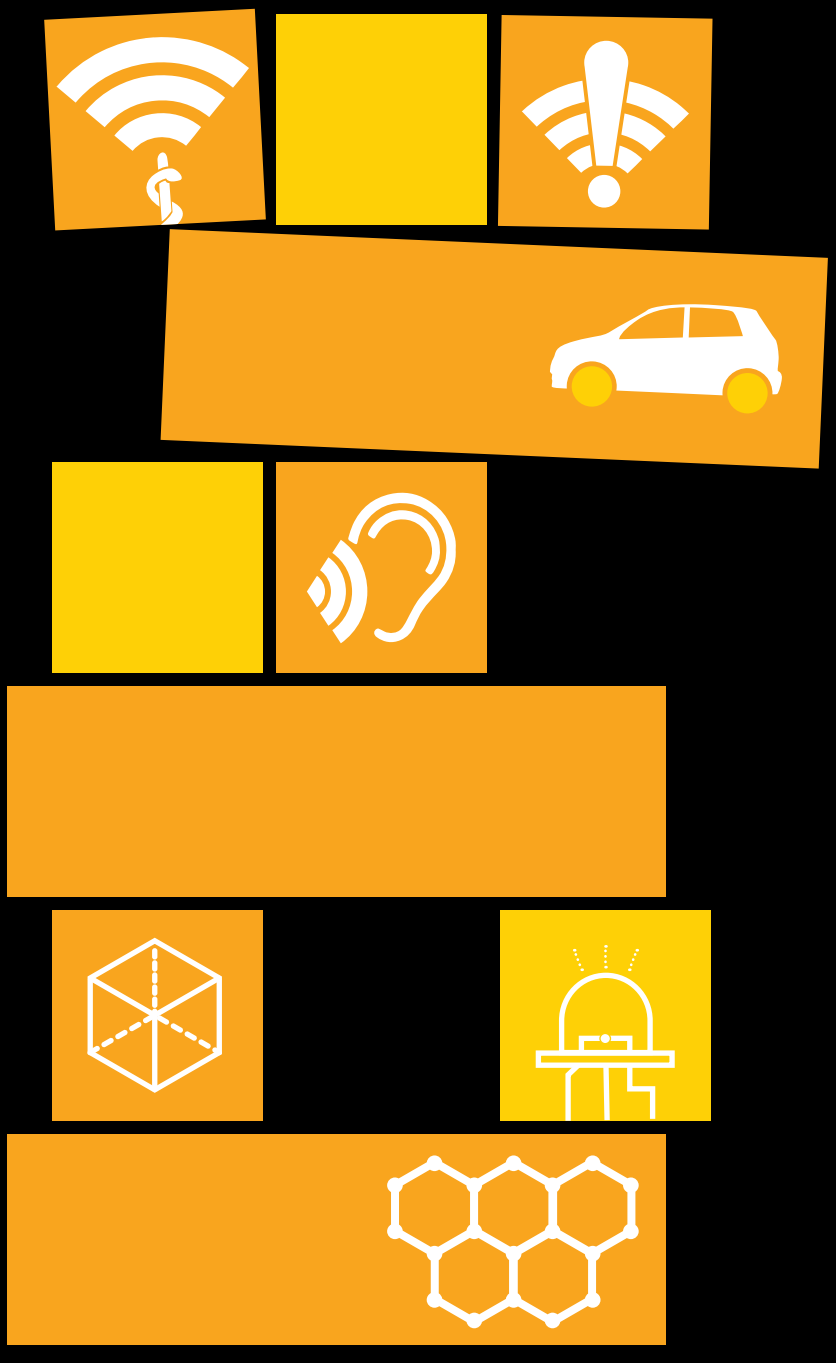
Kennedys

Legal advice in black and white

Emerging risks report 2016



Foreword

> “We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before. We do not yet know just how it will unfold, but one thing is clear: the response to it must be integrated and comprehensive, involving all stakeholders of the global polity, from the public and private sectors to academia and civil society.”
>
> **Klaus Schwab**, Founder and Executive Chairman, World Economic Forum (14 January 2016)

In January 2016, the World Economic Forum launched its much vaunted Fourth Industrial Revolution. Whilst some believe that we remain in the Third (digital) Revolution, the recognition that we are seeing a rapid, powerful convergence of big technology changes cannot be ignored. Autonomous vehicles, genetic editing, sensors, biotechnology, 3D printing, robotics, and artificial intelligence are some imminent changes.

The extent of that impact on society, employment, privacy and corporate control and how to live with it is likely to remain on the global agenda for the near future. Disruptive technologies and the growing digital economy will continue to be a primary focus in the business community – bringing into play the potential for transformation of entire systems of production, management and governance.

As regulators and policymakers grapple with their understanding of these changes, private actors will have a unique opportunity to influence governmental and business leadership, thereby shaping the legislative and regulatory frameworks of tomorrow. Businesses must not only embrace this disruption and evolve to survive. They must also lead and help envision and create new business models.

In the UK, Digital Economy Minister, Ed Vaizey has confirmed his intention to secure the UK as the ‘Tech Nation’, taking the global lead of the digital revolution. As one of the most developed digital economies in the world, UK plc is boosted by around £145 billion a year from digital technology. To build on that base, Vaizey is asking for ideas from the public and from industries on four key areas: unlocking digital growth; transforming government; transforming day-to-day life and building a solid foundation based on education and security (£1.9 billion is allocated to the National Cyber Security Programme over the next five years).

For insurers, operating in a way that is “synonymous with digital” means operating in a risk landscape that is shifting more rapidly. Their taking the lead in determining emerging risks and opportunities in a preemptive way is vital to reducing uncertainty and the deployment of effective risk management. Now is the time to be creative and curious in order to identify emerging risk issues and products. The insurance industry must be seen as a key stakeholder in risk.

If we are to drive innovation, access to a comprehensive knowledge bank is vital. Best practice always requires us to gather evidence whilst it is fresh and then to make informed decisions about risk. The aim of this 'taster report' is to begin to explore technological change through seven emerging issues. Going forward, we will be providing in-depth analyses of individual emerging risks on a regular basis in order to help equip insurers to measure potential harm and respond to the demand for an emerging risk market.

Technological change is, of course, only one of the key drivers of the changing risk landscape. There are others: new economic, socio-political and environmental developments, together with the growing interdependencies between them, which cause an even greater need for risk transfer.

The authors of this report are all leaders in their fields. We welcome all your suggestions as to the risks you would like us to consider in detail.

Nick Thomas
Senior Partner, Kennedys

> "For insurers, operating in a way that is 'synonymous with digital' means operating in a risk landscape that is shifting more rapidly."

Contents

Cyber business interruption:
when connections fail

The issue explained

Business Interruption (BI), including supply chain disruption, is consistently ranked as one of the top perils in risk surveys. The value of BI claims is increasing and is said to be accounting for a much higher proportion of the overall loss in a claim than a decade ago.

A key driver for increasing BI risk is that companies, through advances in the use of technology and globalisation, now operate in a complex web of inter-connectivity and interdependencies. Whilst natural disasters such as flooding and tsunamis have disrupted supply chains around the world, cyber risks and technology pose an even greater threat to the business continuity of companies. It is well established that the failure of plant or equipment due to a computer hardware or software problem, or the malicious activities of a cyber hacker, can be just as disruptive to business operations or manufacturing as a fire or flood.

If the risks of cyber-attacks or the effect of computer hardware or software failures are well known, why then should cyber risks be seen as an emerging threat to business operations?

The emerging threat is in the form of cyber outsourcing. It brings with it the significant risks of cyber supply chain disruption. It is an indisputable fact that companies are relying more on computers and the internet to conduct their day to day business operations. However, whilst companies are embracing the use of computers and the internet they are increasingly doing so by relying on third parties. This is evidenced in the trend and significant growth in the outsourcing of data handling, software services, website hosting and processing to third party cyber providers.

Key concerns

With companies giving control of their computing needs to third party cyber providers, their business continuity often depends on the continuity of that third party provider. Many companies are, it seems, more focused on the benefits of outsourcing their cyber needs than on the risks and financial loss exposures that can arise from such form of outsourcing.

Many companies are also inter-dependent within a cyber supply chain. This is a significant and developing area of risk, particularly when a part of that chain breaks down. The risk is further compounded by the insufficient assessments of cyber security practices of those to whom cyber functions have been outsourced.

Third party providers are also a particularly attractive attack target for cyber hackers and cyber criminals because services and data is most often stored for many different users on a single system. Cyber attackers are targeting those entities that store vast amounts of data or who are key online software providers. They are constantly developing new ways to hack into data storage systems. Indeed, the cyber hacking onslaught is relentless and alarmingly has a successful track record.

Why do insurers need to know about it: risks and opportunities

Companies are increasingly relying on third parties to provide, maintain and control their data and computing resources. The rapid surge in growth in cyber outsourcing to third party providers, particularly in relation to cloud computing, is predicted to redefine the IT landscape and the way companies around the world do business. For instance, in 2015 the global cloud market is said to have grown to £77 billion, an increase from £24 billion in 2011. Latest figures in the UK show that 78% of UK organisations are using at least one cloud-based service.

What happens when the third party provider suffers a cyber attack, outage or data loss? This could cause significant disruption and financial loss to a company whose computing needs are entirely or substantially reliant on a third party provider, many of whom disclaim all liability for financial losses arising. The question is who pays, and to what extent might those losses be covered, if at all, by insurance?

With the rapid growth of cyber outsourcing, insurers need to move beyond traditional first and third party cover that do not deal with the unique risks that arise from cyber outsourcing. The particular challenges in developing bespoke covers for cyber outsourcing include the complexity of understanding the exposures of the third party to whom cyber services might be outsourced. What happens when that third party refuses, for instance, to have its IT security systems vetted or to provide details of its data recovery systems and back-up facilities, which it might consider sensitive commercial information?

Legislative framework

Companies are collecting more data than ever before. Where the cyber outsourcing involves the processing of personal data certain legal obligations arise.

In data protection jargon the outsourcing company is the 'data controller' and the third party processing data is the 'data processor'. However, data controllers are legally responsible for the processing undertaken by their data processors. A data controller therefore remains liable for any breaches of data protection law that is caused by the actions or inaction of their data processor.

With data controllers remaining liable for breaches of data protection law and with large fines for non-compliance, cyber outsourcing could be a risky business for many companies. Indeed, cyber outsourcing could result in no business if there is a disruption to the cyber supply chain.

"With data controllers remaining liable for breaches of data protection law and with large fines for non-compliance, cyber outsourcing could be a risky business for many companies."

Contact

Jillian Raw
Partner
+44 20 7667 9258
jillian.raw@kennedyslaw.com

Nanotechnologies: science fact, the new revolution and the law of unintended consequences

The issue explained

Nanotechnologies involve the engineering of new processes and materials at the atomic and molecular level. One of the most widely repeated predictions for nanotechnologies was its role in creating a trillion dollar industry by 2015. The reality is that such a contribution – or the means to calculate it - is probably impossible to determine. Nevertheless, nanotechnology research is unquestionably at the heart of a scientific revolution and is expected to be a driving force for various industries seeking to industrialise technology systems.

Nanotechnologies have been around for some time. Carbon nanotubes (CNTs) were discovered in 1991. These long, thin cylinders of carbon have unusual properties, which are valuable for nanotechnology (as well as electronics, optics and materials science), exhibiting strong electron mobility and thermal conductivity. Fast forward to today and we can see CNTs integrated with graphene or nitrogen to create nanotubes that are found in flat screen televisions, long-life batteries, mobile phones, sporting equipment (tennis rackets, bicycle handlebars, skis), motor vehicle parts and tissue engineering.

Other forms of nanotechnology, nanomaterials and nanoprocesses exist in food ingredients, cosmetics, construction materials, water filtration, fuels and lubricants, pharmaceuticals and surgical implants. One of the most popular types are nanofilms - thin films that are water repellent, self-cleaning and scratch resistant – as used on eyeglasses, computer displays and cameras.

> “One of the most widely repeated predictions for nanotechnologies was its role in creating a trillion dollar industry by 2015.”

Key concerns

Speculation exists that CNTs could cause adverse health conditions similar to those seem in asbestosis (based on testing of laboratory animals). How then can insurers and businesses start to evaluate this scientific revolution into quantifiable risk and potentially apply the lessons learned from, for example, the liability catastrophe of asbestos?

Why do insurers need to know about it: risks and opportunities

With these advances in science and technology over such a short space of time, the risks associated with the manipulation of particles at the atomic and molecular levels remain disturbingly unquantifiable. Participants in supply chains might not be aware of nanoparticle inclusion in processes and products. Knowledge by end-users (in particular, private consumers of retail products) is currently limited.

Insurers will doubtless want to consider the risks in nanotechnologies in light of that which was learnt from exposure to asbestos liabilities. Doing so will allow them to make an informed decision about whether application of nanotechnologies ought to be excluded from covers, or whether the opportunities are so great that they should be capitalised on and managed in a way to reap the benefits.

Legal framework

This transformational process has the proven capability to generate significant business and revenue around the globe and, as such, present growth opportunities and development for the insurance industry. As insurers and businesses become increasingly global and homogenised, the regulation of the development and distribution of nanotechnologies, and whether international standards will classify and regulate nanoprocesses, will be highly relevant.

Contacts

Robert Welfare
Partner
+44 121 214 8033
robert.welfare@kennedyslaw.com

Janine Clark
Senior Associate
+44 20 7667 9361
janine.clark@kennedyslaw.com

Telemedicine:
transforming healthcare

The issue explained

NHS England is committed to making more ambitious use of technology. Digital will no longer be "on the edge of services" but instead will be "integral" to service delivery (Tracey Grainger, Head of Digital Primary Care Development at NHS England).

Telemedicine or 'instant medicine' (IM) - a means of evaluating, diagnosing and treating patients from remote locations - has the potential to revolutionise healthcare and genuinely confront some of these challenges.

IM already appears to be a success story in Leicester City Clinical Commissioning Group, where patients with lung diseases are monitored carefully via a computer in the comfort of their own home.

Health Secretary, Jeremy Hunt, has acknowledged the need to embrace technology. He believes technology will be used in areas where a proven method already exists, releasing doctors to spend more time with their patients where their judgement is essential.

Patient safety, which would include use of confidential patient information, is of vital importance to healthcare providers. Mr Hunt has highlighted that providers could learn from both the banking and retail industries following their embracing of technology.

Healthcare providers have the opportunity to seize on the role of technology in an attempt to transform healthcare. However, utilisation remains a challenge and serious thought and planning is required to mitigate the associated risks. Understanding those risks now is vital to allow healthcare providers to preemptively prevent and protect themselves from related liability claims.

In particular, IM cannot replace the importance of continued communication with patients. Knowing there is a distinct correlation between poor communication and an increase in claims, IM must be implemented in an appropriate clinical context.

Key concerns

Security and privacy issues

Breach of privacy and concerns around patient confidentiality and patient data are key. Factors to consider include:

- Ensuring integrity of security arrangements around electronic records and associated data.
- Rogue employees.
- Protection from unencrypted communication platforms such as Skype or Google Talk.
- Security verification of the vendor's systems.

Reliability of technology

Failure of technology during a critical moment of a patient encounter cannot be underestimated. Factors to consider include:

- Receipt of incorrect information by the patient or clinician.
- Unclear delivery of electronic communications that leads to confusion.
- Legal responsibility for any such failure.
- Suitable cover under contract for services.

Consent

Difficulties in obtaining and evidencing informed consent will need to be overcome. Factors to consider include:

- Ensuring patients are aware of and consent to the potential benefits and risks associated with IM.
- Awareness must include delays that could result from deficiencies or failures of telecommunications equipment and the potential for security breaches.
- Resource implications for the healthcare provider.
- Provision of medical assistance from outside the UK.

Qualifications of clinicians

The clinician may not have the right medical experience or training for using the technology. However, the healthcare provider will become liable for their acts/omissions. Factors to consider include:

- Due diligence in relation to those advising via IM.
- Responsibility for the acts or omissions of employees or those acting under a contract for services.

Why do healthcare providers need to know about it: risks and opportunities

The healthcare provider will need to be fully aware of the associated risks of IM. Forming a view on where any potential liability will rest is vital and, if necessary, ensuring appropriate employers' liability cover or indemnity in any contract for services is in place.

✓ Checklist

Security and privacy issues

- Examine the latest developments in cyber/privacy insurance coverage and assess what might be needed and when.

Reliability of technology

- Seek reliable vendors with proven records of accomplishment on delivery.
- Obtain legal advice regarding negotiation of vendor responsibility in their contracts to ensure a high level of performance by vendor.
- Consider business interruption insurance to ensure nuanced policies provide coverage.

Consent

- Clinicians should discuss the benefits and risks of IM with patients before obtaining consent.
- Document proof of informed consent in the patient's record.
- Implement systems that ensure medical assistance is being provided within the UK only (at this stage).

Qualifications of clinicians

- Verify the qualifications and registration of every clinician providing medical services. This should include an individual assessment of their revalidation requirements.
- Do not rely on contractual arrangements between IM companies and their employees.
- All clinicians providing medical services to patients in the UK, whether locally or by IM, should be required to register with the General Medical Council.

Legal framework

There are multiple component parts to the legislative and regulatory environment that will need to be reviewed and kept under review as technology develops, so that healthcare innovation is managed and patient safety is preserved.

Data Protection Act 1998

- Gives individuals rights in respect of their personal information.
- Creates obligations for organisations using that information.
- Establishes penalties and an enforcement regime.
- Confirms who has to comply with the provisions of the Act (data controllers and data processors).

Article 8 Human Rights Act 1998

- The right of private and family life is one of the Convention's most open-ended human rights provisions.
- Ensures that there are positive obligations to respect private and family life.
- A failure to securely store passwords on a database could lead to a breach.

Care Quality Commission

- Monitors, inspects and regulates health and social care services.
- Maintains standards with regard to record keeping, taking of consent, management of medicine and staff training.

Nursing and Midwifery Council

- Sets professional standards of practice and behaviour for nurses and midwives.
- Provides guidance on use of social media and social networking so as to ensure public protection.
- Considers risks when confidential information is shared and comments posted.
- Protects the reputation of the profession, mindful of identity theft.

Health and Social Care Professions Council

- Has a code of conduct which sets standards for performance and ethics.
- Seeks to maintain expectations of behaviour and conduct.

General Medical Council

- 'Good medical practice' sets guidance on what is expected of all registered doctors.
- Currently considering use of social media and online behaviour when using Twitter to highlight issues concerning healthcare.
- Reviewing confidentiality guidance relevant to what information can be shared with patients' friends and families.

Contacts

Christopher Malla
Partner
+44 20 7667 9194
christopher.malla@kennedyslaw.com

Ed Glasgow
Senior Associate
+44 20 7667 9129
ed.glasgow@kennedyslaw.com

Young people and noise:
product liability claims

The issue explained

Exposure to excessive noise is a major cause of hearing disorders worldwide. It is attributed in part to occupational noise and the impact of noise induced hearing loss (NIHL) claims in the workplace is well known. The claims presented today range from exposure in the mid 1960's to the present day. Insurers' records show that claims have come from many different industries.

Outside of the workplace, it is estimated that the numbers of young people with social noise exposure has tripled to approximately 19% since the early 1980's. The increase in unit sales of personal listening devices (PLDs) is staggering. In the EU alone, sales' estimates range between 184-246 million for all portable audio devices sold between 2004 and 2008.

Key concerns

There is already evidence of widespread hearing loss amongst young people consistent with a noise-induced cause. In the US, 16% of young people have early signs of hearing loss.

Exposure to recreational music via a PLD supports the concern about an increase in hearing loss. Twenty per cent of young people in the UK are estimated to expose themselves regularly to excessive levels of loud music (often without heeding to warnings about over exposure). The use of in-ear types of audio technology are especially damaging to young people's ears as they channel and amplify the noise into the ear canal.

Perhaps unsurprisingly, studies that point to an increase in hearing loss in young people during the last 30 years coincide with a period of widespread use of PLDs. Some studies go further and warn that if young people under the age of 18 continue to use the equipment in the same way they do now, they are exposing themselves to a risk of NIHL by the time they reach their mid-twenties.

The corollary of the detrimental effect on the wider economy cannot be ignored. Making up the largest part of the UK economy, the services sector is supported by an increasing reliance of telephones (e.g. call centres). The impact of widespread hearing loss may mean, therefore, that as young people who work within that sector age, they are disadvantaged in the workplace by their disability; restricting the pool of a healthy workforce.

Why do insurers need to know about it: risks and opportunities

Manufacturers of PLDs typically provide warnings about the volume, or decibel level (dB) at the ear, and many manufacturers incorporate functions within the device to limit the noise level at the ear. However, by focussing on the volume, the overall daily dose (LEPd) of the noise is typically ignored. Prolonged use of headphones at an otherwise safe level would be the equivalent of a higher volume for a shorter time and therefore be rendered unsafe.

In addition to the public health issues noted above, excessive and harmful noise exposure in the young pose a significant claims risk to insurers. The underlying factors include:

- The ears of young people are medically more susceptible to the effects of noise exposure than older people.
- A young person's inability to read or understand the warnings given.
- Entering into a contract with a minor is voidable i.e. the minor is able to cancel any contract at any time prior to reaching 18. Attempts to limit liability for personal injury will not likely be enforceable.
- The scale of the problem may not become evident for many years due to a given "reservoir of tolerance" for NIHL. Even if hearing loss is measurable, it is not noticeable by individuals until the thresholds typically exceed an overall hearing loss of 25dB in the frequencies of 1k, 2k and 3k at which speech is recognised. This may not present itself until an individual reaches majority, or in some other way becomes aware of the condition.

> "In the EU alone, sales' estimates range between 184-246 million for all portable audio devices sold between 2004 and 2008."

Legal framework

The Consumer Protection Act 1987 (the CPA) implemented the European Product Liability Directive 85/374/EEC, creating a regime of strict liability for defective products. Under the CPA, a product is defective if: '*the safety of the product is not such as persons generally are entitled to expect, to be assessed in relation to all the circumstances.*'

The safety of the product includes appropriate information and warnings to consumers. The younger or more vulnerable the person, the more obvious the warning has to be to render the product safe. US legislation provides for comparable strict liability requirements.

The regulatory environment imposes a requirement for employers to take action at 80db. Historically, it has been possible to defend occupational NIHL claims on grounds of causation. If however a large proportion of the population has an audiometric configuration (qualifying notch or bulge) consistent with noise as a cause, such claims are likely to prove more difficult to defend in the future on grounds of causation. It would be difficult to show that PLDs, rather than workplace noise, was the cause of the NIHL.

As a precautionary step, insurers should ask their policyholders involved in audio manufacture to check the wording of the written warnings in respect of usage of PLDs both for long periods and high volumes, ensuring that warnings are clear, adequate and applicable to safe use by young people.

Should a claim follow from exposure, a claimant would, of course, need to prove that damage can be attributed to a particular device. Nevertheless, taking such a step now could limit exposure and support a defence.

Contact

John Mackenzie
Senior Associate
+44 161 829 2579
john.mackenzie@kennedyslaw.com

Toxic stress:
light emitting diodes

The issue explained

It is widely known that light has toxic potential. Scientific studies have shown that blue light, in particular, which is widely used in light emitting diodes (LEDs), can be harmful to the retina, causing 'toxic stress'.

A particular risk group is children, whose eyes have not yet fully developed, making them more vulnerable to sustaining damage.

Key concerns

Our eyes have inbuilt mechanisms to protect the retina from light induced injury. However, whilst the lens and pigment in the back of the eye provide some protection against blue light, this only lasts for a short period before the light will start to cause damage. Such damage can be irreversible.

Concerns have also been raised that blue light can affect melatonin production and has the potential to disrupt circadian sleep/wake cycles, which can also lead to adverse health effects.

Humans have always been exposed to blue light from sunlight. However, our everyday lives and hobbies are becoming increasingly 'tech dependent' and the use of LEDs has increased significantly over the last decade. LEDs are now typically used in lighting our homes and as components in everyday technology, such as smartphones, tablets and TVs - all of which are heavily used by today's youth.

Children are undoubtedly being exposed to significantly higher doses of blue light than ever before. Products containing LED components are being used from an increasingly early age and in conditions with short and direct exposure distances, such as holding a smart device close to the face and looking directly into the light source.

There is currently little evidence to suggest that product developers and manufacturers are considering the potential risks posed by blue light emitted from LEDs or that they are taking steps to minimise these risks.

Why do insurers need to know about it: risks and opportunities

As with many areas of disease litigation, there are complex issues in respect of latent effects, when an injury can be said to have occurred and relevant considerations in respect of policy triggers.

With the widespread use of LEDs, it would be difficult to prove that a particular product or device has caused injury. However, in other areas of law, the courts have found ways around such causative issues by developing tests, such as the 'material contribution' test as used for managing asbestos claims. Liability risks with regard to LEDs should not therefore be dismissed.

The progressive deterioration of the layers of phosphor used as a coating to convert blue LED light to white light is a potentially significant factor. This could significantly increase the risk from a product with its continued use over time.

Legislative framework

LEDs are subject to photobiological safety standard EN 62471. However, some experts suggest that the standards are not well suited to LED lighting systems. Indeed, due to the directional nature of LEDs, the unified glare rating (used to measure the luminance of a lamp against the background of visible luminance from a room) considers LEDs to be outside an acceptable range of distraction limits.

Component manufacturers have no control over how their products are used by the end-product manufacturer. Whilst the producer may deem a component LED safe, it may be classified differently in its end product, for example due to the addition of a lens. Manufacturers therefore need to test the safety of their end product and not simply rely on test data for a component LED.

It is likely that revised industry standards and guidelines will be required to deal specifically with LED lighting. Health and safety law in this area may also be developed to protect consumers.

Contact

Alex Riley
Senior Associate
+44 20 7667 9690
alex.riley@kennedyslaw.com

3D printing:
the farfetched reality

The issue explained

From high heels to food products, make-up to medical devices, and bionic ears to robotic insects, 3D printing is considered by some to underpin a third industrial revolution; transforming the way products are made and representing a revenue stream of approximately £4 billion by 2019.

3D printing (technically known as additive manufacturing) is the process of making three-dimensional, full colour physical objects of virtually any form or shape from a digital model design on a computer.

First, 3D scanning of an existing object or computer-aided design software is used to create a 3D digital file with specific geometry. The file is then converted into a surface tessellation file and transferred to the additive manufacturing system for building, with the geometry split into horizontal layers of varying thickness.

A number of different additive processes are used and the materials that can be printed range from metal alloys to plastics, powders, ceramics and living tissue. Prototypes can be made on demand and designs can be varied easily without the constraints of tooling and machining.

Key concerns

At present, 3D printing is used mostly in the automotive and aerospace industries and is growing in popularity with hobbyists, jewellery makers and toy designers.

Researchers have already used 3D printers in the medical arena to make splints, valves and a human ear. In April 2014, scientists revealed that they were attempting to use a 3D printer to build a human heart and predictions were made that an entire 'biofical' heart (a blend of natural and artificial) could be printed and assembled in three to five years' time.

As 3D printers are becoming widely available, almost any hobbyist or retailer can become a 'bedroom manufacturer' overnight. Accordingly, tracing a product and proving liability between the retailer/hobbyist, the manufacturer of the 3D printer and the original digital designer of the product could prove problematic.

Modelling files could be easily copied and shared on file-sharing sites. The more products are pirated, the higher the risk of defective products that could result in bodily injury and/or property damage claims. Manufacturers could, therefore, face litigation and product recalls for finished products or component products which they did not manufacture themselves.

"From high heels to food products, make-up to medical devices, and bionic ears to robotic insects, 3D printing is considered by some to underpin a third industrial revolution; transforming the way products are made and representing a revenue stream of approximately £4 billion by 2019."

Why do insurers need to know about it: risks and opportunities

The far-reaching legal implications of 3D printed products include intellectual property infringements, piracy risks, data theft, employee liability risks and multi-jurisdictional risks where 3D printed products are distributed globally.

Product liability is one of the most substantial risks, with failures including:

- Defective original product
- Defective original digital design
- Defective digital file
- Corrupted copy of a model digital file
- Defective 3D printer
- Defective printing material in 3D printer
- Human error in implementing the digital design
- Human error in using the 3D pri nter and/or materials.

Insurers will need to assess carefully at the inception or renewal stage:

- Whether there is any increase in the risk to the insured due to the manufacturing process.
- Any supply chain issues.
- The complexities of traceability, including the ability to trace the parties responsible for the defects in manufacturing and its potential impact on subrogation/recovery rights.
- The number of jurisdictions in which the insured operates and their regulators, to include discussions with each insured's product developers.
- The risks at each stage (manufacture, testing, distribution and end user).
- The risks associated with the quality of the raw materials being used and potentially new combinations of materials which have not been properly tested.

The insured should ensure it has:

- Strategies for managing the imported product risk via more traceability of designs, raw materials and components (including physical identifiers on products).
- An open dialogue with its insurer's risk manager to implement a risk management solution.
- Considered the need for product recall insurance.
- Considered the need for worldwide cover where products are sold globally.
- Mitigating actions and contingency plans in place.
- Negotiated (as vendor or buyer) disclaimers, non-liability clauses or caps to limit its liability, to provide some comfort if liability is triggered.

Legislative framework

Current product liability laws and regulations may not be suitably aligned to deal with the distribution of responsibility for unsafe/defective 3D printed products. This includes the Product Liability Directive (85/374/EEC) and the General Product Safety Directive (2001/95/EC). The framework will need be reviewed, debated and amended by policymakers as the technology develops.

Contact

Karishma Paroha
Solicitor
+44 20 7667 9163
karishma.paroha@kennedyslaw.com

Autonomous vehicles:
back to the future

'An early morning start today. I climb in to my car. "Take me in to the Peak District please". I take a seat, close the door and put on my seat belt. The car, in general terms, accepts the destination. My car sets off down the driveway but comes to an abrupt halt – some schoolchildren have just stepped out into the driveway from behind a wall. If I had been driving, I am not sure I would have avoided a collision, but my car can quite literally look around corners – albeit it is a rather nervous driver.

My car moves off again when it is safe to do so, turns right and heads towards the main road. It lumbers to a stop and the right indicator comes on. It is taking the safer but slower route, but I do not care. It starts to turn out and to the right but again comes suddenly to a halt – this time, just missing a motorbike tearing down the main road from behind parked cars. Again, I suspect I might have hit it had I been in control of the wheel.

Off we set again, down the high street and on to a roundabout where we come to a stop in traffic. Not as much traffic as a few years ago and far more marshalled and orderly as we approach the junction. I have to concede, both the inner city traffic and the pollution is a thing of the past. Public transport has also taken an upturn.

I turn to my right, notice a friend in the back of her car, and give her wave. That sudden impulse to reach for the non-existent steering wheel is less and less frequent now. I decide to get on with some work over the car's internet hub. I rarely need to work from an office anymore; I quite like working from home or driving out in to the countryside and working from the car there. Ironic that the car is now helping people not to work from the office. Who would have thought?

The next time I look up my car is making its way quickly along an A road, out to the sticks. Looking up from my work and to my left, I notice a 'classic car' has crashed into a far newer vehicle. Both vehicles are at the side of the road. The emergency services vehicles, which are also driverless, have already arrived at the scene - no doubt called by the black box in the newer vehicle. Or perhaps the classic car has been retrofitted with a black box.

I have to feel sorry for the 'classic' car driver. These days most cars on the road are both highly or fully autonomous and driverless. With 'driver error' that caused over nine out of 10 crashes expunged, death and serious injury is so rare now. It is going to be hard for the classic car driver to argue that a collision is not his fault. Worse yet, he must be paying through the teeth for his motor insurance compared to the other 'driverless' driver.

Driverless cars now have compulsory insurance, which covers not only traditional motor insurance but also product liability, professional indemnity and other insurance risks. The fault insurer pays all on a strict liability basis with this insurance and then sorts out any contribution from others later.

At first insurers provided this enhanced insurance directly or through the larger manufacturers. More recently, and perhaps inevitably, the car manufacturers are self-insuring (or similar) and offering insurance for the first three years as part of the purchase price of the car.

I say inevitable, as the car manufacturers have such an obviously strong interest in producing safe and sellable driverless vehicles, with a good record of accomplishment and which are properly insurable. They also want to corner the market on repair and maintenance of the ever-increasing list of in-car safety and artificial intelligence devices, multimedia and entertainment equipment. They have such lucrative commercial relationships with the big multimedia corporations – if they are not one and the same.

I have a certain interest you see in cars and insurance. Five years ago, I was a motor claims manager in a larger insurer. The work, the claims and the litigation has almost completely dried up. One of those car manufacturers bought what remained of our team. I work for them now, divvying up who pays what after the infrequent road accidents and enforcing indemnities with the device manufacturers and software houses when the compulsory cover fails to bite (which is rare). The silver lining is, of course, that there are fewer lawyers needed. Thinking back to all those arguments on liability with the now defunct claimant injury firms,

it is quite bizarre arguing the toss with the other in-house legal team over which automated car might have driven incorrectly according to governance and regulatory criteria. Even stranger, if the MoJ online service arbitrates the incident, the telematics data from both vehicles are fed into government-sanctioned software.

Insurers used to lever the telematics data to adjust insurance premiums. That use is near to irrelevant now. The user of the driverless car is also next to irrelevant when underwriting the risk, as is the risk address. It is all about the record of accomplishment of the car, the quality of the safety features and autonomous systems; and the manufacturers are neck-deep in an arms war in that regard.

My car decelerates smoothly. Someone is traveling to work on a bicycle, and they should not be on the side of this A-road; bikes have their own lanes and should stick to them. My car really hates bicycles (and motorbikes) and does not know how to cope with them.

I put the TV on for some background noise, as it is eerily quiet in the back of my car. I really love my car, even though it looks like an ugly squashed bubble.'

Contact

Niall Edwards
Partner
+44 114 253 2041
niall.edwards@kennedyslaw.com

When will such a scenario be reality? 2030? 2040? 2050? Is this the most likely future?

Opinions differ from insurance luminary to their peer, from parliamentarian to futurologist, engineer to scientist, Lloyd's underwriter to Association of British Insurer representative; lawyer to lawyer. Just about the only aspect most people agree upon is that, at some point in the not-so-distant future, most vehicles on the open road will be driverless. It is inexorable, inevitable.

Such a proposition presents profound consequences in many areas, including how we insure against risk of loss on the road and the possible causes of action when things 'go wrong' on the road.

The need to sift through the mire of opinions and predictions to identify the likely implications of the move to driverless vehicles is ever more real. What are the true practical consequences to the motor insurance industry? What can the industry do now, and in the next few years, to inure itself and adapt to these changes?