ICLG

The International Comparative Legal Guide to:

# Product Liability 2016

**14th Edition**

A practical cross-border insight into product liability work

Published by Global Legal Group, in association with CDR, with contributions from:

Addleshaw Goddard LLP
Advokatfirma Ræder DA
Ali Budiardjo, Nugroho, Reksodiputro
Allen & Gledhill LLP
Arnold & Porter (UK) LLP
Bahas, Gramatidis & Partners
Bufete Ocampo, Salcedo, Alvarez del Castillo y Ocampo, S. C.
Caspi & Co.
Clayton Utz
Crown Office Chambers
Drinker Biddle & Reath LLP
Eversheds LLP
Gianni, Origoni, Grippo, Cappelli & Partners
Gowling WLG
Herbert Smith Freehills LLP
Lee and Li, Attorneys-at-Law
Matheson
McConnell Valdés LLC
MILINERS ABOGADOS Y ASESORES TRIBUTARIOS SLP
Orrick, Herrington & Sutcliffe LLP
Pachiu & Associates
Pinheiro Neto Advogados
Seth Associates
Sidley Austin LLP
Squire Patton Boggs
Synch Advokat AB
Taylor Wessing
Tonucci & Partners

CDR Commercial Dispute Resolution

glg global legal group

global legal group

**Contributing Editors**
Ian Dodds-Smith, Arnold & Porter (UK) LLP and Michael Spencer QC, Crown Office Chambers

**Sales Director**
Florjan Osmani

**Account Directors**
Oliver Smith, Rory Smith

**Sales Support Manager**
Toni Hayward

**Senior Editor**
Rachel Williams

**Chief Operating Officer**
Dror Levy

**Group Consulting Editor**
Alan Falach

**Group Publisher**
Richard Firth

**Published by**
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

**GLG Cover Design**
F&F Studio Design

**GLG Cover Image Source**
iStockphoto

**Printed by**
Ashford Colour Press Ltd
May 2016



**ISBN** 978-1-910083-95-6
**ISSN** 1740-1887

**Strategic Partners**

MIX
Paper from responsible sources
FSC® C011748

## General Chapters:

1 **Recent Developments in European Product Liability** – Ian Dodds-Smith & Alison Brown, Arnold & Porter (UK) LLP 1

2 **Update on U.S. Product Liability Law** – Jana D. Wozniak & Daniel A. Spira, Sidley Austin LLP 7

3 **An Overview of Product Liability and Product Recall Insurance in the UK** – Anthony Dempster & Howard Watson, Herbert Smith Freehills LLP 17

4 **The Practicalities of Managing a Global Recall** – Richard Matthews & Fabian Volz, Eversheds LLP 23

5 **Horizon Scanning – The Future of Product Liability Risks** – Louisa Caswell & Mark Chesher, Addleshaw Goddard LLP 32

## Country Question and Answer Chapters:

6 **Albania** Tonucci & Partners: Artur Asllani, LL.M. & Ervin Bano 37

7 **Australia** Clayton Utz: Colin Loveday & Andrew Morrison 44

8 **Brazil** Pinheiro Neto Advogados: Sérgio Pinheiro Marçal & Laura Beatriz de Souza Morganti 53

9 **Canada** Gowling WLG: Mary M. Thomson & Nicholas Kluge 60

10 **China** Squire Patton Boggs (US) LLP: Kelly Liu & Elisa Li 68

11 **England & Wales** Arnold & Porter (UK) LLP: Ian Dodds-Smith & Alison Brown
Crown Office Chambers: Michael Spencer QC 75

12 **France** Squire Patton Boggs: Carole Sportes & Valérie Ravit 87

13 **Germany** Taylor Wessing: Henning Moelle & Philipp Behrendt 95

14 **Greece** Bahas, Gramatidis & Partners: Dimitris Emvalomenos 102

15 **Hong Kong** Squire Patton Boggs: David Goh & Bindu Janardhanan 109

16 **India** Seth Associates: Karnika Seth & Amit Seth 116

17 **Indonesia** Ali Budiardjo, Nugroho, Reksodiputro: Agus Ahadi Deradjat & Herry N. Kurniawan 124

18 **Ireland** Matheson: Tom Hayes & Michael Byrne 130

19 **Israel** Caspi & Co.: Norman Menachem Feder & Gad Ticho 141

20 **Italy** Gianni, Origoni, Grippo, Cappelli & Partners: Daniele Vecchi & Michela Turra 150

21 **Japan** Orrick, Herrington & Sutcliffe LLP: David E. Case & Shinsuke Yakura 158

22 **Mexico** Bufete Ocampo, Salcedo, Alvarez del Castillo y Ocampo, S. C.: Aldo Ocampo C. & Jesus Salcedo P. 166

23 **Norway** Advokatfirma Ræder DA: Ole André Oftebro & Kyrre W. Kielland 172

24 **Puerto Rico** McConnell Valdés LLC: Manuel Moreda-Toledo & Alejandro J. Cepeda-Díaz 179

25 **Romania** Pachiu & Associates: Remus Ene & Adelina Somoiag 185

26 **Singapore** Allen & Gledhill LLP: Dr. Stanley Lai, SC & Amanda Soon 194

27 **Spain** MILINERS ABOGADOS Y ASESORES TRIBUTARIOS SLP: Belén Arribas Sánchez 204

28 **Sweden** Synch Advokat AB: Ida Häggström & Vencel Hodák 213

29 **Taiwan** Lee and Li, Attorneys-at-Law: Patrick Marros Chu & David Tien 220

30 **USA** Drinker Biddle & Reath LLP: David B. Sudzus & Daniel B. Carroll 228

# Horizon Scanning – The Future of Product Liability Risks

Louisa Caswell

Mark Chesher

Addleshaw Goddard LLP

## Introduction

Advances in technology and the impact which they have on how we live our daily lives, how we interact and communicate with each other, and how we work are nothing new. However, the pace of technological developments, and the opportunities and risks which such innovations present, have taken many by surprise.

Driverless cars, only recently thought of as a possibility for future generations, could be on the roads in less than four years. The 'Internet of Things', also known as the "third wave of the internet", could, by various estimations, result in as many as 40–50 billion devices being connected to the internet within five years[1]. Such developments will have a profound impact on product liability law and regulations.

In this article, we consider future product liability risks and look at these in the context of the current legal and regulatory framework (principally the UK's Consumer Protection Act 1987 (CPA) which incorporates the EU's Product Liability Directive). We also explore what further legislation and regulation may be required to accommodate such technological advances.

## Driverless / Autonomous Cars

The automotive industry has been working in stages towards developing driverless cars. A truly driverless car, one that requires no manual input from the human passengers, is not predicted to be on the roads until at least the 2020s[2]. However, autonomous cars, i.e. cars which for the most part operate by themselves, but require some human input, are predicted to be prominent much sooner.

Automation in cars has been developing steadily over the years. For example, most new cars now come with advanced braking systems. There have been advances in cruise control functions, reduced emission technology, increased fuel efficiency and proximity sensors over the years. More recently, there has been a prominence in active parking assist technology, on-board cameras, and auto lane correcting technology. Many of these technologies are partially autonomous, aiding drivers and requiring their assistance at times. However, the industry has now reached a point where it is moving towards fully driverless vehicles, which can analyse the environment, and make adjustments accordingly, with minimal or no human input. This move has come about sooner than many would have predicted, due to advances in GPS mapping, radar, laser and wireless systems, all of which have contributed to making autonomous vehicles a reality.

## Benefits of Automation

One of the primary benefits which autonomous vehicles are predicted to bring is in safety. Autonomous vehicles are expected to reduce both the number of injuries and deaths, as well as the monetary costs of road accidents, by reducing those caused by human error. Computers can react much faster than humans, and are therefore better able to deal with complex rapidly developing situations on the road, and take appropriate action. Currently, it is estimated that over 90% of road traffic accidents are due to human error[3]. Autonomous vehicles are predicted to not only reduce this percentage, but also reduce the severity of accidents when they do occur[4]. Chris Urmson, director of Google's self-driving car programme has written in his blog that between the start of the programme to July 2015 there were only 11 accidents involving Google's self-driving car, and not one was caused by one of Google's vehicles[5].

There are also commercial and environmental benefits to be gained from autonomous vehicles. Being interconnected, with the facility to communicate in real time and transmit warnings, autonomous vehicles will be able to drive closer together and more efficiently, thereby saving fuel, reducing emissions and reducing congestion on the roads. This will have huge implications for the commercial freight industry. The Department of Transport is already drawing up plans for testing driverless "HGV platoons" in the UK. Such a platoon would consist of a leader vehicle with a human supervisor, and a convoy of vehicles behind being driven just metres apart from each other. The platform would communicate using a combination of WiFi, cameras and radar[6]. The Department of Transport is inviting companies to tender for taking licences from as early as April 2016.

The social benefits of autonomous vehicles will include increases in mobility for elderly and disabled people and the freeing up of space, especially in urban areas, by reducing the need for parking spaces. There will also be increases in productivity (or leisure time), as drivers' time spent driving reduces, eventually to zero.

### What is the current legal position on driverless vehicles in the UK, Europe and the US?

Currently, there are very few rules and/or regulations in the UK that cover driverless cars. The catalyst for driverless vehicles has come from the US, the first country to legislate (at state level only) on the testing of automated vehicles. However, with only four states so far having legislated, widespread automation may face difficulties. Chris Urmson of Google has called for federal intervention under the authority of the US Transport Secretary rather than leaving

legislation to individual states. Elsewhere, Germany, France and Sweden have begun considering how to accommodate the testing of driverless vehicles.

### Issues which will need to be addressed

Taking control of vehicles away from humans, and giving that control to computers will inevitably bring about questions of liability when something goes wrong and the vehicle is involved in an accident.

Initially, at least we will see the introduction of partially autonomous vehicles. With these vehicles, the driver will be able to take control if the situation requires it (for example, when exiting a motorway to drive through a built up area). Where a driver has taken control of the car, and the autonomous function of the car has been overridden, then it follows, as is the case with non-autonomous cars, that the driver alone will be liable for the accident as a result of his/her actions. Where does liability lie, however, when the partially autonomous vehicle system is active, and the driver relies on that system? Was the driver correct to expect the technology to prevent him/her having an accident, and not take any control themselves? Did the manufacturer clearly notify the driver of the limitations of the vehicle? How will liability be decided or apportioned?

In an attempt to clarify such questions of liability, at least until new laws and regulations are produced, manufacturers such as Volvo have indicated that they would accept liability for a crash involving their driverless car, if the crash was as a result of a fault in the car's design. If, however, the driver of the vehicle used the technology in a manner which it was not supposed to be used, then the driver would be liable[7]. The move by Volvo is sensible from a sales and marketing perspective as it aims to remove the uncertainty surrounding driverless vehicles, and promote their adoption. However, it is not much of a concession (under EU and English law at least) as it reflects Volvo's position under the CPA which imposes strict liability on producers whose products are found be defective and cause injury or property damage. Deciding questions of defect and/or driver liability will require evidence as to the circumstances of the accident (which developments in dash-cams and inbuilt telemetry systems will be well placed to provide) and expert evidence as to the capabilities and limitations of the vehicle hardware and the software running on it.

There remain many grey areas, including security and data privacy concerns, which are dealt with further below. As with all technology, there will be the requirement for updates to the software and operating systems as the technology evolves. Many of these updates should be available as simple downloads, which the producer automatically pushes out to all its vehicles through the internet or mobile telephone networks. However, if such updates are available and not installed in the cars, will the driver be liable for any crash as a result of the failure to install the update? One can foresee arguments that the updates are "bug fixes" and, these will be countered by manufacturers who will want to characterise them as continuous functional improvements of their products. The so-called "development risks defence" under section 4(1)(e) of the CPA may well be tested early on in such cases.

At present, cars have greater longevity than many computers, smartphones and other hi-tech devices. The final sentence of section 3(2) of the CPA states that:

> "*...nothing in this section shall require a defect to be inferred from the fact alone that the safety of a product which is supplied after that time is greater than the safety of the product in question*."

To what extent will that absolve manufacturers from having to provide updates beyond a contractually agreed period? Will obsolete models have to be continuously supported? Will owners be expected to pay for updates after a certain fixed period? How will MOT tests work on such vehicles? If certain safety features in autonomous vehicles are expected to come as standard going forward, then will a driver be penalised for driving an older vehicle, if it can be shown that any accident could have been prevented had the features been present? What effect will the costs associated with litigating these points affect the insurance premiums for people with autonomous and non-autonomous vehicles? The expected high cost of these cars (at least for the early adopters) will lead to expectations that they will last at least as long as normal cars.

It should be noted that previous advances in car safety have not necessarily required a reinvention of liability laws. Examples are seatbelts, airbags and cruise control, which have all been introduced without significant changes in the liability laws, whilst regulations have adapted to accommodate such advances. However, autonomous cars are a far more dramatic advancement than any of the examples listed above, and therefore new legislation and regulation will need to be introduced if there is to be a widespread adoption of such vehicles, which, in the new age of the 'Internet of Things', is inevitable.

## The Internet of Things

The 'Internet of Things' refers to the huge rise in the number of devices with the ability to gather data through in-built sensors, and to transmit that data over the internet. This ability to receive and transmit data means that an increasing number of seemingly normal everyday objects are connected to the internet, and is resulting in the online digitisation of our physical world[8].

Whilst a number of devices have had the ability to connect to the internet for some time now (e.g. Smart TVs), there has been an exponential growth in the number of connected devices in the last few years. Primarily, this has been as a result of two factors, the first of which is the fall in the costs of sensors used in such devices. Sensors, once costing $20–25 each, are now available at less than $0.50. This price decrease has meant that many more manufacturers have been able to incorporate such sensors into their products. The second factor behind the growth has been the widespread availability of wireless connectivity. Even when wireless connectivity is not available, advances in 3G and 4G technology have enabled devices to stay connected.

### Benefits of connectivity

The 'Internet of Things' has already had an impact on, and will continue to impact, our lives, through the benefits that it brings to a number of industries. The primary reason behind such benefits is the amount of data which the devices collate and which can be used by different industries to enhance the products and services which they provide, often free of charge, because of the inherent value of the data collected.

In the automotive industry, autonomous cars, for example, will rely on the ability to connect and communicate with each other in order to operate. It is through the 'Internet of Things' that this will be possible, and will result in the efficiency and safety improvements mentioned above.

In the healthcare sector, wearable devices allow health professionals to capture vast amounts of data, over extended time periods, and

aide with treating patients, both by reducing the time in which doctors have to spend with each patient (with the data already being available and analysed before a treatment session), and by pre-empting possible future illnesses, enabling treatment sooner. Connected pace-makers can send signals and warnings straight to health professionals, preventing possible heart attacks. Paramedics can use connected devices to send real time patient data to the emergency doctors at the hospital, reducing the time it takes to start treatment.

The manufacturing and retail sectors have benefitted hugely from the 'Internet of Things'. In the manufacturing sector, the increased connectivity has been used to build 'Smart Factories', with many functions being performed solely by computers. Sensors at each stage of the manufacturing process have the ability to sense and foresee when, for example, supplies of a component are low in stock, and automatically start a process to order more of that component in. It is easy to see the potential extension of this through retail outlets, as well as into the home, to the point that your fridge will compose a shopping list for you and let you know when your stocks are running low or your milk is approaching its use-by date. Future product recalls may be facilitated and simplified by this process working in reverse, with products from a particular batch subject to the recall being traceable to particular customers with tailored recall notices sent direct to their mobile phones (or fridges).

Components themselves, along with a vast array of other materials, are now being manufactured through 3D printing. Advances in 3D printers, and the ability to share data on products, have resulted in a vast number of specialist components being produced through such printers. Future developments might mean that replacement parts for products (or even complete products) can be downloaded over the internet and printed at home (medium-sized home 3D printers can be bought for less than £800). That will bring its own issues. Who can the consumer look to if that product or component, printed at home, turns out to be defective?

### Concerns arising from the 'Internet of Things'

As with any system connected to the internet, there are risks which come with using connected devices. For consumers, risks can be broadly split into privacy risks and security risks. For manufacturers, there may be additional risks, which we will explore below.

Privacy concerns centre on how the data collected from these devices will be used. With such an array of data transmitted from the devices leaving "breadcrumb" trails of data, there are concerns about how individual privacy will be maintained. That issue could fill another article or indeed a book, but the key issue for the purpose of this discussion is the potential malicious use of data by hackers to take control of a device or alter its software.

Any device which is connected to the internet comes with the inherent risk of being liable to hacking or manipulation. As the 'Internet of Things' develops, and more devices have the ability to exchange large volumes of data, there are far more opportunities for criminals to undertake cyber-attacks. Any incidence of a hacker launching an attack on an individual, and stealing data from their device, is unfortunate and distressing, but the loss in that instance is usually limited to a possible economic loss to that particular individual. However, if a hacker launches an attack on an autonomous car or switches on an electrical device in the home remotely and causes an accident, then it could result in far reaching consequences, including the loss of human life. Such attacks are a real threat, with hackers in the USA recently crashing a Jeep Cherokee by hacking into its computer from a distance of 10 miles away[9]. The incident resulted in Fiat Chrysler being forced to issue an update to their on-board computer system, with customers having to download and install the update into their vehicles.

The U.S Federal Trade Commission (FTC) issued a report in January 2015 highlighting potential vulnerabilities with connected devices. These included home devices, such as Smart TVs, ovens or thermostats being hacked, with the data being exploited, or the systems being remotely activated causing a fire. Another vulnerability was a particular device being attacked in order to get access to the wider network which the device was connected to, including denial-of-service attacks. Medical connected devices could also be manipulated by external forces. Hackers have the ability to access pacemakers or insulin pumps, and take control of such devices remotely. Such attacks could have serious implications for users.

## The Product Liability Impact of the 'Internet of Things'

Over the years, product liability law for physical products has been fairly well established, with manufacturers required to meet the minimum standards of quality and safety. If a product does not meet such requirements, then consumers can bring contractual or tortious claims against the manufacturers and/or sellers. With the growth of connected devices, there is going to be blurring of the lines between the world of software and physical products. It is now clearly possible for a defective software product to cause personal injury to the end user, liability for which manufacturers and producers will not, under current legislation, be able to exclude by contract.

In some respects, litigation in relation to connected devices will follow the well-trodden path of claims under the CPA. If a connected product, say a refrigerator, were to malfunction and result in a fire, the initial step would be for engineers to investigate the root cause of the fire and determine whether the refrigerator itself was responsible for causing the fire. The presence of the software embedded within the refrigerator, however, adds another layer of complexity to the investigation. Computer forensic experts will need to have the requisite knowledge to be able to analyse the software and determine whether it has played a role in causing the malfunction. It could be that upon analysis the product itself could provide evidence as to why the product malfunctioned, and if this was as a result of something which the consumer did themselves, then the manufacturer could avoid liability. It is likely that devices themselves could send error reports back to the producer, reporting on its own errors or malfunctions, as many computer programs have done for years.

The interventions of malicious third parties are another risk not usually associated with offline products. Even as security provisions improve, hackers find new ways to penetrate such provisions. The question must be raised then, what is a 'reasonable' level of security which manufacturers should embed within their connected devices? If a connected device is accessed by a hacker, will manufacturers have strict liability, despite the embedded security provisions? At some point, will consumers have to accept the risk of a cyber-attack if they choose to use connected devices? What security will be expected of a relatively low-cost, low-risk device (such as a £50 wireless printer) when there is the possibility that data obtained by hacking into that device is used to bypass the security of a much more secure, high-risk device such as an autonomous car.

For producers, under the CPA, there is arguably a new risk that emerges from the 'Internet of Things', arising from the fact that, to the extent they can or could update software on their products, they are in a position where they in effect supply parts of the products remotely, long after the physical product has left their control.

When determining whether a product is defective under section 3 of the CPA, the court is to have regard to three factors set out in section 3(2), the third of which is "the time when the product was supplied by its producer to another". When this was drafted, there was no prospect of a producer being able to change its product remotely. How will this be interpreted in the context of the Internet of Things? Similarly, if a producer provides a software update, does that mean that limitation periods and long-stop dates are reset to day zero in respect of that update (or the entire product)? Do producers also retain "control" of those products for the purposes of section 4 (1) (e) of the CPA – which provides a producer with a defence to a claim if he can show that:

> "*[T]he state of scientific and technical knowledge at the relevant time was not such that a producer of products of the same description as the product in question might be expected to have discovered the defect if it had existed in his products while they were under his control*" (emphasis added).

Similarly, if producers have the ability to monitor the status of their products, this could put them on notice of potential safety issues. While many industries would welcome this, to what extent would a producer of a connected product be under a duty to actively monitor for safety issues? Would it just be for those products deemed to be at high risk of safety issues, if so where do you draw the line? If a duty were imposed on producers to monitor, via the internet, all connected products, would that stunt innovation and force producers of low cost or low margin products to hold back from making their products capable of being connected? All these are questions that may fall to be addressed by the courts under the current regime or by parliament considering any legislation to pre-emptively update the law to deal with these developments.

## Future Thoughts

A key theme that emerges from the discussion above is the role of software and the emergence of defects in software within products as a risk to safety and physical property. From the early age of computing until relatively recently, physical damage and personal injury caused as a direct result of a bug or defect in software has been limited. The so-called "millennium bug" did not result in the apocalyptic scenes of nuclear meltdowns and planes falling out of the sky as predicted by some in the late 1990s. Incidents attributable to software resulting in death, personal injury or catastrophic damage have thankfully been few and far between and have generally been in military applications. Notable exceptions include the *Therac-25* accidents, where a fault with the software of a radiation therapy machine caused at least six patients to receive doses of radiation hundreds of times higher than normal, resulting in death or life-changing injury[10]. However, as more complex software-controlled products enter the consumer sphere, the risks will multiply.

The pace at which technology has developed over the last few years shows no sign of abating. Whilst technology companies have been developing innovative software and products for years, it is only now, with better connectivity and improvements in security, that such products are coming to the market. Products such as autonomous cars, smart household items, connected medical devices and engineering parts produced by 3D printers, in this new economic era of the 'Internet of Things', will increase efficiency, drive productivity, and enhance the way we live and work. There is no getting away from the risks and uncertainties which such products will bring, and it will be up to governments and regulators around the world to produce a framework within which the new connected products can exist. As technological advances continue, the law will have to ensure that it keeps pace and lawyers will have to be on their mettle to advise their clients on the risks they face and the rights they may have in this changing landscape.

## Endnotes

1. The Internet of Things: Evolution of Revolution – AIG report, January 2015.
2. The Pathway to Driverless Cars, Summary Report and Action Plan, February 2015.
3. "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey" – US NHTSA, February 2015.
4. http://www.inhouselawyer.co.uk/index.php/product-liability/10261-driverless-vehicles-liability-and-new-automotive-technologies.
5. https://medium.com/@chris_urmson/the-view-from-the-front-seat-of-the-google-self-driving-car-chapter-2-8d5e2990101b#.m0o4uqflk.
6. https://next.ft.com/content/c253b2b2-e76f-11e5-bc31-138df2ae9ee6.
7. http://www.bbc.co.uk/news/technology-34475031.
8. *Ibid* 1.
9. http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11754089/Hacker-remotely-crashes-Jeep-from-10-miles-away.html.
10. IEEE Computer, Vol. 26, No. 7, July 1993, pp. 18–41.

**Louisa Caswell**
Addleshaw Goddard LLP
Milton Gate, 60 Chiswell Street
London EC1Y 4AG
United Kingdom

*Tel:* *+44 20 7788 5174*
*Email:* *louisa.caswell@addleshawgoddard.com*
*URL:* *www.addleshawgoddard.com*

Louisa is a Partner with over 13 years of experience in commercial litigation, specialising in product safety and product liability.

She has advised manufacturers on claims and safety issues relating to food and drink, consumer goods, pharmaceuticals and medical devices, amongst others. Her clients include multinational companies, with a particular focus on the consumer, retail and pharmaceutical sectors. She regularly provides training on product recalls to manufacturing and retail clients.

She acts for GlaxoSmithKline in its defence of a product liability group action relating to its antidepressant Seroxat and has been involved in all stages of this high-profile and long-running litigation.

"*They are extremely strong in this area and have an enviable client list, particularly in the food and pharmaceutical sectors. Louisa Caswell has a very good team around her who are also very experienced.*" Chambers UK 2016.

**Mark Chesher**
Addleshaw Goddard LLP
Milton Gate, 60 Chiswell Street
London EC1Y 4AG
United Kingdom

*Tel:* *+44 20 7788 5146*
*Email:* *mark.chesher@addleshawgoddard.com*
*URL:* *www.addleshawgoddard.com*

Mark is a Legal Director within the Litigation Group based in London and has over 10 years of commercial litigation experience, acting for various clients including FTSE 100 companies, banks, hedge funds, private companies and high net worth individuals.

He combines broad product liability experience combined with an in-depth knowledge of the pharmaceutical industry and acts for GlaxoSmithKline in its defence of the Seroxat Litigation having been involved in the case since 2003. Mark also spent seven months on secondment to GlaxoSmithKline's product litigation team.

Mark also regularly gives advice on product safety issues to clients from a wide range of industry sectors from telecommunications to food and drink.

Mark worked as a lead associate on four of The Lawyer's "top cases of the year" (2010 to 2014) and was listed as a "Rising Star" for commercial litigation in the 2013 edition of Thomson Reuters' "Super Lawyers" (London edition).

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk