FORUM OF INSURANCE LAWYERS

Informing Progress – Shaping the Future

FOIL UPDATE 10th October 2022

MedTech: a brave new world

This FOIL event took place on 22nd September 2022 and was hosted by the FOIL Product Liability and Technology & Cyber Liabilities SFTs.

Richard Sage (RS) – Crown Office Chambers

The rapid pace of scientific change means that products which would once have been the subject of science fiction are soon becoming features of everyday life, for example, the driverless car. A more common example is the 'smart' lighting and heating control in the home, operated remotely by I-phone. This has implications for product liability.

This talk looks at the relevance of this to the sphere of medical devices, as these are the most likely to give rise to product liability claims, as these are more likely to cause injury and damage. Technological advancements have included diagnostic programmes, implantable devices, equipment trackers, medication dispensing, smart health devices and virtual wards.

Implanted devices will increasingly be used by the medical profession as an aid to diagnostics, worn not in the hospital but at home. Whilst pharmacists remain at the centre of dispensing medication, setting and adjusting the dosages may increasingly be dis-planted by technology. This will allow for real-time, day-to-day monitoring of the medication someone needs.

IN BRIEF

Three expert speakers looked at the law relating to product liability claims in the context of technological advancements and in particular computer programmes, software and artificial intelligence in the field of medical devices.

What could possibly go wrong? The software might fail or have a glitch or a bug in it: instead of being prescribed the correct amount of medicine, the wrong amount is prescribed; instead of being diagnosed with the correct illness, one is diagnosed with having no illness. These are mistakes made by machines and the mistakes may be the fault of programmers, who are just as fallible as doctors.

How does the law deal with this sort of issue?

If a product malfunctions and injures someone, the product is likely to be an unsafe product and a remedy may be sought under the Consumer Protection Act (CPA).

Contractual claims for defective products

This is not primarily the route to a remedy for personal injury claims but contractual claims are still relevant. There may be a contractual relationship with a medical provider, allowing for a claim for breach of contract, if the product is defective. There will have been a breach of the implied term that the device will be of satisfactory quality and reasonable fit for purpose.

SE Wood v Days Health Care (2016) EWHC 1079

The NHS had provided the claimant with a motorised wheelchair, free of charge and so there was no contract. The claimant then paid the NHS Trust an additional £500 for an add-on unit. Here there was a contract. The add-on unit failed and the claimant brought a claim for breach of contract (breach of the implied terms under the Sale of Goods Act 1979 (SGA)) and the claim succeeded on an application for summary judgment.

Metal-on-metal defective hip claims have been brought against the manufacturers under the CPA. In the background are numerous other claims against various bodies, including surgeons, who had provided those products. If the hips are found to be defective, there will therefore be claims either for breach of contract or under the CPA (strict liability).

The problem lies in the treatment of digital content under the SGA, which applies to contracts for the *transfer to another [of] the property in goods.* The law has never fully accepted the idea that software/programmes can be a product. The law thinks about tangible products, whereas a computer programme is not tangible.

One of the early cases grappling with this issue was *St Albans DC v International Computers Limited (1996) 4 ALL ER 481 (CA).*

The claimant had bought a computer system and some programming to work out what was the level of community charge it needed to set for the residents in its area. The defendant's representative then installed the programme on the computer system the claimant had purchased. The amount of the charges was miscalculated as a consequence of a glitch in the programme and the claimant made a financial loss.

The Court of Appeal considered what was a product and found that a computer programme was not a product. The court drew the following distinction. If a disc is bought with a computer programme on it, that is a product. However, if a computer is bought without a programme on it and someone later comes along and installs the programme, that is not a product. The computer is a product but the programme is not: it is effectively a service provided by someone.

This case illustrates why increasingly in the future there will be situations where a product is bought but software is downloaded onto it at a later stage but the SGA will not be fit for purpose. The

government acknowledged this deficiency, leading to one of the provisions in the Consumer Rights Act 2015 (CRA). In Chapter 3 there are new provisions relating to digital content. These are intended to circumvent the arcane distinction between goods and services. The implied terms will apply to a *contract for a trader to supply digital content to a consumer* (S33 CRA). The Act will therefore apply to any consumer who buys a programme to download (they are buying digital content). The Act creates the implied term:

Every contract to supply digital content is to be treated as including a term that the quality of the digital content is satisfactory [S34(1)).

When considering whether it is of satisfactory quality, one aspect is *safety* [S34(3)].

Safety is itself a concept in which the courts are prepared to show a level of sophistication. The courts have accepted that medical products which may bring benefit to many may cause adverse side-effects for a minority. Such a product would not necessarily be a defective product. However, where software contains a glitch, can there be any doubt that it is defective? Probably not, but it is a fact sensitive question. For example, the problem may not be with the software but with the product onto which it has been installed. The CRA at least provides a single defendant, the supplier, where there is a contract, irrespective of whether it was supplied with the product or downloaded later.

Software is often updated. The CRA caters for this to an extent by providing that the digital content must be of satisfactory quality and fit for purpose after update [S40(1)]. However, it also provides that limitation runs from initial provision and not from update. This creates a problem in a contractual claim if the defective update is supplied more than six years after initial supply. This would leave a claimant exploring possible claims in tort or under the CPA.

All of this throws-up a number of issues. First, are providers of med-tech insured for strict liability in contract? A piece of software may have been downloaded across multiple hospitals/by numerous doctors. This could lead to multiple and/or high value claims

Secondly, contractual claims often see contribution claims, as the contractual liability passes up the chain to the ultimate manufacturer. The difficulty that may arise here is as follows: the claim between the consumer and the supplier will be under the CRA and the warranties of quality will be imposed on the supplier. When the supplier seeks to pass on that liability up the chain to whoever supplied it to them, that will not be subject to the CRA. It will not be subject to the same warranties of quality. The supplier seeking indemnity may be faced with the argument that this was not a supply of goods and thus need to show that the supply to them was of software developed without reasonable skill and care, i.e., that the software was programmed in a negligent way. Defendants may therefore find it much harder to pass on their liability to third parties up the contractual chain.

Emma Corkhill (EC) – 39 Essex Chambers

<u>The Consumer Protection Act 1987</u>

The CPA provides for strict liability if a product is defective and is helpful in both contractual and non-contractual claims. It removes the need to prove negligence, if the product is shown to be defective.

There is no need for a contract. A claimant can sue the producer, importer and in some circumstances the supplier of a product. But what under the CPA is a product? It applies to *any good or electricity* and this has not been updated for digital content. There are various explanations within the Act as to its application and who can be sued as a producer. Producer includes the person who manufactured the substance or won or abstracted it, or where essential characteristics of the product are attributable to industrial or other process. But again, the Act anticipated tangible products.

How does med-tech fit into the CPA, where the software and data aspects create the biggest issue? This difficulty is highlighted by the comments of the judge in *The Software Incubator Limited v Computer Associates U) Limited (2016) EWHC 1587 (QB)* where it was said: '*case law dealing with the status of software is scarce and limited in effect',* suggesting that the previous obiter comments of judges were wrong.

This case related to software and looked at whether the software was a product or a good. This was not considered under any of the legislation already mentioned but under the Commercial Agents Regulations 1993. There is no definition of goods under those regulations.

The High Court Judge decided software is a good, albeit not a tangible one. He took the view that digital software '*possess a functional equivalence of goods.'* This suggests that the essential characteristic cannot depend on the mode of delivery these days. There is no longer a need for a disc or a USB stick in a physical form, when there are means of delivery that do not involve a physical product.

The case of *London Borough of Southwark* held that there was no sale of goods. What existed was a licence to access software and not a transfer in ownership. By analogy: is there a transfer of property in goods where you are paying a subscription to Netflix? This same applies to downloading a book or a song. Netflix is a service; the downloaded song that is purchased is a good. The court commented, obiter, that software could be a good, but an annual licence to use something is probably a service.

In this case, the judge held that even where there were licence conditions, there was still a transfer of ownership, which differed from the annual subscription scenario. The judge was quite certain that software is a good and a product and not just a service.

The Court of Appeal disagreed and went back to the old interpretation that software supplied electronically and not on tangible medium is not a good. The Supreme Court referred the matter to the European Court of Justice, which in 2021 held that there is a sale of goods when software is supplied for a fee by electronic means with a grant of a perpetual licence (rather than an annual subscription). The ECJ found that goods were products that could be valued in money and were capable of forming the subject of commercial transactions: tangibility was irrelevant.

<u>Problems with the CPA</u>

Limitation in personal injury claims is three years but there is a 10-year limitation period under the CPA at which point the claim is *extinguished*. S33 Limitation Act does not work outside the 10-year longstop. What then about a latent defect or a software update issue? The speaker felt that as the law currently stands, the CPA would be a bar to a claim.

There are various CPA defences and it is not clear how software cases fit into these. For example, that the defect did not exist at the time the product was originally supplied but arose from an update supplied more than 10-years after that original supply.

Medical and tech knowledge are moving on rapidly and what may have been safe and reasonable product five years ago, might become outdated but that does not mean that it was 'defective' when it went to market in the first place.

In the context of med-tech it will also be necessary to consider exactly what has gone wrong with this product: the whole product or just part of it? Who supplied the defective component? Alongside what the machines are doing, doctors still have a role to play and may not be able to hide behind a statement such as '*But the tech told me this…'*

What happens if a software update goes wrong and causes an injury?

The first question is whether the patient has a contract with anybody, such as a private healthcare provider? If so, they can utilise the CRA and the terms of that contract. This raises issues of who had responsibility under that contract and what for? For example, will the supplier provide an update to software or is the onus on the patient to download updates? There could also be issues around what warnings have been given about the risks of not downloading updates (possible contributory negligence). But, the CRA does pose potential limitation issues, because of the six-year limitation period in pure software cases, although the personal injury limitation provisions would probably get around that.

With the CPA, an issue will be whether the particular software was a product provided to the claimant; or was it software used by the defendant to interpret data, in which case the claimant has no direct contract with the provider? Under the CPA they could still go after the provider of the software, if it was defective but care will need to be taken to establish exactly what has happened factually. The longstop provision under the CPA may also be relevant.

Otherwise, the claim may arise only in tort. It may be very difficult to prove negligence, in the context of a piece of software. Claims against the NHS would be in tort.

What changes could be made to improve upon this legislation?

Under the CPA, there needs to be clarity over supplying the initial product or later updates. If it is a later update, when does time start to run? Should it be a new event to set time running? But the CRA has not done that. The CPA definition of 'product' could be amended to include something like that in the CRA or the Medical Device Regulations 2002.

Limitation is another area where there could be changes, such as providing an exception to the CPA longstop in cases of personal injury.

Both the CRA and CPA could review the status of software updates.

David Hopkins (DH) – 39 Essex Chambers

Cyber risks

A definition of cyber risks: *Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It*

also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of date, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments. [CRO Forum] This definition includes personal injury.

Cyber risks and cyber security incidents are not merely an IT risk but an enterprise risk. The level of risk will vary for different enterprises. In the medical sector, cyber risk/losses may be more important than physical risk/losses (e.g., long-tail reputational loss, where the manufacturer of a defective medical device might never be trusted again).

There is widespread under insurance of cyber risks, particularly with SMEs.

Stand-alone, ideally modular/bespoke, cyber cover is a key part of commercial cyber risk management. Different activities require different cover. Med-tech companies also need to consider who will be using their devices.

Typical cyber risks include denial of service attacks, malware, ransomware, insider misuse (a rogue employee), hardware loss, especially mobile devices; data breaches, and systems failures, both internal and external (with med-tech products, the data may be stored off-site).

There have already been numerous ransomware attacks on healthcare organisations around the world, with significant increases between 2020 and 2021. These are very real and not theoretical problems, which will continue to increase in number.

Effective insurance cover against cyber risk is first party and third party. First party will cover the cost of remediation; the cost of damage to digital assets; the cost of alerting interested third parties, such as patients; ransomware payments. As far as third party liability is concerned, some non-affirmative cyber cover may go some way to meeting regulatory fines, in so far as they are insurable. There may be cover against data subject claims.

Few policies are likely to provide ‘silent cyber’ cover, e.g., under a property or professional negligence policy.

There may also be limited affirmative cover by endorsement, with low sub-limits, which in practice will probably not do enough.

Thus, affirmative stand-alone cover against cyber risk is by far the preferred option. It should be sector-specific; with modules and extensions, for example to cover systems failures, extortion payments, contractual liabilities.

The issues arising in cyber cover include:

- Claims-made issues: retroactive date, notification of circumstances, aggregation;
- Cover for loss caused by a cyber event occurring at a third party data storage;
- Policy definitions of ‘computer system’;
- Policy definitions of ‘interruption’;
- Whether any ransomware payment is subject to insurers’ prior approval;
- Exclusion of pre-existing problems (‘anything likely to give rise to a claim’).

Q&A

There was discussion around the 'culpability of artificial intelligence' (AI). **RS** commented that the issue was often not about the AI itself but the way it is used. Any product can be misused and cause harm. More complex products have the greater potential to cause harm because they are harder to use. Inputting data into more sophisticated equipment carries a greater risk that a mistake might be made. Defendants may well say that there was nothing wrong with their product but that it was just misused. The focus of any enquiry might then be on issues around use, including instructions and safeguards against misuse.

A question was framed around a doctor being offered a decision tree by AI but choosing the wrong path out of two offered, leading to catastrophic consequences for the patient. **RS** confirmed that the patient had two potential remedies: a professional negligence claim against the doctor, if they made an error; and/or**,** if injured by the (defective) product, (and not as a result of its misuse) a claim against the manufacturer.

EC added that diagnostic systems often build up by experience, comparing the data from one case with similar fact cases it has been told about before. The manufacturers therefore stress that this is a tool to help the doctor but is not intended to replace the doctor's thought process. This may mean that the more obvious target for a claim is the doctor, or the hospital.

Q: for **DH**: any views on the proposed new duties in the Product Security & Telecommunications Infrastructure Bill?

A: DH There are provisions in the Bill relating to the requirement for any manufacturer to comply with any relevant security requirements. However, a 'relevant security requirement' has to be defined by the Secretary of State in regulations. The effectiveness of the provision will come down to how well the regulations are drafted. DH's concern is that the Bill may only be covering what manufacturers already have to do, without affecting any real change.

By way of general observation, a delegate thought that the fact that the OPSS and the EU have produced reports about AI and product safety but haven't actually come up with any firm views/proposed changes shows how challenging it is!

Q: RS may have had a Scots Law Times (SLT) case on his slide where the St Albans case appeared? As a Scottish practitioner, the delegate was interested to know if the Scottish courts have taken a different or similar approach to the definition of a product.

A: RS The name of the case was *Beta Computers (Europe) v Adobe Systems (Europe) 1996 S.L.T. 604.* The judge did take a different view from that prevailing in England at the time. He found there was ownership and not merely a licence in software that had been purchased. This divergence between Scots and English law was instrumental in the passing of the CRA in England, which also applies in Scotland.

A further general observation was that it was of concern to the wearers of remotely monitored pacemakers, that they might wear them for 50-years or more but were faced with the 10-year longstop, should there be a technical glitch.

Q: Where will claims be brought, given the globalisation (multiple domiciles) involved in data storage and hacking?

A: DH The correct forum could be a real issue. There could be a patient in the UK, using a pacemaker made and supplied from the USA, where the manufacturers were storing data in a third country. With any damage suffered in England & Wales, it may be possible to argue that England & Wales was also the correct forum (the jurisdictional gateway). **EC** also referred to the *Brownlie* decision of the Supreme Court which found that where the injury was suffered abroad but there were ongoing symptoms in England & Wales, the jurisdictional gateway was satisfied.

Q: Is UK law failing to keep pace with developments in IT and AI?

A: EC Not if case law treats software and programmes as products. The existing legislation needs to deal better with software updates and limitation. **DH** observed that software companies may be increasingly aware of the difference between goods and services, as they are increasingly offering licences by subscription as a periodical service.

Q: Does RS think that the warranty as to satisfactory quality in relation to digital content (under the CRA 2015) would encompass the need for adequate security measures (against malware etc) where the device/ digital content allows internet connectivity?

A: RS was of the view that if a med-tech product did not include adequate measures to secure it against hacking, it would not be of satisfactory quality. There do not yet appear to be any examples of this happening. **EC** commented that this might be subject to the state-of-the-art defence (the product was reasonable at the time it was put into circulation). That *might* in turn be subject to a duty to update the software.

Q: What advice would the speakers offer to insurers?

DH: Underwriters need to consider their expertise and appetite for risk: what it is they are covering. Questionnaires need to drill down into the proposer's cyber risks and cyber security, including who is responsible for data.

EC felt that there was a real need to understand tech or have access to real expertise.

RS: The short answer is for insurers to make sure they have in the necessary exclusions and ensure that they are not responsible for defects without fault, i.e., on a strict liability basis. Care must also be taken to ensure that claims can be passed back-up the food chain by including suitable warranties in contracts.

Deputy Head of FOIL's Product Liability SFT, Karishma Paroha emphasised in the closing remarks that there should always be a focus on the warnings, guidance and instructions provided to users of such products.