Browne Jacobson

"Silent AI": The risk of unintended consequences

31 July 2025   Joanna Wallens and Tim Johnson

Silent artificial intelligence ("silent AI"), refers to the risk posed to insurers of issuing policies that do not explicitly state whether AI risks are covered or not. This typically arises as a result of most policies having been written before the AI boom and can result in unintended and unsatisfactory outcomes for insurers and customers alike.

In the age of AI, insurers are encouraged to anticipate AI risks and ensure their wordings are explicit as to the cover they give (or not, as the case may be). AI currently lacks regulation, which could assist insurers in navigating how it is being used by its customers. There is a patchy sector-based approach to AI regulation. UK ministers have delayed proposals to regulate AI by at least a year, but a bumper bill to regulate AI and its use of copyrighted material is planned.

In recent years, the insurance industry has gone to great efforts to reduce unintended exposure caused by non-affirmative cyber cover, and to provide clarity to customers by either clearly excluding or affirmatively including cyber in insurance policies. Insurers sustained large losses due to cyber risks unintentionally being covered by non cyber policies. Lloyd's of London mandated that first party property damage policies provide clarity regarding cyber coverage by either excluding it or providing affirmative coverage. But what about silent AI? Ambiguous coverage leads to disputes and increases costs – so where are the key areas where insurers are, perhaps inadvertently, giving cover for AI risks?

What policies might be impacted

In short, given the extremely rapid rise in the use of AI across all sectors and all walks of life, to a greater or lesser extent AI risks can impact almost all insurance polices. We consider some of the key product-specific considerations below.

Motor insurance

Motor policies may be particularly at risk of silent AI risks. The Government has now brought forward pilots of self-driving taxi and bus like services, to spring 2026. It has also opened a call for evidence on the Automated Vehicles Act. Implementation of the Automated Vehicles Act remains in the second half of 2027, but the Department for Transport is accelerating ahead of that with trials and pilots. Driving innovation – 38,000 jobs on the horizon as pilots of self-driving vehicles fast-tracked according to gov.uk.

Automated vehicles rely on AI to function. Andrew Macdonald, Senior Vice President of Mobility at Uber has said *"We're ready to launch robotaxis in the UK as soon as the regulatory environment is ready for us"*.

This also intersects with product liability insurance, as if an automated vehicle makes a faulty decision leading to an accident, then the car manufacturer could face claims. For more on insurance vehicles see - Insurance and the Automated and Electric Vehicles Act 2018.

One of the most obvious ways of dealing with silent AI is to simply exclude it. However, this is unlikely to be possible with minimum legal requirements for motor insurance in the United Kingdom. Insurers will have to think carefully about the exposure faced by the increasing use of AI, and how that aligns with their underwriting appetite. Insurers will also want to think carefully about those exposures within motor policies that are not subject to compulsory regulation (such as first party property damage) and consider whether they want to build additional protections into their wordings.

Business interruption

Operational shutdowns resulting from AI malfunctions could trigger business interruption claims. As AI becomes more integrated into business operations, its potential for errors and failures could lead to significant disruptions. Businesses increasingly rely on AI for critical functions.

Complex supply chains often operate with the assistance of AI systems. A failure in one part of the system could trigger a chain reaction, affecting multiple businesses and potentially leading to significant financial losses.

Whilst most core business interruption covers are subject to a material damage proviso and would not cover interruptions caused by AI failure, the increased use of extensions within many business interruption policies could inadvertently bring AI-based risks into play.

Professional indemnity

AI is increasingly used in professional services. Professionals could face claims for incorrect advice or misinterpretation. There is a clear risk of professionals and companies over-relying on AI without appropriate governance and oversight. We have already seen a number of claims and professional disciplinary action in a number of jurisdictions as a result of professionals making significant errors as a result of failing to identify AI 'hallucinations'.

Recent examples include lawyers who have been disbarred and faced significant claims as a result of using made up cases in their submissions to court as a result of not checking their AI's output. In these situations, the claim is one for a professional error or omission, but the cause is the AI. Many professions are subject to mandated minimum terms (such as chartered accountants, lawyers and surveyors in the UK), which will limit insurers' ability to control the risk through coverage. However, insurers will want to understand the extent to which their insureds are using AI, and what guardrails they have in relation to its use.

Professional indemnity insurers should also be mindful of additional covers that are often included within their policies. For example, PI insurance often covers claims for unintentional copyright violations through the provision of professional services. In the absence of any provision stating otherwise, such extensions would likely cover claims arising from breaches that were themselves caused by AI.

Product liability

Manufacturers and suppliers of products could receive claims where AI failures during the design or manufacturing process have resulted in their product causing property damage or personal injury. AI failures and errors could also result in violations of product liability regulations, which could in turn lead to prosecutions and product recalls.

Directors and Officers ("D&O")

We have already seen a rise in claims against directors and officers alleging that they failed to oversee or mitigate the risks associated with implementing AI processes, leading to financial loss or company reputational damage.

Such claims can often be 'secondary' following a claim against the company itself (for example an errors and omissions or product liability claim). Insurers will want to consider their appetite for such claims, and ensure their policies accurately express that appetite. Where insurers do have an appetite for such risks, underwriters will want to understand what processes, procedures, systems and controls were in place when the company was making decisions as to AI implementation and procurement.

Additionally, directors and officers may make decisions where they relied on or were influenced by information generated by AI. If this information is incorrect, it could result in a claim covered under a D&O policy. D&O claims for infringement of intellectual property, defamation and improper use of personal information are also possible.

Finally, there is an increasing trend of companies being accused of overstating their AI capabilities to attract customers and investors, notably in the United States, although we have started to see such claims in the UK. These claims (referred to as AI-washing) would be covered under typical D&O policies, where made against a company officer or employee.

Employment practices liability ("EPL")

Hiring, retention and advancement processes which use AI systems could inadvertently introduce bias and result in discrimination claims against employers for unfair employment practices.

A number of AI powered tools are already in use in talent acquisition. Such tools resume scanners and video interviewing software, which evaluates and scores candidates.

Depending on how a claim is framed, if AI results in discrimination and an adverse employment decision, then absent any AI exclusions there may be cover under an EPL policy. Insureds and brokers are likely to expect this cover to ensure that companies can navigate the use of AI in employment with reduced financial risk. As AI use develops, insurers may choose to add express cover for such claims to eliminate uncertainty.

Further, AI is set to cause significant disruption to the workforce. Positions may be eliminated, job roles amended and team structures changed as a direct result of AI implementation. It seems likely that such changes will be a driver for employment practices claims.

Cyber

There are new risks for cyber insurers due to AI, including data poisoning attacks. Data poisoning is the name given to a cyber-attack where a dataset used by AI is compromised to influence or manipulate the operation of the AI. This can be done by intentionally injecting false or misleading information into the training dataset or deleting a portion of the dataset.

AI systems can rely on the collection, storage and use of a large amount of data. This is a significant risk to data privacy and security.

AI has created additional use of third parties by companies for the development of AI and its implementation. Third party providers can introduce additional vulnerabilities as they may have a different level of security measures. If a popular third party AI provider is targeted successfully, multiple companies could be impacted. There is a systemic risk across multiple insureds.

AI is increasingly being used to facilitate security breaches. Cyber attacks can use deep fake videos and voice cloning to create extremely convincing misinformation. A sophisticated impersonation involving one of M&S's external partners is said to be behind its recent £300 million cyber-attack.

Business UK

A number of risks from AI may be covered under cyber insurance. However, cyber policies were typically drafted in a pre-AI world, and as such simply do not consider AI-based attacks. For example, many policies' definition of hacker refers to a 'person', which would not include an AI hacker. This could easily result in unintended outcomes either for the insurer or the customer. It is recommended that insurers review their cyber insurance products and provide affirmative cover where needed (or exclusions) to account for AI.

Property damage

When considering AI risks, it is easy to overlook the risk of property damage caused by AI, although that risk does exist. It is likely that insureds and brokers will expect physical damage to property caused by AI to be covered under a property insurance policy.

It is notable that when addressing silent cyber, it is first party property damage policies that Lloyd's required to be addressed first, as it was felt that there was a significant risk of unintended exposures and outcomes. It follows that silent AI should also be considered in the context of such policies.

Interplay with silent cyber

As mentioned above, in recent years many policies have been updated to take account of silent cyber. In addition to malicious cyber incidents, many silent cyber clauses also addressed non-malicious incidents such as loss caused by software failure.

Those clauses were typically drafted before the recent rise in AI use, and as such were not drafted with AI in mind. However, depending upon how those clauses were drafted, some such clauses will apply to AI-based losses. For example, exclusions relating to losses caused by software failure may exclude claims arising from AI hallucinations (which can be a form of software failure). However, as such clauses were drafted in a pre-AI world, whether they accord with underwriters' current intention is likely to be entirely down to chance.

In many cases these exclusions will technically operate to exclude risks that underwriters are prepared to accept, or vice versa. When reviewing existing wordings against AI exposures and intention, careful attention should be given to silent cyber clauses.

Reinsurance

When considering AI exposures, insurers must be mindful of their reinsurance arrangements. All of the considerations above apply equally to reinsurance treaties. As with primary insurance policies, reinsurance policies and treaties were largely drafted before the emergence of AI, which means they are also likely to be silent as to AI exposures. When considering their own policy wordings and underwriting intention, insurers must consider their own reinsurance arrangements to ensure they are not inadvertently breaching their

treaties. This may involve opening a dialogue with <u>reinsurers</u> to understand their intention and potentially seek to clarify reinsurance documentation.

Recoveries

When considering insureds' use of AI, underwriters are advised to consider their recovery options. Where a loss is caused by AI, unless AI is developed in-house, in many cases insurers will want to consider their rights of recovery against the third party AI provider. However, most AI providers' standard terms are subject to extensive limitation and exclusions of liability, which can significantly impair any recovery claim.

Not only might this result in limited opportunities for insurers to recoup their recoveries, it may also impact the cover provided by the policy. Many policies contain exclusions or conditions relating to the insured restricting its recovery rights, which insureds may do inadvertently when entering into contracts with AI providers. Again, this can lead to unintended outcomes for policyholders.

As part of the underwriting process, underwriters may want to consider the contractual frameworks governing the provision of the insured's AI software, as it could materially impact insurers' ultimate exposure in the event of a claim.

Conclusion

Insurers whose wordings were drafted prior to the AI boom and without specific consideration of AI issues run the risk of facing unexpected outcomes and exposures, as do their customers. These issues are only likely to increase as time passes and the adoption of AI continues apace. Insurers are advised to review their policy wordings and specifically address AI where possible to remove any ambiguity. Some insurers may expand (or confirm existing silent) coverage by offering affirmative AI cover, whereas others will choose to remove exposure by adding specific AI exclusions.

The insurance market is developing policies to specifically address AI risks. Insurers will be evaluating the opportunities and risks of providing such policies. Examples of AI cover include:

1. Policies which insure the risk that AI performs as promised. If underperformance occurs, some policies are compensating insureds based on agreed thresholds.

2. Cover for a company's own damages, covering financial loss due to underperformance of internally developed AI systems such as business interruption or reputational damage.

3. Cover against legal liability for third party claims arising from outputs such as infringing IP or violating data privacy.

Contents

Authors

Joanna Wallens

Associate

joanna.wallens@brownejacobson.com

+44 (0)330 045 2272

Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

Related expertise

AI regulation and governance

Artificial intelligence

Cyber liability and data security insurance

Data protection and privacy

Insurance claims defence