in the use of civilian drones and introducing new regulations to govern that use. *Robotics Law Journal* asked the Irish Aviation Authority to provide details of their current position.


Dublin Airport

How did the IAA go about developing its UAV regulations?

The IAA started reviewing the regulation of Small Unmanned Aircraft (SUA) in 2010, in response to the increasing SUA activity. A number of amendments to the existing legislation were published and a new regulation was published in 2015 (S.I. 563 of 2015). When developing the new regulation, IAA took account of developing SUA legislation worldwide, the work on-going in JARUS (Joint Authorities for Rulemaking on Unmanned Systems) and the framework for future SUA regulation published by EASA (European Aviation Safety Agency). Further details on IAA SUA regulation can be found here: https://www.iaa.ie/general-aviation/drones/drone-regulations-guidance

What is the current level of activity in the area? How much do you expect it to grow?

There has been significant growth in the use of SUA in Ireland in recent years, reflecting the worldwide trend. The IAA expects this trend to continue. There are currently over 5,000 SUA registered with the IAA, which includes both drones and model aircraft.

The European Union is leading the development of regulatory standards to cover the use of SUA across the whole of the EU and Ireland is actively participating on the EASA working group.

How many specific permissions have you given for UAVs? How long does it normally take for the processing of an application to take place?

A Special Operating Permission (SOP) allows users to operate their drones beyond the limits that are defined in legislation in certain circumstances and subject to certain conditions. The length of time it takes to process an application varies according to the quality and compliance of the application. There are approximately 120 SOPs currently valid.

Which commercial areas of activity do you see as being among the most important in future? (eg agriculture, aerial photography, filming...)

At the moment, drones are being used in Ireland for a variety of purposes including recreation, aerial photography/video and aerial survey. The IAA expects that as the industry develops, SUA will be utilised across many more areas.

Could you give a brief outline of the major features of your regulations?

The IAA uses a risk-based approach to the safety regulation of drones. A Special Operating Permission (SOP) allows users to operate their drones beyond the limits that are defined in legislation in certain circumstances and subject to certain conditions. Each application for an SOP is assessed on its merits and with a view to ensuring safety. The IAA has engaged with those who have operated drones unsafely and come to our attention, with each case dealt with on an individual basis and evaluated for its potential impact on safety. Any unauthorised use of SUA may be referred to An Garda Siochana (the Irish Police) for investigation.

Do you expect to update your rules after European rules are introduced through the EU and EASA?

The European Union is leading the development of regulatory standards to cover the use of SUA across the whole of the EU and Ireland is actively participating on the EASA working group. Normally, whenever a new EU rule is introduced, it automatically becomes law in Ireland.

How and when do you expect to see Beyond Visual Line of Sight flying to develop? (Is it allowed or catered for in your current regulations?)

Some operators have already tentatively indicated an interest in pursuing Beyond Visual Line of Sight operations. Each case will be accessed and an SOP issued if the IAA is satisfied that such operations can be undertaken safely.

To what extent are you liaising with the police and other security forces? Is enforcement something that the IAA is primarily responsible for - or will it be shared with the police and other bodies?

The IAA is actively discussing aspects of SUA use with other State agencies, including An Garda Siochana and the Data Protection Commissioner.

The IAA has engaged with those who have operated drones unsafely and come to our attention, with each case dealt with on an individual basis and evaluated for its potential impact on safety. Any unauthorised use of SUA may be referred to An Garda Siochana for investigation.

How will you address the issue of trying to keep the regulations abreast of the fast-developing technology in this area?

The IAA closely monitors developments within the SUA industry and maintains a dedicated staff with responsibility for the area. The IAA actively participates on international fora, such JARUS (CONOPS, Ops and Licensing working groups), EASA and the EU.

How much contact do you expect to have with the Unmanned Aircraft Association of Ireland and other manufacturers and operators?

The IAA is in regular contact with the UAAI and SUA manufactures. The IAA also actively participates at various SUA related events and trades shows, such as Drone Expo and MojoCon.

Lifelong Learning

Seamus Nevin

Technology is taking hold of the workplace and the education system needs to adapt. A new report from Seamus Nevin, Head of Employment and Skills Policy at the Institute of Directors (IoD), suggests some reforms.

Demographic and technological changes are transforming the world of work. These changes inevitably raise concerns about the impact of this impending revolution on the number of jobs and the future of society. However, the ageing workforce and the so-called 'rise of the robots' do not need to presage the apocalypse that so many are predicting. Since the first industrial revolution, each wave of economic change has been met with public anxiety. Yet, in the long run, each bout of worry has proved misplaced. The lesson from these events is the importance of enabling people to re-skill and upskill in order to succeed in the new economy. As the fourth industrial revolution continues to radically alter the world of work, reforming education and training will be of vital importance. There are four key areas where significant progress needs to be made to ensure the UK is prepared to succeed in this new economic landscape.

Curriculum

- The UK education system began to take shape in 1858, and featured mass public examinations based on pupils' ability to recall information and apply standardised methods. This remains essentially the same way we educate today.
- The expansion of the internet means the labour market no longer rewards workers primarily for what they know, but for what they can do with what they know.
- UK education policy is at risk of turning our schools into 'exam factories' still teaching method and recall, the easiest skills to automate.
- Schools must refocus on the application of knowledge rather than simply the acquisition of it, to boost the level of soft skills in future generations.
- A welcome emphasis on coding and increased emphasis on Stem (Science, Technology, Engineering and Maths) subjects will provide stronger foundations for the digital revolution, but teaching new technologies using old approaches is no longer suitable.
- Education curricula should be independent of political interference and instead informed, and continuously re-examined, by an expert body of providers, businesses, academics and other stakeholders with a focus on delivering education today for tomorrow's workplace.

Guidance

- The level of careers guidance given to young people is inadequate, with what little there is focused on an outdated and static idea of a jobs market
- In the UK education system, learner choice is playing an increasingly important role, so it is vital that students have the information they need to succeed in a rapidly changing labour market.
- Stem skills will underpin many of the potential high-growth industries in the UK economy, but the misperceived importance of higher A-Level grades is turning students towards subjects they will do well in, rather than those that will be most valuable in the workplace.
- In the 21st century, education doesn't end at school and businesses must play their part. The focus must be on in-work training and providing a career lattice, rather than a career ladder, where employees can develop by doing a range of different roles, gaining experience, developing new skills, and tapping into alternative networks.
- Government must play its part too, bringing together industry-wide collaboration between businesses and employers, ensuring every school has a suitably qualified, dedicated full-time careers coach whose job is to provide independent careers education and guidance and to coordinate employer engagement for students.
- Multiple, high-quality work experiences should become compulsory for all students from the age of 13 onwards so that young people can learn from employers and be better informed and equipped to make the right choices to help achieve their future career aspirations.

A welcome emphasis on coding and increased emphasis on Stem (Science, Technology, Engineering and Maths) subjects will provide stronger foundations for the digital revolution, but teaching new technologies using old approaches is no longer suitable.

Provision

- Automation and digital technology offer new routes for the provision of education via computer-based outlets.
- Distance education is nothing new but recent innovations in 'Massive Open Online Courses' (Moocs) enable independent vocational learning more conveniently and cheaply than ever before.
- The cost savings, convenience, and flexibility that online learning offers has the potential to revolutionise education provision, but only if businesses and the education sector work together.
- In this self-guided environment, students and workers will become central in regulating their learning and determining the development of their own skills, meaning that one of the core functions of 21st-century schools will be teaching students how to learn for themselves.
- In a world of online media, which can become an echo chamber of one's existing opinions and interests, digital skills will need to be complemented by the development of critical analysis, evaluation skills and self-regulation.
- This will be vital as global credit transfer systems develop that will allow student consumers to use courses offered by one institution (both online and in-house) to count towards their qualification from another, and to build up gradually to a degree at different times rather than completing it all in one go.
- Rather than thinking of progress as a linear measure through the curriculum, the breadth of development will also be important.
- The government should use the new higher education Teaching Excellence Framework (TEF) to incentivise education providers to expand their provision of computer-based and blended learning opportunities to enhance access to education, reduce the costs of provision, and capitalise on a growing demand for alternative learning opportunities.

Finance

- On-the-job training and e-learning offer part of the solution but finance is also key.
- Affordability and limited credit options are the biggest barriers to workers enrolling on part-time or further education.
- Lifelong learning has a key role to play in boosting productivity, contributing to economic growth and aiding social mobility. For these reasons, financial incentives to facilitate continuous engagement in education throughout a person's life should be explored by government.
- The relevant government departments should work together to facilitate lifelong learning. The value of tax incentives can provide a worthwhile 'nudge' towards the enhanced uptake of lifelong learning opportunities.
- An enhanced tax deduction for employers would encourage them to invest in training their staff.
- The income tax system should therefore be flexed to encourage and enable individual learners to upskill throughout their working lives.

The fourth industrial revolution will bring significant challenges, but also huge opportunities. If the UK is to build a competitive economy for the 21st century, a shift to lifelong learning will be crucial to ensuring that UK workers have the skills they need to succeed in the new world of work.

IN 2013, MCKINSEY & COMPANY ESTIMATED THAT IF THE USE OF ROBOTIC PROCESSES GROWS AT THE RATE EXPECTED, THEN BY 2025, AS MANY AS 110 TO 140 MILLION FTES WILL BE REPLACED BY AUTOMATED TOOLS AND SOFTWARE

Robotic Process Automation – Outsourcing 2.0

Chris Holder, a partner and outsourcing expert with Bristows, looks at new developments in Outsourcing

Chris Holder

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 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 the method of 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 to 140 million FTEs will be replaced by automated tools and software.

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

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.

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 additional advantage would be the ability to obtain 'better' data and feed it into related applications. This would mean that the likelihood of data errors being compounded by human error would be reduced, allowing the enterprise to make better decisions.

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.

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.

> "robotic processes (or digital workers) are being used to replace human involvement and full time equivalents or FTEs"

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

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 application and premium administration service, which is currently outsourced by a customer to an offshore based company, this service is normally provided by the supplier subject to the terms of a service agreement and priced, mainly, with reference to FTEs.

The software and support that sits behind the process is usually invisible to the customer but the scope of the services, the level of services and the cost of the same is transparent and is 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 adapts how a supplier provides its services to its customer may not necessarily be required to be spelt out via a contract change because the customer still sees the same service being provided to it.

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.

The implications, therefore, of systems automatically making decisions in regulated areas without human involvement may be quite serious and this may result in some of these RPA solutions attracting the interest of relevant regulators if, for example, these systems are providing financial advice to end users.

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 created by the FTEs and assigned to the customer via an 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. 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.

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.

In Nova Productions v Mazooma Games, 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 person's 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.

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. 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.

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.

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 price, 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 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.

> "the impact for the offshoring industry, where its growth has been underpinned by the wage arbitrage effect, could be vast. No longer cheaper, it will have to adapt"

Summary and conclusion

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 replaced 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 Legal Implications of Cyberwar

James Connelly

James Connelly, Professor of Political Theory at University of Hull and Director of the Institute of Applied Ethics, has just presented a paper at the 2016 Euro-ISME conference and is the principal investigator of the ESRC funded project, 'The Common Good: Ethics, Rights and Cyber Security'. He discusses some of the questions surrounding the ethics of cyber counter-terrorism and the implications for legal systems with the Robotics Law Journal.

What is cyberterrorism and is it distinct from cyberwar?

They are distinct but their definitions overlap, and can sometimes be used interchangeably. The old-fashioned view of a war is that you have two opponents who openly declare war, and if it is to be a just war, there are also certain conditions that are upheld regarding how the war will be fought – not harming innocents, treatment of prisoners and so on. In the case of cyberwar it's not clear if it's ever declared. A lot of cyberwar consists of a series of cyber attacks, but when do they constitute a war? Is one attack a war? Cyberwar, in a sense, has a parallel with Pearl Harbour in this regard. Pearl Harbour itself wasn't a war, it was an attack with no declaration, though it led to the US declaring war. Cyberwar seems often to take that form. Cyberwars are usually not of the type or duration of war that we're used to. In that way it is remarkably like cyberterrorism.

The difference between the two often depends on who the perpetrators are and you have to consider what distinguishes conventional war from terrorism in the first place. One way of looking at it is to say that terrorism is something that non-state actors do (even though state actors can use terror, you don't normally call them terrorists). Terrorism tends to have political goals, as does war. However, terrorism does not typically abide by, or seek to abide by, the rules and conditions of war. In principle, cyberterrorism and cyberwar are overlapping but different.

> "In the future, it's likely that we will stop talking of cyberwar or cyberterrorism as being separate entities, instead being just a component of war and terrorism"

In cyberwar, the effects that we are concerned with are principally measurable physical effects. In that way, it is clear that cyberwar and cyberterrorism are almost the same as war and terrorism respectively but simply by other means.

It's a delicate question because they are closer to each other than traditional war and terrorism are to each other. Though it has to be noted that conventional warfare has changed a lot in recent years. It has now moved to small asymmetrical guerrilla-type conflicts, instead of a traditional conflict between two opponents. Examples include fighting in the Vietnam jungle or Iraq desert as opposed to the British and the Germans taking it in turns to bomb each other.

In the future, it's likely that we will stop talking of cyberwar or cyberterrorism as being separate entities, instead being just a component of war and terrorism. Cyber attacks will still be recognised as distinct, but the other lines will have blurred.

Which systems are most likely to be targeted?

Ultimately, the only attacks that will be seen as worth doing are the ones which have physical effects, and most cyber attacks do. The most 'innocent' looking attack will have some effect you can feel, even if it is just slowing down a system. For example, if you were to hack into the stock exchange and just slow down its processes, people will gain or lose money, and therefore gain or lose power, property and so on. Slowing down that system at a specific moment might be enough to gain a crucial advantage.

Certain types of weaponry are obvious targets, either their development or their operation. On the state level, if you suspect another state of secretly developing a nuclear bomb, you target a nuclear power station's systems, in order to hinder or disable the development. Most types of weaponry now are part of the internet of big things, with ships being designed and arranged electronically; gaining access to such a ship's operation would grant you great power in the physical world.

Terrorism is unlikely to ever draw the distinction between military and civilian targets, and in the cyber world, civilian systems are being targeted more often. Anything that's operated electronically will offer some route of remote access. Cyberterrorism is likely to want to cause as much havoc as possible in order to cause the terror to gain its political goals. Cyberterrorism is likely to target civilian systems; as collateral damage, or where you want to simply slow down a system to gain an advantage.

Cyberwar, being considered the cyber arm of normal war, might target all sorts of systems but remain restricted to military targets. Obviously sometimes in war there is collateral, some civilian loss of life or civilian harm caused indirectly by targeting a military target, but there is usually an attempt to keep such damage to a minimum. A cyberwar is likely to maintain this restraint against targeting civilian systems, or to at least keep this collateral at a low level.

However, the opening up of civilian systems makes the possibility of 'Total War' that much closer. If a war becomes a 'Total War' both parties might start targeting civilian structures, directly or indirectly.

What are the responses to cyber terrorism?

There are two major responses: one is just making sure that you are building good cyber walls against any potential attack; the other is to attack the potential attackers, either pre-emptively, or if you have failed to build a good cyber wall, retroactively. Primarily, the response is to focus on enhancement of cyber security.

The reason for this is because of the proliferation of cyber attacks; it has to be assumed they are happening all the time. As a very primitive example, phishing emails are rife in the internet, and are sent to everyone. Most of the time these are safely ignored, but the numbers are impossible to quantify. It then goes all the way up to more sophisticated and invisible attacks,

equally hard to quantify. So we don't know how much of this is going on.

On a personal level, you know when you have had a computer virus, but not necessarily when you receive an unsuccessful attack, just as with physical colds and viruses. I have been in contact with people who have had them and not known about it. But on those occasions when I have caught a cold, one of the first thoughts is, 'who gave me this?'.

Tracking a successful attacker is desirable, but if you have a good enough security system, you're unlikely to be able to find out who it was as the attack will have likely just 'bounced off'. So it's almost a paradox that it's possible to have a great security system but it denies you the ability to find out who are these agents and so you can't improve it further. Due to the severe quantity of attacks and the difficulty in ascertaining the identity of the attackers, the main response is to increase the security.

Even more important than who is how. Whether or not the full extent of the attack was successful, how they got through the security system is vital information for increasing the level of security.

How is this coded in law?

Essentially it is a case of modifying the existing law to cover cyberwar or cyberterrorism, or simply stating how it will be applied in these situations.

The Tallinn agreement is the most high profile international agreement, though non-binding, about how international law applies to cyberwar (due for a second edition later this year). There is an enormous amount of international law and agreements of the conduct of cyberwar out there, ranging from international and regional agencies, to action plans released by the G8. So there is a lot of legislation there, aimed mainly at ensuring that states have the right tools to combat the cyber threat.

Proportional response is a much trickier issue with cyber attacks, which often take the form of small and seemingly insignificant attacks over a period of time, each one almost unnoticeable, but that have a huge cumulative effect. In response to an individual attack, a direct attack in response would seem to be out of proportion. The questions of at what point are you justified in fighting back becomes difficult to answer, and depends on the nature of the cyber attack. Sometimes they have immediate and obvious effects, but often they are less tangible.

> "Terrorism is unlikely to ever draw the distinction between military and civilian targets, and in the cyber world, civilian systems are being targeted more often"

How do you think the law needs to change in the future?

Both with the law – domestic or international – and ethics, the prevalent view is that we don't need to change the principles we have, it's more useful instead to just modify their application. We need to keep them up to date for new circumstances, instead of panicking and thinking that we have to change everything, which leads to regarding cyber actions as a completely and utterly new issue, different from everything else. A cyber attack is still the basic idea of 'I'm going to attack you for a purpose,' whether it's cyberwar, -crime, or -terrorism. It's the threshold questions that are different.

If you start with cybercrime the question is what is it in law you need to focus on? Is it the intended outcome of the crime or is it the means that they employ? Normally it's the intended outcomes, and that's no different to the laws we have now. It doesn't matter if you sneak your way into the Bank of England, explode your way into it, or electronically transfer funds out of it, the point is, you're trying to run off with the money. That is what you are targeting in law, not specifically the means of the theft.

Attacking the means is not usually a viable option. In the example above, it would be similar to banning all cars just because the robber used a car to get to the bank. The method is not relevant compared to the intended outcome; and if cars are banned, the burglar will just walk to the bank the next time.

It should be an extension of law, rather than something you have to rebuild from the foundations. The Tallinn agreement is essentially doing that, codifying the way that the law needs to be applied to cyberspace as oppose to redefining the law.

What are the main challenges for the law?

There are new and more cunning methods of attack being developed all the time, leading to unanticipated possibilities using cyber means. Because of this, in the cyber world, the law can fall behind very quickly.

The speed of new technologies and methods of attack can take advantage of loopholes in law, similar to tax havens. Tax evasion is illegal, but there are ways to get around that that are exploited. There are new ways of laundering money using the internet and other technologies, making it easier than it is do that physically. Because the range of the means keeps expanding, the law must be updated regularly to keep pace.

Identity theft using Facebook meta data is something no one thought could be a possibility ten years or so ago. This example is still tied in to the idea that there are limits on how much you are allowed to find out about people. The prevalence of information afforded by the internet has given us this new problem (or new aspect to an issue) which needs to be coded in law.

Something that can be directly criminalised is deliberate attempts to gain information, knowledge or property that isn't yours, which is why intellectual property rights are so important. If I am trying to hack into a system to gain knowledge which isn't mine, that's no different from any other form of robbery or theft.

We want a free internet; if we're not paying for it, then we're the product. We are the ones the companies are buying and selling, that's why people want our data, we are the products for the companies. What are the limits of that data gathering? That is one of the truly new things that we need to account for in law.

Who needs to be involved in the discussion of the ethics of counter-cyber terrorism?

It's a question of stakeholders. One can argue that there are differences and distinctions between cyber war, terrorism, crime. The principal stakeholders are the main agents of the state. The armed force, police force, the security force, the intelligence force, all these are going to be involved in cyberterrorism, as is the case with normal terrorism. All the organs are going to be called in to counter cyberterrorism. The difference is that there are going to be specialist divisions in those agencies to specifically deal with the new type of threats.

The other people that need to be involved are normal citizens. People are being asked to report others if they see examples of cyber bullying or mysterious behaviour. If someone is suspected of recruiting others to go to IS through a laptop, citizens are being encouraged by the state to turn in those people. There is obviously a danger of this going overboard – people reporting anyone because of personal biases and so on. Vigilantism has to be avoided, but citizens keeping an eye out for potential problems should not discouraged. Engaging the public properly is going to be important if they are going to be involved in this discussion. The public is an important stakeholder.

This work was supported by the Economic and Social Research Council

Drones on the Up

A new report from PWC looks at the potential future value of the drone market

PricewaterhouseCoopers released a global report examining the commercial applications of drone technology. 'Clarity from above', dated May 2016, seeks to quantify the impact of the emergent technology across industry sectors. The use of the term 'drone powered solutions' reflects the broader applications of drones, rather than just the use of the machines themselves, such as the increased ability for capturing data. Consideration is also given to the regulations involved and their impact in the development of the drone industry.

$127 billion industry

$127 billion is the value of current business services and labour that could be replaced by drone powered solutions in the near future, according to the report, broken down across these sectors.

One of the biggest assets that drones provide is the speed at which they can monitor a large area. This is particularly useful in infrastructure and agriculture, the sectors that have the largest values in the report. Providing detailed field data improves the speed and quality of the planning stage of a construction site, while during the construction stage they can provide incredibly fast progress reports, overlaying plans onto photos of the actual state of construction, able to identify discrepancies of even 1cm. This level of accuracy, combined with their speed, demonstrates the value of drone powered solutions to this sector.

Performing dirty, dangerous, difficult jobs is one of the principal uses of drones, allowing a lot of sectors to increase their level of safety for employees. Maintenance of radio or phone towers is a potentially dangerous job for someone, risking injury or loss of life, especially in bad weather. Sending up a drone has little risk of harm and also avoids the need to set up any equipment that a human would need to climb the tower, enhancing its speed.

Mostly used in open-cast mining so far, drones are a faster and cheaper replacement for helicopters and can provide solutions for the labour-intensive stages of planning and exploration

The ability for drones to assist in sectors such as mining is significant, and demonstrates the huge value and untapped potential for this technology. Mostly used in open-cast mining so far, drones are a faster and cheaper replacement for helicopters and can provide solutions for the labour-intensive stages of planning and exploration. While still limited, due mainly to their reliance on GPS which is ineffective underground, there are future solutions using 3D scanning currently being researched. Telecommunications is another area where the potential for drones to assist in broadcasting signals is greater than their current application.

Regulators

The report concludes that for drone operations to be commercially viable, national and international regulatory frameworks may need to be completely overhauled, instead developing a set of international regulations, which would provide global consistency for UAV use. The International Civil Aviation Organisation (ICAO) is working on guidance for UAV operations and expects to complete its standards and recommended practices by 2020, with a manual for UAV operations ahead of that by 2018. The delay means that current regulation needs to be able to counter the various issues that arise with the use of drones, especially with regards to privacy and safety.

Performing dirty, dangerous, difficult jobs is one the principal uses of drones, allowing a lot of sectors to increase their level of safety for employees

POTENTIAL VALUE OF DRONE MARKET

SECTOR	VALUE	APPLICATIONS	FUTURE APPLICATIONS
INFRASTRUCTURE	$45.2bn	Area surveys during pre-construction and construction phases Maintenance inspections Asset inventory	Drones performing the maintenance tasks after diagnosis
AGRICULTURE	$32.4bn	Crop supervision Soil and field analyses Health assessment of crops	As the technology improves, so too will crop management and yields, making agriculture much more data-driven
TRANSPORT	$13.0bn	Delivery of parcels, spare parts, food Medical logistics	Airlines to offer drone transportation services due to similarity of fields
SECURITY	$10.5bn	Border and site monitoring Rapid reaction and real-time data monitoring	Autonomous sentinel duty and mass surveillance systems will be possible
MEDIA AND ENTERTAINMENT	$8.8bn	Aerial photography and filming Advertising Special effects Drone racing	Racing to become mainstream and better quality of filming and special effects
INSURANCE	$6.8bn	Risk monitoring and assessment Claims management by inspection of property	Improved predictions of damage by combining drones with machine learning
TELECOMMUNICATIONS	$6.3bn	Maintenance enhancement	Network optimisation by clearing signal between towers, and direct broadcasting of telecommunication signals
MINING	$4.3bn	Planning Exploration Environment Reporting	3D scanning technology as a replacement for GPS, allowing for comprehensive underground exploration

RECENTLY THE INDEPENDENT CONSULTANT DRONE INDUSTRY INSIGHTS MADE A STUDY COMPARING MODELS OF DRONES ACROSS THE GLOBE. FIVE OF CATUAV'S MODELS FEATURED IN THE TOP TEN FOR THE CATEGORIES OF 1-4KG AND 4-25KG WEIGHT DRONE

Blue Sky Drones - A view from Catalonia

Robotics Law Journal interviews Marc Beltran an aerospace engineer who works for CATUAV a drone manufacturer based outside Barcelona.

Urban Orthographic from a Drone

CATUAV is the oldest UAV company in Europe and has a core team of only six people. Recently the independent consultant Drone Industry Insights made a study comparing models of drones across the globe. Five of CATUAV's models featured in the top ten for the categories of 1-4kg and 4-25kg weight drone. They have also built their own drone testing centre – one of only ten in the world – with a bioclimatic and sustainable building, giving the ability to host their own piloting courses.

How has a company comprising only six people managed to compete globally?

I think the expected answer is about a unique business model, but instead it's just about passion. If you are happy with the things you are doing you work more efficiently. We think we are more competitive than other potential competitors that are a hundred people strong just because of this passion that we have for designing our UAVs and providing our services.

It's a case of having the right people; we've carefully chosen the people we want to have with us. Each of them is, for us, the best in those positions, giving us what we feel is a very competitive team.

Also our age is an advantage. We are the oldest UAV company in Europe and a lot of competitors have three years' experience at the most. Getting in at the start of a new technology gives you a real competitive edge and we are very fortunate in that regard. Our founder, who had been exploring the potential of UAVs in his spare time, was investigating their use in an airfield when the pilot of a landing jet plane was an executive of a company called Indra. After talking to the founder, he saw the potential of UAVs and soon after a contract was signed to develop UAVs for Indra. Fortuitous circumstances to allow us to get an early start but we have capitalised on it.

Is there anything specific about Catalonia?

For flying drones, the weather and climatic conditions really matter. There are other centres in Finland, Denmark, Iceland, North Dakota; but in these areas you have fog, the principal enemy of UAVs. Here in Barcelona, we can fly for more than three hundred days throughout the year where we have excellent conditions with no wind and a lot of sun. These factors are hugely significant.

South Portugal is another place where a lot of companies get their piloting licences due to similar conditions. In northern latitudes you don't have the same weather conditions to learn how to pilot effectively. Having a UAV test site close to the Mediterranean is a guarantee of having good weather and the availability of being able to fly for many days throughout the year.

Here in Barcelona, we can fly for more than three hundred days throughout the year where we have excellent conditions with no wind and a lot of sun. These factors are hugely significant

Is Catalonia/Spain going to be a hotbed of development?

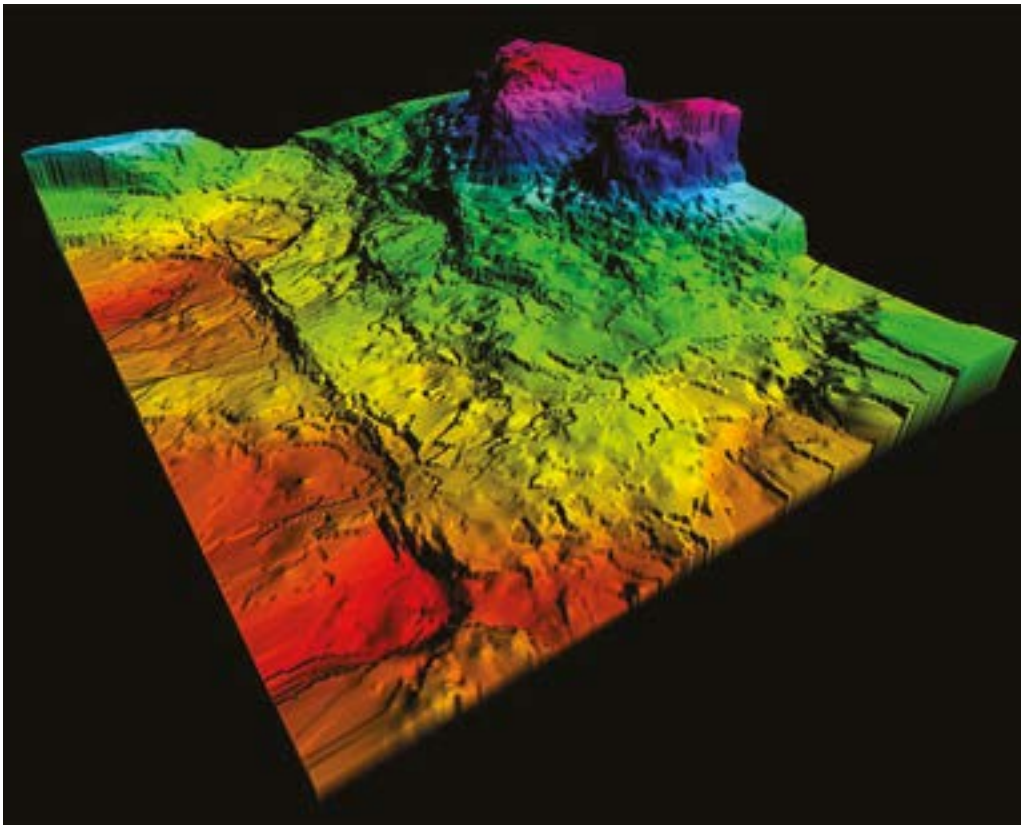
A few weeks ago, we held a meeting, supported by the Catalan government, where we put together all the principal actors in Catalonia that are dealing with drones. We were forty or fifty people representing different companies. It showcased how the area is fast becoming a hub in terms of UAVs; many new companies are being formed and there's a rising degree of interest. We're trying to coordinate with each other, so that we don't repeat the things another company is doing, such as one company focussing on agriculture observations, another industrial management and so on.

We think competition is good but at some point it's better to cooperate. If you're competing you're repeating things. If you're cooperating it's better for society in general. You've got all the necessities covered, it allows us to focus and get specialised in our areas, without having to dilute that specialism.

Is the regulation of UAVs suitable in Spain for your purposes?

So far it's provisional and a bit too restrictive. It's totally understandable due to it being a new technology that's rising fast, so the government has to put in regulations quickly to avoid collisions in urban areas and so on. At present, there is a ceiling of 120m, you cannot fly further than 500m, you cannot fly above urban areas, at night, above a concentration of people and so on. And of course you need to have a licence.

The tendency is for it to be like the automotive industry: having certified cars, have licences, only driving certain places. The idea here is that this becomes a specialised service. Not everybody can or should fly these things with the same degree of regulation. Tomorrow, if you were to buy a phantom for personal use, you could be flying it over the city, and if you have never flown it before, it



Large scale Topographic image

might be dangerous for the others. In specialised hands, under current regulation, that possibility for danger is greatly reduced.

What would you like to see happen with future regulation?

I would like, and I think it's going to happen, that a common regulation agency or system will be established for the entirety of Europe. We're within the European Union, it makes no sense that if you cross the border you face new regulations in terms of drones. So we will see something unified and a little less restrictive, but for the people who are specialised.

I want the law to become less restrictive for the specialised people and more restrictive for the hobbyists. It's safer for everybody but also more productive for everybody. Designate a lot of places where the hobbyist can fly and are not endangering anyone as well as not running the risk of accidentally falling foul of the law. As a citizen, I wouldn't want to see a cluster of drones fly near me and for the pilot to not know enough about how to operate them. As a specialist, I need to be able to pilot a UAV with a bit more freedom to maximise its potential.

We have one person who is an aerospace engineer. Unfortunately, he has to spend almost 80% of his time working here on complying with regulation

What is your legal team like and what are their priorities?

We have one person who is an aerospace engineer. Unfortunately, he has to spend almost 80% of his time working here on complying with regulation; it's becoming a little tedious really. Before an operation, he has to send emails saying we're going to be flying here, with this model; even in our test site, we have to specify which models are flying and everything. It all requires a lot of groundwork. So we have one person out of six doing all that groundwork.

Will it expand? It depends on how many operations you are doing. If you have a lot of operations, you should be dealing directly with the safety arm of the Spanish aviation agency.

Is there enough specialist knowledge among lawyers?

It's a big sector coming up. There are more and more drones coming up and people need to have insurance for drones which differ a lot from the previous insurance. It's something people don't know about a lot yet, but it's coming up. There will need to be an increase in the specialist knowledge so that the law can keep up with the technology.

Who are your main clients?

Our income comes from around the world, not just Spain. It's a global market, there's are so many different applications of drones everywhere. For example, Ecuador had a terrible earthquake recently, which wrecked communications. Nobody knew what exactly was happening and where. A picture from above facilitates the job of many people, helping the emergency services allocate their resources, as one example. In countries in Africa, there's the application of looking for elephant hunters.

Our income is divided into three streams. The first segment is the services we provide: we fly for somebody and they pay for the maps and photos. The second segment is the drone flying courses that we host at our drone test centre. The third segment is the test site for people renting out our facilities for their own demonstrations.

In terms of clients in services, we have precision agriculture, landmine detection, the marine projects and many more. It's a diverse client base, with the occasional governmental contract as they start to show more interest in this sector.

Is your client base likely to change in the future?

It's going to expand a lot. According to the recent report by PwC, it will balloon up to $127 billion by 2020. We hope it's going to increase and diversify our client base.

We were the early adopters and we feel that our experience will count for a lot when this sector undergoes a rapid expansion.

A GLOBAL SURVEY OF FINANCIAL SERVICES COMPANIES FOUND THAT 49% SAID THEY EXPECTED THEIR ORGANISATION TO USE AI AS PART OF ITS RISK ASSESSMENT PROCESS WITHIN THE NEXT 3 YEARSPROCESS WITHIN THE NEXT THREE YEARS

Compliance and AI: Sharing the burden

Financial services organisations are struggling to keep pace with regulatory demands. AI can help.

Mallinath Sengupta

Earlier this year, a global survey of 424 senior executives from financial services and fintech companies released by law firm Baker McKenzie found that 49% of respondents said they expected their organization to use Artificial Intelligence (AI) as part of its risk assessment process within the next three years. Twenty-nine percent expected it would be used in know-your-customer and anti-money laundering monitoring and 26% expected it would be used to help with regulation and risk and compliance.

NextAngles is a company in the Mphasis group which was recently bought by Blackstone from Hewlett Packard. NextAngles is using AI to promote smart compliance – using cognitive software to perform repetitive compliance tasks in a more efficient way and has a growing list of clients in the financial services sector.

Robotics Law Journal spoke to Mallinath Sengupta, the Chief Executive of NextAngles.

Following on from the financial crash in 2008, an ever increasing number of people are employed by the banks to work in the compliance sector. "The Chairman of HSBC once said that 10% of their employees were engaged in some sort of compliance activity. Banks are spending a huge amount in this area – 8 to 10% of their total costs are accounted for by compliance," said Sengupta. They are prompted to do so by the "pain model" – being pursued by regulators who will leverage huge fines if systems are not fully compliant.

But on the other side of this compliance equation, almost all banks are losing profitability with revenues spiralling downwards and they are looking to cut costs wherever they can. It is this perfect storm of regulatory and economic pressure that has created the opportunity for AI to produce a more efficient series of compliance processes.

Banks are spending a huge amount in this area - 8 to 10% of their total costs are accounted for by compliance

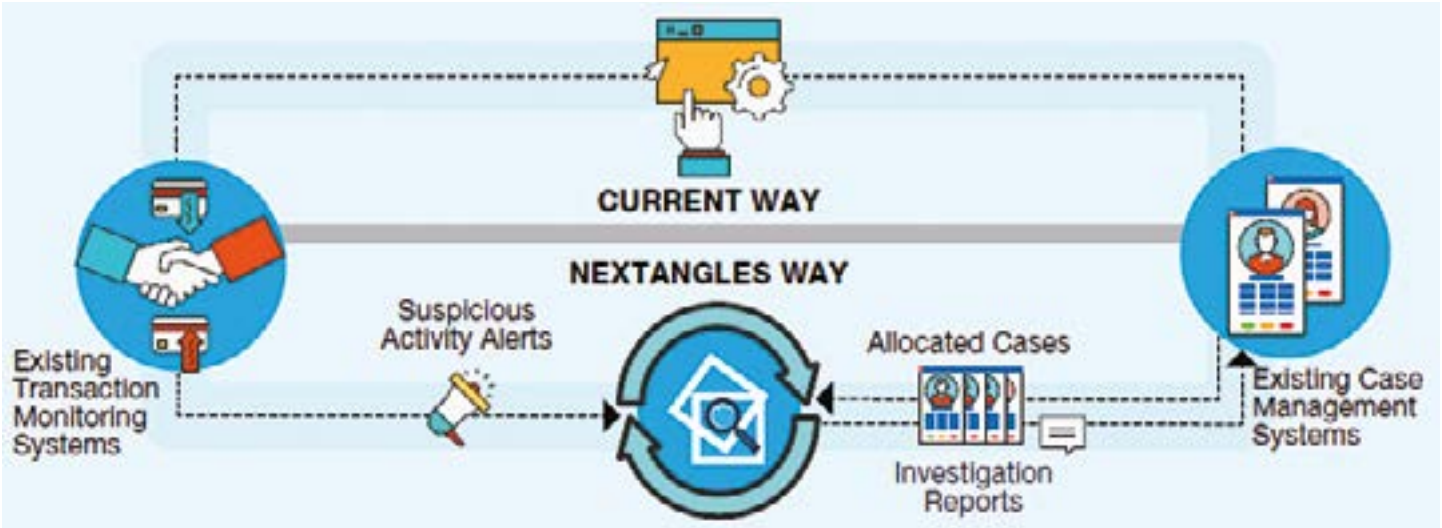
"Inside banks there are millions of transactions and thousands of employees. It is very difficult to check all of these manually. Banks are usually arranged into very different businesses with different regulatory needs and different systems all trying to be compliant," said Sengupta. Manual processes carry a greater probability of error and banks are also struggling to recruit enough numbers of the appropriate compliance professionals.

Unlike the iPhone type of AI which is wide but shallow, the AI we use is inch wide but mile deep. You need to go deep into the domain to get AI to work in real life

Anti-Money Laundering (AML) and Know Your Customer (KYC) protocols have been in place for years. Version 1.0 was basic information about your customer to prevent fraud. Version 2.0 after the financial crisis brought more regulation and enforcement. "Version 3.0 consists of two parts," according to Sengupta, "the use of Knowledge models and the availability of Interconnected Data." Knowledge models are built using specialists like Ontologists and the AI structure used is very focussed. "Unlike the iPhone type of AI which is wide but shallow, the AI we use is inch wide but mile deep. You need to go deep into the domain to get AI to work in real life."

Inside banks there are millions of transactions and thousands of employees. It is very difficult to check all of these manually

NextAngles automates today's largely manual AML investigation process to bring in 30% or more cost and time savings



NEXT ISSUE

JULY FEATURES INCLUDE:

"AI: An update from BAE Systems on patents and Artificial Intelligence

HR: As machines take on more and more repetitive tasks in the workplace, how does the role of the HR Director change?

Robots: Gartner estimates that 45% of the fastest-growing companies in the world will "employ" more smart machines and virtual assistants than people by 2018

If you would like to become a country correspondent for The Robotics Law Journal please contact Claudia Tan claudiatan@globalcitymedia.com

Analysis and insight for the industry - lawyers, regulators, manufacturers and users

THE ROBOTICS LAW JOURNAL

SUBSCRIPTION INFORMATION

The Robotics Law Journal provides lawyers and others working in the industry with a clear understanding of the increasing opportunities that are now presenting themselves to manufacturers and users of robotics and AI - and all the regulation that this needs and entails.

Central to the journal is the focus on the drone sector - predicted to become an industry which will be bigger than that of manned aviation.

YOUR ANNUAL SUBSCRIPTION TO THE ROBOTICS LAW JOURNAL WILL BRING YOU:

The Robotics Law Journal delivered to you bi-monthly (6 per year) in a digital pdf format via email.
A paper (hardcopy) edition mailed to you (optional)

Full access to the Robotics Law Journal online service which will include:

- Latest issues and archived issues
- All premium editorial content
- Regulation update
- News alerts bringing you the latest breaking news
- Timeline of key industry regulatory and other milestones
- Drones Focus

For more information on how to subscribe please contact

subscriptions@globalcitymedia.com
or call +44 (0) 20 7193 5801

www.roboticslawjournal.com **Editor:** Des Cahill , descahill@globalcitymedia.com. **Assistant Editor:** Tom Connelly, tomconnelly@globalcitymedia.com. **Reporter:** Victoria Basham, *victoriabasham@globalcitymedia.com.* **Events Director:** Maria Sunderland, *mariasunderland@globalcitymedia.com.* **Head of Asia:** Claudia Tan, *claudiatan@globalcitymedia.com.* **Head of Digital:** Elanganathapillai Sivakanthan, *siva@globalcitymedia.com.* **Marketing Exec:** Sonia Fernández-Ponce, *soniafernandezponce@globalcitymedia.com.* **Social Media Exec:** Thomas O'Brien, *thomasobrien@globalcitymedia.com.* **Design:** Paul Carpenter, Stimulus Design. *paul@stimul.us.* **Publisher:** Mary Heaney, *maryheaney@globalcitymedia.com.* **Chief Operating Officer:** Ben Martin, *benmartin@globalcitymedia.com.*

Subscriptions: T: +44 (0) 20 7193 5801 *subscriptions@globalcitymedia.com.*

Published by: GCM Publishing, Global City Media Ltd, 86-90 Paul Street, London, EC2A 4NE, United Kingdom. T: +44 (0) 020 7193 5801

GCM PUBLISHING