



TECHNOLOGY PREDICTIONS 2025

CGC
DAC BEACHCROFT



For further information or enquiries, please contact:

Hans Allnutt

Partner
hallnutt@dacbeachcroft.com
+44 (0) 20 7894 6925

Charlotte Halford

Partner
chalford@dacbeachcroft.com
+44 (0) 20 7894 6492

Scan here to view our full suite
of predictions for 2025.



AVIATION

1. UK VTOLS are go!

The UK's regulatory framework for VTOLs (vertical take-off and landing aircraft) is promisingly taking shape. In September 2024, the Civil Aviation Authority (CAA) announced the establishment of two key working groups and it is now focused on introducing regulations that are in step with other regulators (principally the US and EU) but appropriate for the UK environment. In January 2024, the CAA consulted on (i) the handling rules for VTOL aircraft using battery power for propulsion and (ii) design proposals for vertiports at existing aerodromes. All this bodes well for the UK's ambitions to lead the way in this important sector of the aviation industry, while maintaining its usual high regulatory standards. As outlined in the UK's Future of Flight action plan (a Government-Industry Statement of Intent, published in March 2024), piloted eVTOL flights in the UK are identified as a key aim in 2026 "as a first step to scaled operations and a sustainable industry". The plan envisages a partnership between government, the CAA and industry to forge operational capabilities, physical infrastructure and the nurturing of associated manufacturing and technological development. As we look to the next 12 months, the UK's position of prominence in the VTOL space looks assured.

2. Old tech is still good tech

From 1 January 2025, it will be mandatory in the UK for a functioning carbon monoxide (CO) detector capable of alerting via aural and/or visual warnings to be fitted in certain piston-engine aircraft when operating with passengers. The aim is to restore "an acceptable level of safety". CO poisoning has been cited as a factor in multiple general aviation accidents globally. Under CAA Safety Directive SD-2024/001 (V2), which comes into effect from 1 January 2025, the Civil Aviation Authority (CAA) will recognise both aviation-standard and commercial, off-the-shelf CO detectors. As to the latter, there is a wide range of competitively priced, commercially available units intended for use in domestic environments. Although not specifically approved for aviation use, findings from the CAA's 12-month study suggest that these devices can function reasonably at typical recreational GA altitudes.

BERMUDA MARKET

3. The wave of biometric class actions will intensify

The growing wave of class actions in the United States related to biometric data privacy violations will continue to rise, with the state of Illinois at its forefront with its Biometric Information Privacy Act. There have already been a number of significant settlements with companies like Facebook, Google, TikTok and Meta in various states, with further actions expected. Enforcement efforts are expected to continue, particularly in California, with clarity on enforcement expected from its Supreme Court. Legal challenges over insurance coverage for biometric data privacy claims will also develop as jurisdictions interpret cover for novel actions.

CONSTRUCTION AND ENGINEERING

4. Rooftop revolution will have significant implications

Labour's plan to encourage millions of homes to be fitted with solar panels (the so-called rooftop revolution) and create more solar farms will lead to more claims. Technology is developing at pace; initial installation costs are high; not all roofs are suitable; safety and fire risks are high; and the skilled workforce is unlikely to be able to meet anticipated output. While the industry gets to grips with all of this, we predict greater risks for insurers that all stakeholders will need to consider. Construction all risks underwriters need to consider their exposure carefully and ensure wordings and premium accurately reflect the risks involved.



D&O AND FINANCIAL INSTITUTIONS

5. Financial institutions are appointing CAIOs to oversee AI initiatives and reduce the risk of consumer claims

AI has reshaped the financial services industry. It is widely used to summarise information, automate credit and loan decisions, detect and prevent fraud, drive operational efficiency and productivity, and reduce the risk of human error. But if AI learns from incomplete or imperfect data, there is a significant risk of unintended discrimination or unconscious bias, and unchecked reliance on AI could affect large data sets within a customer base and ultimately lead to claims for consumer redress. Recognising the critical importance of AI to corporate strategy and operations and the claims risk, financial institutions are increasingly appointing Chief AI Officers (CAIOs) to oversee the execution and integration of AI projects, promote ethical AI-practices, and ensure the adoption of AI aligns with corporate vision and regulatory requirements.

DATA, PRIVACY AND CYBER

6. Data processors will find themselves under increased scrutiny

Following the Information Commissioner's Office's (ICO) stated intention to issue the first fine to a processor for breach of its obligations under data protection law, processors will look to shift how they document their own compliance, including due diligence when appointing sub-processors in their supply chain. It will also result in many processors likely adopting a more robust position in contracts with controllers when negotiating liability caps for data breaches. Although the final penalty or enforcement notice has not been issued yet, the provisional decision has undoubtedly created a renewed focus and raised potential concerns for processors, reminding them of the importance of things like multi factor authentication. In the event that further fines are levied against processors in the coming year, the rationale behind these regulatory decisions will be awaited with great interest. Any fines issued to private sector or public sector controllers will provide additional understanding on whether the ICO will look to take a harsher line on processors who deliver software and services to the public sector only, or whether the ICO is adopting a wider remit of targeting processors across all sectors.

7. CrowdStrike incident will prompt system and supply chain cyber incident discussions

Representing one of the most significant global technology outages since NotPetya in 2017, the CrowdStrike incident will act as a poster child to prompt policyholders and insurers to review their policy wordings and coverage where a systemic or supply chain cyber incident has the potential to cause a massive financial impact. Coverage for non-malicious cyber events, including 'system failure' cover, is not always available or purchased by policyholders, and the CrowdStrike incident highlights its need. The CrowdStrike incident acts as a useful case study to review appropriate interruption periods, 'waiting periods' and retentions for non-physical damage BI cover, if purchased. It also prompts future discussion as to where the line is drawn between a policyholder's software and systems, and a managed services provider. Policyholder reliance on systemically important and vulnerable systems is continuing to increase beyond infrastructure and the cloud, challenging insurers to determine appropriate coverage limits and value appropriate premiums.

8. Cyber security laws will gather pace to keep up with technological developments and the evolving threat landscape

Digital threats are becoming increasingly common, more sophisticated and more impactful as society's digital transformation continues and there is an ever-increasing dependence on digital technology. As a result, cyber security laws will increase both in number and extent. At a UK level, we have already seen the Cyber Security and Resilience Bill introduced in the Labour government's first King's Speech. The Bill aims to "strengthen the UK's cyber defences [and] ensure that critical infrastructure and the digital services that companies rely on are secure" and will expand existing regulations to cover "more digital services and supply chains". In parallel, in September 2024, the UK government classified UK data centres as 'Critical National Infrastructure', a step designed to improve the security and resilience of these engines of the modern economy. Similarly, in the EU, the requirements of the revised Network and Information Systems Directive (NIS2) had to be implemented by EU members states by 17 October 2024, replacing the outdated laws implementing NIS1.



9. Privacy laws will slow the pace of AI developments

AI capabilities have developed exponentially in the past two years. In particular, advances in generative AI have resulted in this technology leaping to the top of board room opportunity and risk agenda and into the minds of the general public. However, it appears that the roll out of AI systems across organisations has slowed, in part due to complex privacy considerations. As data protection regulators continue to intervene, this trend will continue. As the privacy challenges arising from the use of AI systems crystallise and the regulatory focus increases, the Data Protection Impact Assessment will emerge as a crucial data protection tool.

10. Data breaches will remain a major concern for data controllers

Threat actors will continue to breach defences and cause loss, with the human factor remaining the weakest part of organisations' security systems. The continued search for the best balance between system security and usability will allow for continued penetration of systems. New challenges such as AI-related scams will create further risk. Although tools such as multi-factor authentication make third-party access harder, with cloud-based systems and resilient back-ups aiding recovery, none represent a panacea. In the future, we anticipate that data will simply be stolen, compared to current trends where data is often encrypted and ransomed against publication. For consumers affected by these incidents, while bank redress schemes may offer some form of remedy, they may encourage threat actors to see data theft as a victimless crime. For businesses, however, there will be no such redress.

11. Data claims will need to evolve

In the absence of a more generous approach by the courts when assessing quantum and costs, the pursuit of data breach claims on behalf of individuals will prove to be a question of financial risk for claimant representatives. Recent decisions have demonstrated the difficulty in succeeding in data breach actions where minimal distress or loss has been caused to a claimant. Alternatively, claimant representatives may look to pursue actions on behalf of numerous individuals in a class action. However, these actions are by no means a guaranteed route to success. The decision in *Farley v Paymaster* saw a significant percentage of data breach actions in a mass claim dismissed for not meeting the appropriate threshold of seriousness, and *Adams v Ministry of Defence* demonstrated the challenges of using an 'omnibus' Claim Form, where multiple claimants are added to a single claim. The Civil Procedure Rule Committee is considering this method of pursuing multiple claims, and this route may be closed off or narrowed significantly upon further guidance. Nonetheless, we still expect that claimant practitioners will explore other avenues to pursue data breach actions in response to judicial guidance and other pressures, as they have done in the past.

INSURANCE ADVISORY

12. 2025 will be a busy year for regulators, carriers and insureds as they embed operational resilience frameworks

Resilience is not just a cyber security issue, but a broader and pervasive concern for all. Many insurers with EU-regulated entities will be in-flight with technology, controls, contractual and organisational compliance activity in readiness for the EU's Digital Operational Resilience Act's (DORA) application on 17 January 2025. DORA and related regulatory activity, such as the UK's Operational Resilience rules and proposed rules regulating Critical Third Parties, reflect concerns over operational resilience risks for the insurance sector, particularly where threat vectors are technology-enabled, as many are. A feature of the new rules is their interest in the mapping of adverse resilience impacts (and firms' impact tolerances to these), and how supply chains may be vulnerable - and not just at the tier 1 level, but all the way down the sub-contractor stack. The CrowdStrike outage in July 2024, which at one point grounded the major US airlines, showed how business-critical systems can be vulnerable to cascading failures originating not from threat actors, but from tech firms.



13. AI could lead insurers into a D&I minefield

At the 10th Dive in for Diversity Festival this autumn Sir Trevor Phillips, former head of the Commission for Racial Equality, warned about the potential negative impacts of AI on diversity and inclusion. He put the market on notice that it must be alive to the dangers of drifting into this minefield unawares. As certain roles are reshaped or even eliminated by AI, it is necessary to step back and look at the relative impact on disadvantaged groups, asking whether they are disproportionately represented in those roles. Many in the sector are already concerned about the ability of AI to take over certain functions that were always carried out by junior staff and trainees and how that might impact the future talent pipeline but they must also look at how that might potentially limit access to the industry and its supporting professions, especially by people from diverse educational backgrounds. The challenge will be to create entry points for people that ensure everyone has the same opportunities. With greater scrutiny, measurement and monitoring of all aspects of diversity, businesses could quickly find themselves going backwards and publicly held to account if they do not make this a key focus of their adoption of AI.

INSURANCE WORDINGS

14. Risks of silent AI will motivate careful policy drafting

The focus on the benefits of AI for insurance companies will give way in the coming year to addressing how to manage the related risks. Policyholders and insurers will need to focus on how policies respond to developments in this area, including whether adjustments to policy wordings, affirmative endorsements or exclusions are necessary. As previously identified with cyber-related issues, the risk of 'silent AI' continues, with potential exposures contained within more traditional policies which may not specifically deal with AI risks. There is now an emerging series of products designed to address this issue, with careful drafting being applied to deal with concepts not addressed in existing wording.

INTERNATIONAL CASUALTY

15. Algorithms and addiction - Action against social media platforms will gather pace

The first bellwether trial against social media companies for addictive product design and other allegations will potentially upend traditional principles on product liability, design of digital products and corporate responsibility. The trial is part of US multi-district litigation brought on behalf of children and scheduled to take place in late 2025. The action alleges intentional creation of products with addictive engagement, driving compulsive use and algorithmic manipulation, resulting in various physical and emotional harms, including death. European regulators, rather than litigators, are challenging social media platforms with the European Commission opening formal proceedings under the Digital Services Act. While we do not expect civil claims to necessarily follow in Europe, the impact of the Representative Actions Directive may alter perceptions on pursuing these types of claims.

LEGAL INDEMNITIES

16. Increased use of AI in conveyancing will boost the purchase of 'self-issue' legal indemnity policies

Conveyancing practitioners will be offered increasingly sophisticated software to automate the due diligence required prior to the purchase of a property. These software packages will be able to identify title risks and offer to put insurance solutions on cover. As the due diligence process becomes more automated we expect to see an uptick in the purchase of these self-issue legal indemnity policies. Insurers will work with the developers of PropTech solutions to promote products designed to mitigate any risks that are identified.



MARINE, ENERGY AND TRANSPORT

17. Technology and data is key to supply chain resilience

Critical supply chains relying on marine transportation in key hubs around the world may face logistical challenges similar to those encountered at the Port of Baltimore earlier this year (when the Francis Scott Key Bridge partially collapsed after being struck by a container ship), causing major disruptions and economic ripple effects on global supply chains. Revisiting guidelines and putting into place robust emergency plans will increase the resilience of supply chains internationally and in turn prevent an increase in ocean freight container shipping rates. Data sharing and the use of AI for managing the inflow of information when redistributing the affected cargo will reduce any negative effects on global supply chains.

MEDICAL MALPRACTICE

18. The ongoing growth of AI in clinical practice will continue to raise complex legal questions

The use of AI in clinical practice will continue to grow as sophisticated systems are deployed in the healthcare setting. With this comes an increased risk of patients coming to harm as a result of failures in AI. Faithfulness hallucination is one example of a risk that was simply non-existent in the pre-AI world. Hallucination in the context of clinical note summaries in particular (whereby the AI model generates summary content that is incorrect or inaccurate when compared with the source medical notes) is one area of risk that has the potential to lead to serious consequences. Of course, understanding how an AI device has reached a decision may not be transparent (known as the 'black box problem'), and this of itself is an issue, particularly when considering where responsibility for harm might lie. Choosing then whether to pursue a claim for clinical negligence or product liability (or both) poses yet further questions for a patient that may have come to harm. For healthcare providers and insurers, there will be questions of how to respond to such claims and how blame should be apportioned.

MOTOR

19. The Automated Vehicles Act will drive a number of consultations in 2025

The Automated Vehicles Act 2024 passed into law in May. Full implementation, though, will require passing numerous regulations relating to operator licensing, marketing restrictions, information gathering, investigatory and monitoring powers, policing and adjustments to existing vehicle legislation. Many of these regulations will require consultations, starting with one on the foundational safety principles. Expect the publication of the statement of safety principles consultation in early 2025, with other consultations on regulations relating to authorisation, operator licensing and marketing restrictions to follow. Given the importance of insurers having a voice in how the UK's motor fleet and road network adapt to these new technologies, insurers should be prepared to offer detailed and considered responses to the consultations.

20. Fraud tactics will continue to evolve

We expect to see continued growth in 'exaggerated loss' frauds, across both injury and damage claims. This expansion goes hand in hand with the layering of claim related costs. There remains a small, but significant, cohort of claims companies and associated enablers who are deploying a business model concerned only with maximising cost generation, regardless of legitimacy or claimant need. Furthermore, insurance application fraud is growing significantly, explained in part by the ever increasing ease of access to software used in the creation of shallow-faked documentation, which can be created using basic photo editing platforms such as Photoshop.



21. Further digitalisation expected within the court system

Set against a backdrop of lengthening delays to bring matters to trial, the government is under pressure to reimagine the civil justice process. While digitalisation of the civil justice system will take time, expect to see an increasing emphasis in the use of alternative dispute resolution as parties seek to find quicker, lower cost, non-judicial ways to settle their claims. The system of compulsory mediation in small money claims may still be in its infancy but it is expected that the ambit of the scheme will be expanded to other categories of small claim, and potentially beyond. The work of the Civil Justice Council around Digital Pre-Action Protocols and the recent Court of Appeal decision in *Churchill v Merthyr Tydfil County Borough Council* are both suggestive of a direction of travel which promotes a trial before a judge as very much the last resort.

POLITICAL RISK, TRADE CREDIT AND POLITICAL VIOLENCE

22. AI-generated disinformation is a risk to watch

AI-generated disinformation campaigns are expected to heighten political unrest and violence globally. Incidents in 2024 serve as examples: fake stories about public officials, UK riots sparked by false social media information, and disinformation targeting French elections. As generative AI becomes more accessible and sophisticated, there is a risk of it being weaponised to push radical narratives and conspiracy theories, such as fabricated coup attempts or amplified extremist content on social media platforms. Increasing public distrust may spark widespread civil unrest, heighten geopolitical tensions, and lead to targeted political violence and terrorism.

PRODUCT SAFETY, LIABILITY AND RECALL

23. Product liability reform will become necessary in the UK

The need for product liability reform in the UK is becoming critical. As EU reforms deal with product safety and liability, it highlights the risk of UK legislation becoming inadequate to deal with technological developments. The UK Product Regulation and Metrology Bill, if passed, will represent a significant update to the product safety framework in the UK. However, the draft Bill does not address amending the current product liability regime under the Consumer Protection Act. The 2023 consultation preceding the draft Bill paid lip service to the question of updating the UK's product liability framework when compared to the updated EU Product Liability Directive, which widens liability to include software and digital processes. The need to update UK legislation to reflect technological advances such as products with non-physical elements is a pressing issue. The current absence of specific regulation in the UK for AI generally also creates a legislative gap within product liability, to be addressed sooner rather than later. Again, the lack of clarity invites unfavourable comparison with the European Union where the renewed Product Liability Directive will amend the definition of 'product' to include software, which includes AI systems. We expect steps will be taken this year, which could take a number of forms, such as a consultation with draft legislation further down the line.

24. The MHRA will pave the way with AI Airlock

AI will continue to make a significant contribution to the way healthcare is delivered in the UK in the coming year. The transformative potential of AI is discussed daily but is usually accompanied by the caveat that it must be designed, developed and deployed safely. To deal with these issues, the Medicines and Healthcare products Regulatory Agency launched its AI Airlock project to address the challenges involved in regulating AI as a medical device (AIaMD). The regulatory sandbox model is a recognised mechanism to help address novel regulatory challenges and the AI Airlock applies this to healthcare. The objective is to identify the issues posed by AIaMD and to work collaboratively to understand and mitigate any risks that are uncovered while ensuring the viability of the devices in the pilot. The findings from this partnership between government, regulators and industry will then inform future projects and feed into future UK and international AIaMD guidance. Other sectors will watch with interest.



25. Advanced Therapies will break new ground

The number of Advanced Therapy Medicinal Products (ATMPs) approved by the Medicines and Healthcare products Regulatory Agency (MHRA) is expected to rise significantly in the coming years. The MHRA has only approved an average of two ATMPs annually but the UK is leading the way with clinical trials in this area despite uncertainty remaining about how long the benefits of ATMPs might persist. The potential benefits are such that the investment is vital. ATMPs including cell and gene therapies offer hope for diseases previously considered untreatable. ATMPs are already being used to treat some rare conditions, including haemophilia and spinal muscular atrophy. In some cases, these therapies can transform people's lives with just a single treatment. Therapies now in development are aiming to address conditions that affect larger patient populations, including certain types of dementia and Parkinson's disease.

PROFESSIONAL LIABILITY: LEGAL

26. AI will remain high on the opportunity/risk spectrum

In last year's predictions, we mentioned the developing impact of AI in the legal sector and the opportunities and risks that come with it. One year on, this remains highly topical, reflected in an updated Law Society Guidance Note issued in August 2024, and a Law Society Gazette roundtable report in September 2024. The Law Society is calling for a 'balanced' approach to reflect that there are both risks and opportunities, in response to the UK Government's pro-innovation approach. The momentum is increasing and fears have been expressed about a two tier landscape, with smaller firms being unable to offer the tech-savvy solutions demanded by increasingly sophisticated clients. Technological advances are nothing new, but the use and misuse of AI will be a recurring theme for the profession over the next 5-10 years.

PROFESSIONAL LIABILITY: TECHNOLOGY

27. More problems will arise from IT updates, upgrades and fixes

With the ever increasing number of connected IT products (hardware and software – often referred to as the Internet of Things), we predict that knock on effects from updates, upgrades and fixes to one product will lead to an increasing number of complications with other products and result in claims. We have already seen from the CrowdStrike outage what real life damage such knock on effects can cause and, in our view, the real question is about "when" and not "if" such issues will rear their heads again. The likelihood of such occurrences (whether of the scale of the CrowdStrike outage or (much) smaller) brings into sharp focus the importance of properly drafted terms and conditions (and in particular their limitation of liability provisions) for all manner of IT products (including hardware with embedded upgradable firmware or its own operating software).

TRANSACTIONAL LIABILITY

28. AI-powered solutions will speed up the M&A process


M&A activity has slowed in recent years and the deals which are going through require buyers to investigate a range of factors including the impact of recent economic challenges, regulatory compliance, tax, ESG and litigation risk. AI technologies are now widely used to speed up the due diligence process and decision making. AI solutions undertake enhanced due diligence and swift reviews of large data sets, check financial crime and AML compliance, and efficiently flag inconsistencies and potential risks for further investigation by the buyer and its legal team. The adoption of AI is also freeing up manpower, allowing deal makers to focus on other aspects like negotiations and communications. Providing sensible human oversight is applied, the opportunities for using AI in the M&A process are revolutionary.





insurance.dacbeachcroft.com

dacbeachcroft.com

 Connect with us: DAC Beachcroft LLP

 Follow us: DACBeachcroft

DAC Beachcroft publications are created on a general basis for information only and do not constitute legal or other professional advice. No liability is accepted to users or third parties for the use of the contents or any errors or inaccuracies therein. Professional advice should always be obtained before applying the information to particular circumstances. For further details please go to www.dacbeachcroft.com/en/gb/about/legal-notice. Please also read our DAC Beachcroft Group privacy policy at www.dacbeachcroft.com/en/gb/about/privacy-policy. By reading this publication you accept that you have read, understood and agree to the terms of this disclaimer. The copyright in this communication is retained by DAC Beachcroft. © DAC Beachcroft 2024. Prepared November 2024.

