

Electronic persons: time for a new legal personality?

Product liability law has to get to grips with the emerging complexities of artificial intelligence, say [David Kidman & Stephen Turner](#)



IN BRIEF

▶ Smart technology, with interconnected devices speaking to each other, makes it difficult to establish liability.

In May 2017, the European Commission published the results of a public consultation on the fitness for purpose of the Product Liability Directive (enacted in the UK by the Consumer Protection Act 1987). Many questions set by the Commission related to the Directive's application to smart objects, robots and new tech. Approximately two-thirds of respondents agreed that producers of software, apps and algorithms should potentially be held liable, but that there are difficulties allocating liability in respect of products interacting with other products or services (eg smartphone malfunction due to an app) and in respect of products operating on algorithms (eg cars with parking sensors), including self-learning algorithms (AI).

Crucially, 58.33% of respondents did not agree that there should be liability exemptions for innovative products under experimentation, indicating that consumers would resist a substantial allocation of the risk of harm arising from untested technology. In a similar vein, the utilitarian notion of an autonomous vehicle sacrificing the owner in the car to save ten people on the pavement caused unease in a 2015 study (Bonneson and others) and was considered a challenge to those wishing to sell autonomous vehicles with utilitarian ethics.

Swiss Re's annual SONAR report, published in June 2017, highlighted various emerging risks, including 'Blame your robot'—emerging artificial intelligence

legislation'. It referenced the concept of a new legal personality for 'electronic persons'. At first glance, it seems far-fetched (as perhaps did 'corporate persons' 400 years ago). However, for a person injured by an autonomous vehicle who otherwise might have to sue the driver, the vehicle manufacturer, the software provider responsible for updating the algorithms and/or the data provider responsible for ensuring a live and accurate stream of safety-critical information, wouldn't an 'electronic person' be a simple focal point to sue, particularly if coupled with a strict liability regime and compulsory insurance?

We have also seen smart technology products coming into homes and businesses. The so-called 'internet of things' (IOT), with interconnected devices communicating with each other and third parties, without express user intervention, is no longer merely a futuristic vision. These include central heating controls which can be set remotely, appliances which can make a service call if a fault develops and smart security systems which can transmit CCTV images. The era of the smart fridge which detects that you are running out of milk and automatically re-orders more with your next online shop is arriving.

Opportunities & risk

IOT undoubtedly brings opportunities and new markets for manufacturers and service providers. It also brings risks, both conventional and new. With increased use of interconnected electronic devices in the home, if a fire breaks out, working out which device might be responsible becomes more challenging, particularly

if incompatible chargers are used and/or the issue arises due to miscommunication between different hardware or software producers. This links to a wider issue for smart technology manufacturers, namely the lack at present of a common platform or standard for interconnected devices. Various rival technology companies are competing in a race to roll out new technology. Whether this will make it easier for consumers and businesses to have confidence that any particular smart device will communicate with another remains to be seen. Compatibility issues pose a significant commercial risk for manufacturers, particularly in respect of devices or software that come onto the market after the manufacturer's own product, and are unlikely to be insured under standard product liability insurance. At what point does a manufacturer's obligation end in respect of providing regular updates to protect against 'new' risks that may compromise its product and cause harm?

A key emerging risk for interconnected devices and the IOT is whether smart devices will make consumers and businesses more vulnerable to cyberattacks. The recent 'WannaCry' attacks underline the importance of hardware and software being kept up to date. A key risk is whether a smart interconnected device may turn out to be the weak link in a home or business network. Establishing the cause of a security breach where hackers use a connected fridge to gain access to banking details stored on a home network will pose new challenges in allocating liability between the smart device manufacturer, router supplier, security software provider and the user.

Just as we will see traditional manufacturers address the interaction of their products with new technology, so this is being mirrored in the insurance world. Last year the Prudential Regulation Authority wrote to insurers and launched a consultation on the risks of 'silent cyber' insurance cover. This affects insurers writing conventional insurance such as product liability for a traditional manufacturer without an express exclusion for cyberattacks. Old technology risks can unexpectedly give rise to liability for new technology.

In the words of Isaac Asimov, 'today's science fiction is tomorrow's science fact', with unexpected technology and unintended consequences making this a fascinating but complex time to practise product liability law.

NLJ

David Kidman & Stephen Turner are members of FOIL's product liability sector focus team. David is a partner at DWF & Stephen is a legal director at DAC Beachcroft.