REPRINT

CD corporate disputes

TECHNOLOGY DISPUTES

REPRINTED FROM:

CORPORATE DISPUTES MAGAZINE

APR-JUN 2026 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

Skadden

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

www.corporatedisputesmagazine.com

MINI-ROUNDTABLE

TECHNOLOGY DISPUTES

PANEL EXPERTS

Verity Quartermain
Counsel
Norton Rose Fulbright LLP
T: +44 (0)20 7444 2003
E: verity.quartermain@nortonrosefulbright.com

Verity Quartermain is a litigation and disputes lawyer based in London. She focuses on contentious commercial and technology matters, working primarily on disputes relating to IP rights, cyber incidents, misuse of confidential information, IT projects and outsourcing arrangements. She also advises on non-contentious matters, and has a wide range of experience assisting financial services and fintech clients with regulatory investigations and commissions of inquiry.

Bijal V. Vakil
Partner
Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates
T: +1 (650) 470 4520
E: bijal.vakil@skadden.com

Bijal Vakil is a highly accomplished first-chair trial attorney who advises on contentious patent matters, copyright and trademark litigation, trade secrets disputes, complex technology transactions and cross-border deals. He represents publicly traded and venture-backed companies and has extensive experience in high-stakes intellectual property and technology litigation.

CD: How are companies navigating the enforcement of technology-related judgments across multiple jurisdictions? What strategies are proving most effective in mitigating conflicts between differing legal frameworks?

Quartermain: Technology contracts are often multijurisdictional. Companies are increasingly attempting to mitigate conflicts between differing legal frameworks and address enforcement issues at the drafting stage. This is being done through no longer treating the dispute resolution provisions of a contract as 'boilerplate'. Parties are purporting to agree robust dispute resolution provisions, increasingly looking to build in an expert determination step for certain issues where appropriate, or otherwise taking care to ensure that arbitration agreements agreed are valid and fit for purpose.

Vakil: Silicon Valley builds technologies that now run on a global stage, from social media and semiconductors to autonomous vehicles. Technology ignores borders, and so do the disputes that follow. High stakes intellectual property (IP) and contract battles almost never stay inside a single country, and the companies that win are the ones that treat cross-border enforcement and litigation as a single, integrated strategy. There are three core principles that drive strategy. First, design your jurisdictional architecture. Sophisticated companies intentionally place IP, affiliates and key contracts in selected jurisdictions to preserve options to sue, defend and collect meaningful remedies in multiple forums. Second, map your business to your rivals. Know where competitors sell, manufacture, hire talent and raise capital, then align your filings and enforcement so you can bring pressure in the markets and courts that matter most to them. Third, run a coordinated global defence. Parallel proceedings are now standard in major tech disputes, so you need consistent positions, evidence and messaging across all cases to avoid self-inflicted conflicts and to maximise leverage on a global level.

CD: With artificial intelligence (AI) and quantum computing blurring traditional intellectual property (IP) boundaries, what approaches are being adopted to define ownership of algorithms, training data and AI-generated outputs? Where do you see the biggest gaps in current legislation?

Vakil: Artificial intelligence (AI) and quantum are colliding with IP rules that assumed human creators and tidy, standalone inventions. In response, leading companies are shifting to a layered view of IP that separates algorithms, data and outputs,

and treats that structure as both a challenge and an opportunity. On algorithms, the legal toolkit still looks familiar: trade secrets, tight contracts and selective patents on real technical advances. But the real moat now comes from proprietary tuning, deployment scale and how deeply models are wired into products and workflows. Training data has become its own high stakes asset class. Ownership and risk are being pieced together through licences, representations and warranties, and indemnities, which is why 'clean' data pipelines are suddenly board-level issues, not just an engineering concern. AI-generated outputs are still a grey area. Different jurisdictions draw the line on human authorship in different places, so companies are quietly shifting risk into their contracts and usage terms while they wait for the law to catch up. The biggest gaps in the statutes are clear: who really counts as an author or inventor with AI in the loop, what 'lawful' large scale data ingestion looks like, and how to enforce rights in algorithmically generated content across borders. That uncertainty is exactly why now is the right time to build AI governance policies and structures that can stand up to scrutiny later.

Quartermain: In the context of copyright ownership questions, in the UK AI is likely to continue to be approached from a software perspective. There is a slight gap in the ownership of outputs in the absence of definitive guidance – AI systems are currently viewed as a tool and so the ownership of outputs will be with whoever 'made the necessary arrangements' to create outputs, but it is untested whether that is a user – which is probably what most analysis leans to – or a developer of the system. Sophisticated parties would benefit from clearly setting out the ownership position in their contracts. Algorithms themselves will continue to be protected through copyright, confidentiality arrangements or in light of the Supreme Court's *Emotional Perception* decision, through patents where granted. In terms of gaps, the main one seems to relate to training data. All cases in the UK have grappled with the potential copyright infringement by the use of unlicensed training data. The UK and some other countries specifically permit text and data mining for research purposes, but in the UK this exemption is currently under review after a public consultation. Most respondents voted in favour of stronger licensing requirements and increased protection for copyright holders. However, we will have to wait until at least Q2 2026 to see how the government approaches this, given the UK's desire to foster innovation and overall favouring of AI development.

CD: As regulatory regimes like the EU's General Data Protection Regulation and China's Personal Information Protection Law tighten, how are organisations

balancing compliance with operational agility? What trends are you seeing in multiparty disputes following major data breaches or ransomware attacks?

Quartermain: On the data breach side, while we are seeing an increase in complaints being made by individuals following incidents, we are yet to see a real increase in multiparty group litigation. This may be due to issues associated with demonstrating loss and damage and also because of the global nature of large incidents. Personal data claims to one side, with major data breaches or ransomware attacks impacting business operations of not only the victim of the incident but their customers and others in the supply chain, we are increasingly seeing claims being made for system downtime, workarounds and downstream exposure. As claims for these types of losses can take time to crystalise and be difficult to evidence, we are increasingly seeing companies consider whether there are ways to estimate these losses and contract for them at the outset through liquidated damages clauses or the like.

Vakil: Strict privacy regimes in the European Union (EU) and China do not just affect local companies, they effectively set the default for anyone shipping a single global product. The winners are the teams that can move fast while still staying on the right side of EU, China and US enforcement, using flexible, modular architectures that can absorb new rules as they emerge. When something goes wrong, speed and transparency around a breach do more to contain legal and reputational fallout than any press release drafted weeks later. The real action is usually at the weakest link in the digital supply chain, which is why companies are tightening vendor due diligence and rewriting contracts to spell out shared security and privacy responsibilities up front.

> **"Tackling bias in AI is tough because models are only as fair as the data and design choices behind them, and historical inequities tend to leak straight into the maths."**
>
> *Bijal V. Vaki,*
> *Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates*

CD: Given the growing scrutiny of social media and marketplace platforms, how do you expect intermediary liability and safe harbour protections to evolve? What impact will this have on dispute resolution strategies?

Vakil: Intermediary liability rules were built for a much more static internet, but today's platforms actively curate and amplify what people see, which changes how users value and spread content. Safe harbour protections probably are not going away, but rising anxiety about AI making decisions for us is driving calls for more proactive monitoring, clearer transparency reporting and real accountability. On the disputes side, companies should expect to be judged on their good faith efforts to reduce harm even before regulation catches up. The fight will be less about whether certain content was on the platform and more about whether the platform acted reasonably, consistently and quickly in response. Internal logs and records of algorithmic decisions are likely to move to centre stage as the key evidence in these cases.

Quartermain: In the EU, the safe harbour provisions have already been disapplied for copyright-protected content for certain types of platforms, although not marketplaces, under the Digital Copyright Directive. However this applies only to specific circumstances. The overall focus in the EU is certainly on improved consumer and rightsholder protection, but this is achieved through more detailed requirements on reporting systems. There is still no requirement for proactive monitoring of all third-party content by online platforms in relation to illegal content, such as through pre-filtering. The UK has not decided to follow the same approach and has not yet given any indication that it would. Although there are not necessarily new avenues for direct action by rightsholders or consumers, the increased fines and regulatory scrutiny may give rightsholders a new lever in litigation.

> **"We have increasingly seen parties turn to adjudication and expert determination to resolve some disputes, and arbitration to resolve others."**
>
> *Verity Quartermain, Norton Rose Fulbright LLP*

CD: What practical challenges do businesses face in defending against claims of bias or discrimination in AI-driven decisions? How might emerging regulations such as the EU AI Act reshape litigation risk in this area?

Quartermain: The potential causes of action relating to bias or discrimination remain unchanged for now, as the EU AI Act does not create a new direct right of action. It is still unclear what businesses using AI should expect – litigation to date has focused mainly on large AI developers and online platforms, including attempts at class actions under the EU AI Act involving platform algorithms, and US claims relating to bias in recruitment. There is no indication of similar claims emerging in the UK. Although the AI Liability Directive did not pass, some litigants may try to seek non material damages under the Product Liability Directive for harmful AI outcomes. Because this legislation is implemented differently across EU member states, any consistent approach is likely to take time to emerge – if the strategy is attempted at all. For businesses, the greater risks stem from deploying AI systems they cannot properly assess for bias and for which suppliers often refuse to take liability. Despite clearer regulatory guidance on safeguards and governance, many suppliers exclude liability, deny being AI providers under the EU AI Act, and push responsibility onto businesses lacking the expertise to evaluate deployed AI. In future, we may see increased contractual disputes across AI supply chains, particularly around legal compliance obligations and attempts to use audit rights to obtain more system information.

Vakil: Tackling bias in AI is tough because models are only as fair as the data and design choices behind them, and historical inequities tend to leak straight into the maths. When those systems are challenged, the real test is whether you can show technical defensibility and mature governance, not just a fairness statement. That is where strong human in the loop oversight and detailed audit trails become critical, because they are what you will have to put in front of a court or regulator to prove you took this seriously. The real edge will go to teams that treat fairness testing as a continuous practice woven into their pipelines, not as a onetime certification you can check off and forget about.

CD: In high-stakes disputes over service outages or data loss, what contractual provisions – such as liability caps and indemnities – are becoming flashpoints? How can businesses better futureproof their agreements?

Quartermain: In parallel to the recovery efforts that organisations face following an incident, they are often hit with claims relating to service outages or data loss from individuals and third parties. In relation to these claims, security provisions, liability caps, indemnities, exclusion clauses and even force majeure clauses are put in the spotlight. Dealing with disputes on these issues is made more difficult and complex when the agreements are dated or not readily available. To better futureproof their agreements, businesses should have the impacts of an incident in mind, and be clear as to what customer recourse will be available and when. However, businesses should resist the temptation to be too prescriptive in their approaches and also be mindful of how their contractual obligations fit with their regulatory obligations. Standard terms should also be considered through an Unfair Contract Terms Act 1977 lens.

Vakil: High-stakes fights over outages and data loss often hinge on boilerplate provisions everyone barely looked at when the deal was signed. Companies are now trying to future-proof those agreements with tiered liability – think different caps for data protection breaches, IP infringement and ordinary service hiccups. It also means syncing contract language with what your cyber insurance covers and what your tech stack can realistically deliver. Clear definitions of security standards, incident response duties and cooperation obligations cut down on ambiguity so everyone is rowing toward the same goal – minimising risk for all parties.

CD: Do you see arbitration and tech-focused judicial tracks as the future of resolving technology disputes? What are the key advantages and limitations compared to traditional litigation, particularly in terms of confidentiality and enforceability?

Vakil: Technology disputes are getting more technical, more cross-border and more commercially sensitive, so it is no surprise that specialised arbitration and tech-focused court tracks are on the rise. Arbitration brings certain business advantages in this space: proceedings can stay confidential, which protects trade secrets and reputations, parties can pick arbitrators with genuine technical expertise, and awards are broadly enforceable across borders under conventions like New York. The trade-offs are familiar too – limited appellate review, potentially high institutional and arbitrator fees, and narrower discovery in some forums than you would get in court. Tech-focused court tracks, by contrast, offer the authority of a judge and the ability to create precedent, which can be strategically valuable when you are trying to shape industry wide standards. Most likely, the future will be hybrid: arbitration for

sensitive commercial fights, and targeted litigation when a party wants clearer, public guidance on legal principles. The main takeaways are that jurisdiction, forum, confidentiality and enforceability are no longer boilerplate – they are strategic levers that should align with the underlying business objectives from day one.

Quartermain: In the UK, there is a specialist court which deals with complex technology, construction and engineering disputes. There have been a number of large technology cases being heard in this court in recent years. However, we have increasingly seen parties turn to adjudication and expert determination to resolve some disputes, and arbitration to resolve others. These approaches, particularly adjudication and expert determination, are being looked to because of the speed at which they can resolve disputes that arise while the business relationship continues. They are also being looked at because, in addition to enforcement concerns, concerns around reputation and concerns around the confidential subject matter of the disputes themselves, parties have more control over the form of disclosure outside the courts, and the proceedings are more flexible and adaptable to new technologies. Parties also have more control over who hears the dispute – access to subject matter experts is a benefit which cannot be overlooked. CD