COMPUTERS & LAW

FemTech and the use of AI

Also in this issue:

Assessing Design Quality in IT Contracts

Emerging technologies and the climate: charting a pathway to pre-emptive oversight

The Post Office Horizon IT Scandal: How should organisations react when IT systems go wrong?

The EU AI Act Finalised

The Automated Vehicles Act - unlocking the opportunities

Plus book reviews and the latest techlaw cases

Society for Computers & Law
The leading educational charity for the tech law community
www.scl.org

SUMMER 2024

Special Deal for Trainees:

Free SCL membership for a maximum of two years

Did you know that trainee solicitors, trainee legal executives, trainee paralegals and pupil barristers are entitled to apply for **free membership** of SCL for a maximum of two years (or until you qualify - whichever comes first)?

We want to encourage you in honing your knowledge of tech law and support you at this exciting and challenging time in your career. This category of membership will include full access to the content of the website and attendance at SCL events at the members' rate.

Plus, after you've qualified, you'll be invited to become a fully-fledged professional member at a reduced cost, and you can attend your first meeting for free!

For full details please visit our website
https://www.scl.org/about/trainees or email hello@scl.org

SCL

Society for Computers & Law
The leading educational charity
for the tech law community
www.scl.org

Contents

ISSN: 0140-3249

Published by the Society for Computers and Law.
Cover design: Ken Planter, Graphic, Bristol.

Editor's Note

I write this just before I go on holiday. I'd booked the trip way before Rishi Sunak rather unexpectedly called a general election so the postal vote has, by necessity, been cast. By the time I get back, in all likelihood we will have a new government but the question is whether there will be a new mindset in Government when it comes to the regulation of technology, in particular AI?

So far, while the Labour Party's slogans are all about change, the reality is Sir Keir Starmer's overall approach to the campaign has been largely about not frightening the horses. So I am not expecting much. However, there are some pledges on AI in the Labour manifesto that indicate a change in direction, even if subtle. (At this point I should say I think it is fair to assume the result - I am not advocating an opinion either way).

Proposals in the manifesto include:

- removal of planning barriers for building new data centres,
- a National Data library collating existing research programmes,
- longer ten year budget cycles for R&D projects in higher education,
- and, possibly key, creation of a new Regulatory Innovation Office which will 'co-ordinate issues that span existing boundaries'.

As I say, hardly a call to arms but the last one does hint at a more proactive regulatory approach than has been advocated by the current administration over the past couple of years, with its relentless light touch, pro-innovation rhetoric.

The contents of this current issue perhaps give ammunition for adopting a more proactive approach. AI is the thread through several articles but look at the sectors and activities it knits together.

Automated vehicles for one: AVs are in large part AI on wheels. And technology aimed at women under the guise of FemTech is another. Then there is the impact on the climate of all those new data centres Labour hope will spring up once liberated from planning rules (though given our rich tradition of nimbyism there may be greater opposition to that policy than they are expecting). To cap it all, we have an overview of the EU AI Act which will be in force by July and is in many ways a deliberately European riposte to the more laissez-faire approach over here and over the pond in the States.

Of course it is not only AI a new administration will be forced to grapple with. Much of the implementation, and future enforcement, of the Online Safety Act is still evolving. Labour have already hinted at stiffening fines for those platforms failing to protect children properly. It also remains to be seen whether the failed data protection bill is resurrected or a revised one put in its place. Then there is the proposal set out in the Liberal Democrat manifesto suggesting a significant rise in the digital services tax. My feeling is this is a fundraising measure the new Chancellor, of whatever political persuasion, will find hard to resist and who will probably dress up any increase as a tax to pay for the harms the social media networks are often credited with.

All of which is a rather long hand way to say techlaw is set to remain headline news for years to come, regardless of who is in Government. Lucky I've got some time off now then. A bientot!

David Chaplin

Editor of Computers & Law

4 Pump Court has long been recognised both domestically and internationally as the pre-eminent set for the full breadth of technology and telecommunications disputes. 4 Pump Court are the standalone tier 1 ranked set in both Chambers & Partners and Legal 500.

- Banking
- Commercial Disputes
- Construction
- Cross Border Investment
- Energy
- Financial Services
- Fraud
- Insurance
- Intellectual Property
- International Arbitration
- Professional Negligence
- Shipping
- Sports
- Technology & Telecoms
- Transport

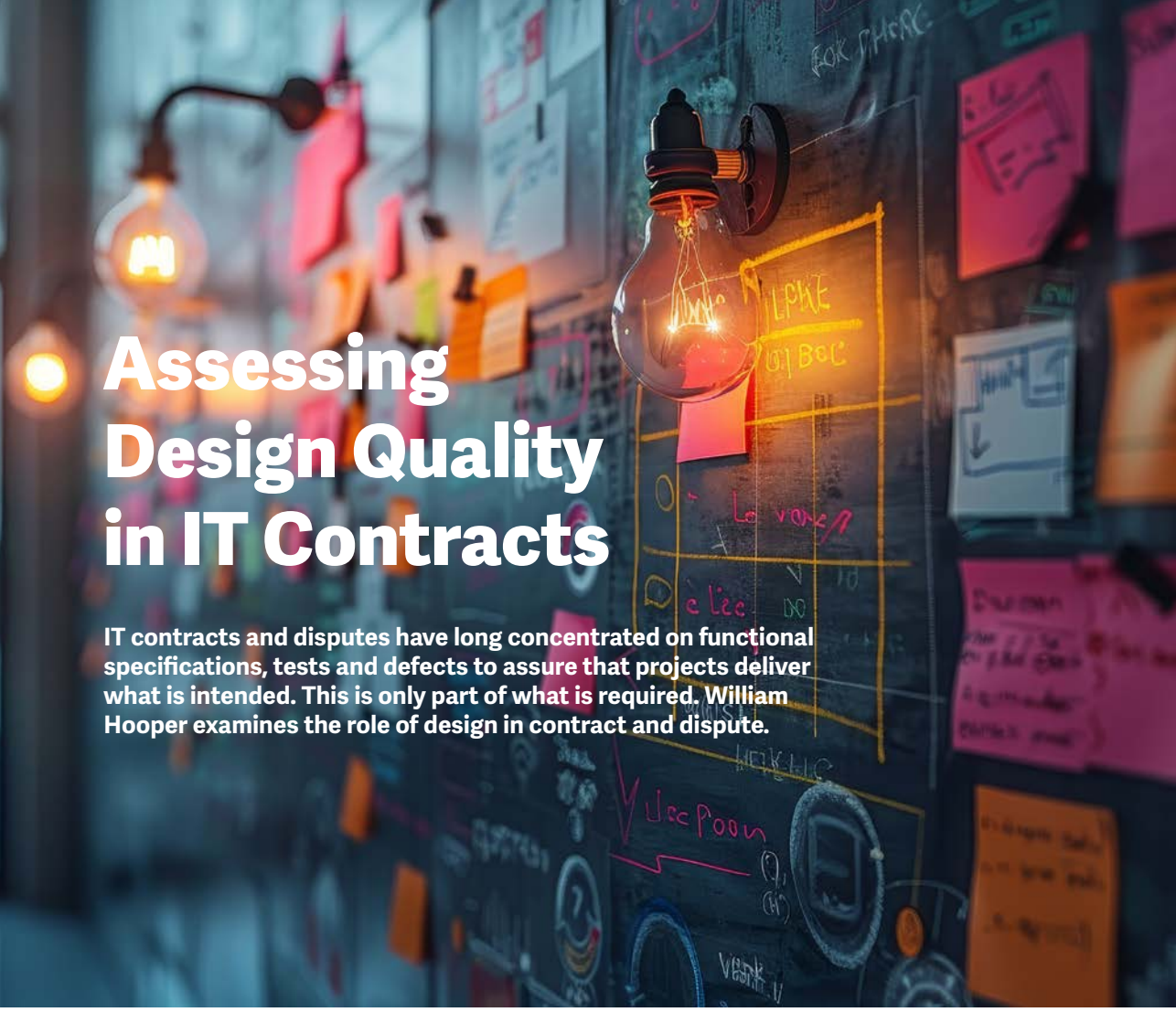
"4 Pump Court barristers, silks and juniors, continue to lead the London Bar in relation to technology, telecoms and software disputes."

"I consider 4 Pump Court to be the leading set for technology and telecoms disputes. They have expertise at all levels"

"Overall 4 Pump Court remain the go-to chambers for IT/outsourcing disputes (for example the recent Co-op and IBM case was mostly staffed with 4 Pump Court barristers on both sides)."

Pump Court

www.4pumpcourt.com | clerks@4pumpcourt.com | +44(0)207 842 5555



Assessing Design Quality in IT Contracts

IT contracts and disputes have long concentrated on functional specifications, tests and defects to assure that projects deliver what is intended. This is only part of what is required. William Hooper examines the role of design in contract and dispute.

Customers of failed IT projects frequently protest that they do not like the way the solution has been designed. "I do not like it!" is all one hears. What can a customer do when drafting a contract to insulate against the risk of this failure? How do you implement operational measures in delivery? How can an expert clarify the issues for the court?

Functions

The recent focus on design thinking has shone light on something that many knew for years: the elimination of defects alone does not make a product good. Many contracts are replete with functional requirements. I, for one, have put a lot of effort into writing them over the years. These, when done well, provide testable conditions necessary to the success of the service, for example, requiring the ability to process payments from customers. A *function* is a behaviour of the system that can be defined, delivered separately from others, and tested. If it works as expected, it is passed. If not, we call it a *defect*, and send it back to be fixed.

Many experts charged with investigating failed systems start by analysing the defects. The patterns we see in the data tell us much about what was working and what was not.

Non-functional requirements

Contracts will often also contain non-functional requirements. These refer to the performance of the system in areas such as

security, availability, response time. You will hope to see the performance levels specified in a schedule as a service level agreement (SLA). Testing should cover these too.

Your expert will look at these test results. They are not commonly at the heart of a dispute but may be seen along the way. These too may result in defects from test.

For those of us who love data and contractual certainty, functional and non-functional tests and specifications have obvious appeal.

Indignant customers

Customers in IT disputes commonly protest in colourful language, that the system is "terrible". Yes there were defects, but there is more to it. The system just works horribly. It is illogical. Users trip over even simple transactions. They hate using it and rebel. Others who have gone live find that even a minor change has so many knock-on effects that the system is close to unsupportable.

Many such complaints are expressed inarticulately. This only adds to frustrated fury. There are rarely explicit breaches that a customer can rely on other than a thin "good industry practice" clause. This is changing. Stronger contractual provisions will help to support customers in holding suppliers to account. The best suppliers strive to deliver delightful outcomes and will not resist.

Fixed price

The process of design is iterative. Good engineers and designers are expensive. A programme manager will typically separate a large endeavour into multiple work-streams. A unifying solution architect is appointed to coordinate them to assure end-to-end coherence. So as one part is designed, it rubs up against issues caused by its favoured approach in another. Steve Jobs, late of Apple, explained this beautifully.[1]

When should the design team stop refining? There is no right answer. They will typically keep going until ordered to stop or objectives have been met. It is much the same for a poet.

> *"All I can do is turn a phrase until it catches the light"*
>
> **Clive James, May Week Was In June**

If your contract is fixed price and that price is low, the product is often base metal not burnished gold. If you expect to shine, you will still want value but elegance has no fixed price and does not arrive on schedule. For most in business, this is too much. "Good enough" will rule. We still need good design to reach that standard, even if we are not in search of the artistry of the Sistine Chapel.[2]

Aspects of design

Most of us think we know good design when we see it. Apple has long competed on the fabled beauty and utility of its user experience, sustaining a premium over competitors. This justifies their high costs of development.

When thinking of design, most first think of screen design. That is the window into the system. Good design goes far deeper. Areas that should be encompassed include:

- User Experience: the totality of a user's interaction with an organisation, its services and products. The user interface and aesthetics.
- Data design: What is asked for and when. How what is known is used and structured.
- Process: The flow and sequence of operations to realise the user's and organisation's objectives.
- Architecture: The selection and arrangement of the system building-blocks to realise the system's objectives.
- Software: The internal code design and realisation in code that is easy to maintain. Or not.
- Deployment: The approach to delivering the

[1] *Steve Jobs Rock Tumbler Metaphor https://www.youtube.com/watch?v=njYciFC7mR8 (3:31)*

[2] *Michaelangelo took from July 1508 to October 1512 to paint the ceiling.*

completed, tested system to the business and users.

Design frameworks

There is a large number of frameworks that describe aspects of the approach. Some, like *Design Thinking* and *Agile*, are content-free processes. Others bring useful insight into aspects of human and technical behaviour to bring the two together. I am a particular fan of *Concepts* in software.[3] I do not advocate a customer's imposing its preferences for framework on a supplier. All good frameworks have significant overlap and suit some situations better than others.

IT architects typically seek to optimise the lifecycle cost of ownership of a system. They can invest more up-front, adding to development costs, in the hope of reducing the later costs of maintenance and support. If you prefer another objective, you should communicate that before your team gets started. You may observe that this objective is not the same as maximising sales value, customer loyalty or many other good business initiatives. Your team must be given the objectives and focus you seek.

Design in contract

Your contract will of course contain a "good industry practice" clause. If you have that, award yourself 1 out of 10 as a start.

In the dialogue that precedes appointment and contract, a customer has a golden opportunity to explore what is most important to them. Design may be on your list.

When working as a sourcing advisor, I assess the supplier's capability. Do they have an approach? What framework do they say they are using, and how do you and they assure that it is to be followed? Does it hold water? Do any of the people on this delivery team have personal experience or do the team rely on an occasional call at 2am with colleagues in Outer Mongolia? Do the skills of the named team cover all the areas you need? How will staff movement be measured, managed, reported? How will they measure design quality and report to you? You will see design change. Who manages this and how do we assign the costs? If you capture the interaction (or edited highlights reflecting your interests), you will build contractual certainty through holding the customer to the delivery method they have contracted for.

Building design integrity in

The quality of design is likely to be soft and largely intangible. You may turn some of the approach into activities that must be undertaken and link milestone achievement to their delivery. You may also consider whether some aspects are best related to the achievement of business outcomes, such as the level of customer adoption and interaction with the solution. A minority of payments may be related to the achievement of outcome targets, where you can measure them confidently.

A supplier's risk register is a useful artefact to focus the review of the proposed approach. Have they considered what are the major design decisions they must make and scheduled work to make these early? They can be very expensive to change later. Expect them to state some dependencies on the customer. Are you capable of keeping up with the supplier? If not, what are you to do about it? If a supplier has little concept of risk and size of bet, walk away now.

Design in operation

Design is all about making choices and trade-offs. These should start with principles, such as Agile's "Working software over comprehensive documentation".[4] A good set of principles supports your leadership of the endeavour and allows designers to frame choices in the context of a rationale that supports the selection of the best option from the several they have considered.

Governance is about review, scrutiny and holding people to account. Design review is a

[3] *The Essence of Software, Daniel Jackson, Princeton University Press, 2021*

[4] https://agilemanifesto.org/

sub-set of programme governance. When done properly, it centres on the ongoing critique of the design in the context of the principles. The critic must understand what is being reviewed, which is often a challenge. The reviewer is there to scrutinise, not to take over the design. That is an invisible line, frequently over-stepped to the cost of the programme. Design Thinking puts great emphasis on User Testing. User testing is an important step in the process, but many of the big bets go nowhere near the user, so those aspects are not touched by user testing. Major issues of design arise early (data structure, for example) and can be very expensive to change later. Design review is your principal assurance.

Obtaining good quality user input is vital and difficult. Many failed programmes see the uninformed loudly instructing technical experts how to design, despite their having no appreciation of the impact of design options. Managing this requires a high level of skill on behalf of the supplier's analyst and robust support from a consistent and decisive governance body.

Design in disputes

Way back in 1977, a software researcher, Edsger Dijkstra, contrasted the "correctness problem" — whether a program meets its specification — with the "pleasantness problem" — whether the specification is appropriate to the situation of use.[5] He identified the first as being susceptible to mathematical formulation and analysis. The second was unfamiliar territory for IT folk. He identified that for the result of a user's interaction with a system to be reliable, both the conformance (functional) element of the IT and the human aspect of user interaction must behave as expected. He gave both equal weighting.

Since those early days, the human aspect has been relegated. I confess that on occasion, I have joined this trend. On hearing "But I don't like it!", smiling sweetly and moving on. Sometimes I pause to ask "what is the requirement that this behaviour breaches?"

Fixing bugs is necessary but does not fix bad design. Neither does it make bad software good.

It just works

Later research and entrepreneurial investment looked at what users signed up to, such as the Zoom messaging service over lock-down. Users do not typically study the manuals for web-based apps. Gow and others noted that users infer behavioural theorems by observing their interactions with systems and come to rely on those theories.[6] If the system behaves consistently and sensibly, they stick with it. If not, they seek another that performs more reliably (if they have the choice). Gow examined user behaviour in context. This leads users to generalise from the particular behaviour they see, assuming general consistency.

This provides a test for the quality of design, that is independent of the framework used. It also points to tests beyond the user interface. Its use allows the assessor to apply measurable, objective criteria and avoid subjective judgement.

Tests of design quality

The mantra "I don't like it!" remains unsatisfactory in itself. It is uninformed, opinionated and divorced from good industry practice to which it makes no reference. It can however be used to identify instances that with investigation can overcome these challenges.

The design products

(1) Is there a design?
(2) Is the design complete?
(3) Is the design informative?
(4) Is the design consistent with the principles and itself?

---

[5] *Edsger W. Dijkstra. A position paper on software reliability (EDW 627). 1977. At https://www.cs.utexas.edu/users/EWD/transcriptions/EWD06xx/EWD627.html referred to by D. Jackson in The Essence of Software.*

[6] *Jeremy Gow, Harold Thimbleby, Paul Cairns. Misleading behaviour in interactive systems. Proceedings of the British Computer Society HCI Conference. Research Press International, 2004 https://harold.thimbleby.net/cv/files/hci04gow.pdf*

(5) Is the as-built product consistent with the design?

The design process

(1) Did the supplier identify the process they were to use?
(2) Did they adhere to the declared process, framework and principles?
(3) Was the process governed effectively and consistently?
(4) What did the contemporaneous design scrutiny reveal?
(5) What did contemporaneous user testing reveal?
(6) Were the contemporaneous design products amended appropriately in the light of comments?

In the above, the quality of investigation of design can be more insightful if it has a complete document, design, build, test set to work with. Should it fail at the first hurdle (no design), the fig leaf over modesty is likely to be blown away.

Should your contract provide rich pickings concerning the approach to be used, the above assessment can rely on the standards set within the contract. If not (as is most common), the applicable standard is "good industry practice", not perfection. My approach is to start with whatever I can find within the contract and refer as needed to whatever widely deployed frameworks I can identify, using this as a standard objectively to assess design quality. Experts must consider a range of industry practice where this exists. Practice will also change over time.

Impact and damage

Impact and damage may vary greatly from case to case. Although the complaint may start with minor cosmetic issues, the quality of design can go to the root of whether a system can be relied upon. A user who expects one form of system behaviour and is misled in acting may set off a disastrous chain of actions.

As in all disputes, it is important to establish at an early stage which of the possible issues are likely to form the basis of a successful claim, narrowing the issues appropriately. Investigation can be expensive and must be maintained at a proportional level.[7]

Conclusion

Functional and non-functional testing are still necessary. They are not sufficient in many cases. The better the contract and subsequent scrutiny of delivery, the better the probability of achieving a favourable outcome. The best of all outcomes is a product delivered successfully on schedule at the first attempt. If things do go wrong, there are objective standards to measure design quality to deliver persuasive evidence.

---

[7] https://www.scl.org/12149-managing-a-legal-dispute-arising-from-a-failed-it-project-part-1/

William Hooper

William Hooper acts as an expert witness in IT and Outsourcing disputes and a consultant in service delivery. He is a member of the Society of Computers and Law and a director of Oareborough Consulting.

The Post Office Horizon IT Scandal: How should organisations react when IT systems go wrong?

Andrew Woolsey and Sophie Ashcroft take a fresh look at the legal issues surrounding defective software through the lens of the Post Office Horizon IT scandal

The Horizon Post Office Scandal has been described as one of the greatest miscarriages of justice in UK history and has become a pivotal case study on the subject of legal integrity. In addition to the more widely publicised issues associated with the Scandal, the matter also offers critical lessons in the governance and oversight of large-scale public contracts and IT systems management. This article focuses on the latter topic, and specifically, practical steps that organisations can take to mitigate against potential liability in situations where IT systems go wrong, whether that be due to system or human failure.

> **It is important to be alert to the fact that IT systems sometimes fail**

Background

The Horizon Post Office Scandal features heavily within public consciousness due to the nature of the Scandal, the long-running public inquiry, and various television dramatisations.

More than 900 subpostmasters were convicted of theft and false accounting after shortfalls in their branch accounts were discovered, and were wrongly prosecuted by Post Office and the Crown Prosecution Service. The Post Office itself took many of these cases to court, prosecuting 700 people between 1999 and 2015, whilst another 283 cases were brought by other bodies, including the Crown Prosecution Service.

One of the underlying causes of this injustice was Horizon, a digital accounting system provided by the IT multinational, Fujitsu and rolled out to thousands of Post Office branches in the early 2000s. Almost immediately after the installation, there were reports of unexplained accounting shortfalls. Under the previous paper-based system, it would have been relatively easy to review the accounts and find the cause for any shortfalls. The design and implementation of Horizon, and the reliance placed on the software within Post Office branches, meant the reason for the shortfalls could not be established. Whilst sub postmasters owned their own businesses (namely the local Post Office branches) they were agents for Post Office. As such, and in the first instance, explaining any accounting shortfalls would be the responsibility of the subpostmasters. Given the lack of clearly identifiable evidence, proving the shortfalls were attributable to IT system error was near impossible for many.

The evidential and factual fight battle subpostmasters engaged in was made more difficult by the fact that computer-generated evidence in English law cases is subject to a common law presumption that the computer system producing the evidential record was working properly at the material time and that the record is admissible as real evidence. This presumption is rebuttable if evidence to the contrary is adduced, in which case it is for the party seeking to produce the computer record to satisfy the court that the computer was working properly at the material time.

Ascertaining who is at fault when IT systems fail

The context described above is not unique to the Horizon Scandal, and the question of who is liable when IT systems go wrong will always be a factual one. When systems fail there will be a multitude of assessments that seek to establish (i) why the system failed; (ii) who was responsible for the failure; and (iii) who is liable for any losses that have been suffered as a result of the IT system failing. Difficulties in assessing these issues can lead to time consuming and expensive disputes. For instance, did the system fail because of an underlying issue that was present at source (as was the case with the Horizon system), or was it because of the way in which the system was installed and

implemented by the organisation or was the failure due to the way in which the system was operated by the employees and/or agent whose job it was to operate the IT system. Whilst a number of potential disputes between various different stakeholders might be triggered due to IT system failure, it is important to bear in mind that the nature of these disputes largely depends on the contractual relationships (i.e. between system provider (Fujitsu) and employer (Post Office) and between employer and employee/agents (sub postmasters)), what specifically goes wrong, and what is stated in the various liability and risk provisions of the relevant contracts.

Considerations for organisations when IT systems go wrong

One of the starkest aspects of the Horizon Scandal (as detailed in the public inquiry) was the way in which the concerns of sub postmasters were dismissed by the Post Office in favour of the reliance placed on the Horizon system.

Organisations should not default to the presumption that computer systems producing evidential records were working properly at the material time. It is important to be alert to the fact that IT systems sometimes fail, and that failure could very easily be because of an inherent issue with the system itself as opposed to human error. In the case of a potential IT system failure, it is essential that organisations act quickly by investigating and documenting, to the extent that this is possible, the (i) the date on which the issue/s first arose; (ii) a description of the relevant issues; and (iii) any apparent and obvious causes of the system failure. Organisations should also consider instructing forensic experts at an early stage as this will provide a much clearer understanding of the cause of the failure and, importantly, ensure that the organisation is evidentially prepared for any litigation that might ensue. The early instruction of independent forensic experts can also mitigate against any potential bias and/or impartiality arguments being raised in relation to the investigation by other parties to the litigation.

A further lesson from the Horizon Scandal is that it is essential to ensure that the roles, responsibilities, expectations and allocation of risk between the various parties involved with the provision, installation and operation of the IT system are contractualised and defined in detail. When it came to Horizon, the Post Office could not say for certain where Fujitsu's role and responsibilities ended and theirs started, which resulted in reliance being placed on the default position that the Horizon software was infallible, and as such, the only logical explanation was that the subpostmasters were to blame.

In the event that an IT system fails, then it is likely that there will be multiple claims, with stakeholders seeking to recover their losses from the party next in the contractual chain. The claims will typically be for breach of contract arising from a failure to provide services in accordance with the express terms of the contract and/or with reasonable care and skill. Such claims may give rise to damages, termination rights and/or other contractual remedies specified in the contracts. Organisations should ensure that contractual arrangements with IT suppliers and employees/agents include specific warranties, indemnities and limitation provisions that are, to the extent that this is possible, tailored to the specific purpose of the IT system and should be based on standards that are clearly and objectively measurable.

Conclusion

The contractual issues referred to above are highly specific to the use to which the IT system will be put so contracting parties should seek to engage as early as possible with their stakeholders, consultants, lawyers and other experts to help them navigate this area.

As noted in the introduction to this article, the Horizon Scandal offers critical lessons in the governance and oversight of large-scale public contracts, and IT system management. Effective governance processes and audit trails are crucial for ensuring data oversight and for

exposing discrepancies and inconsistencies in IT systems as early as possible.

From a corporate governance perspective, it appears surprising that the Horizon narrative was not challenged at a board level. As the Horizon Scandal demonstrates, in situations where IT systems fail and litigation ensues, directors could potentially find themselves to be in breach of section 172 of the Companies Act 2006, which places on company directors a legal "duty to promote the success of the company", and/or the UK Corporate Governance Code (UKCGC) 2024 which notes that "all directors must act with integrity, lead by example and promote the desired culture". To mitigate against this, and to improve trust and transparency, organisations should establish internal guidelines and policies, and implement an appropriate governance framework to address the specific risks associated with IT system failure.

Given the close scrutiny the Horizon Scandal has attracted, we anticipate that the courts may re-evaluate the common law presumption cited above. Notwithstanding the fact that it is common for IT systems/software to fail for all manner of reasons, the rebuttable presumption will likely become increasingly unsuitable in a world in which Artificial Intelligence use is becoming ever-present. The inherent complexity and uncertainty associated with AI means that, in most cases, it will be virtually impossible to ascertain why the AI failed and who is to blame – was it the data used by the AI developer to train the AI tool or was it because the training methodology used by the AI developer was flawed or inadequate, or did the IT supplier fail to exercise sufficient oversight over the outputs that the AI tool produced before submitting outputs to the end user?

How the courts re-evaluate the common law presumption on computer-generated evidence could easily form the basis of a separate article. For present purposes we would suggest that there needs to be, at the very least, clear recognition that errors do arise in evidence from IT systems. One possible solution would be to shift the burden of proof onto the organisations seeking to rely on computer generated evidence and stipulate that early disclosure (either in the pre-action phase or during pleadings) of documents and evidence be provided to allow the court to consider and assess, to the extent that it can, whether the computer-generated evidence is reliable and admissible.

Sophie Ashcroft

Sophie Ashcroft is a Partner in the Commercial Dispute Resolution at Browne Jacobson. She specialises in resolving disputes arising when large IT projects go wrong, as well as disputes between SMEs and their managed service providers.

Andrew Woolsey

Andrew Woolsey is an Associate in Browne Jacobson's Commercial Dispute Resolution team, based in London. Andrew works on a variety of commercial disputes, with a focus on technology disputes arising from complex IT projects, outsourcing and managed services.

Emerging technologies and the climate: charting a pathway to pre-emptive oversight

Once upon a time technologies like artificial intelligence and the metaverse were confined to the annals of science fiction. No longer, both innovations exist in the here and now, with vast potential to transform our world. These emergent technologies, however, are not without attributes of concern, one of which is energy consumption and the consequent emissions.

These technologies and their transformative capacity are no doubt here to stay so this short brief posits that we must chart a pathway to responsible regulation of their energy consumption before the tech world runs away with itself.

Trusting the tech world with climate protection?

The tech industry positions itself as the forerunner of tomorrow's world, embracing policies of carbon neutrality. Alphabet have pledged to meet net zero; Apple are seeking supply chain neutrality by 2030; Microsoft's Azure platform is intended to run on renewables by 2025; and Meta claim to have already reached net zero emissions. Examining Meta, it convincingly pushes a carbon neutral narrative, yet inspection reveals some of this rhetoric might just be hot air.

Meta purchases only clean energy so is able to make an allowable claim of carbon neutrality. However, Meta is draining the market and its Irish datacentre used the equivalent clean energy of 151,000 homes in 2021. It is not resupplying energy grids, nor is it engaged in projects advanced enough to generate replacement energy. Yes, Meta does have some green proclivities, and is involved in restoration projects, but these are all located in the USA and lack efficacy when compared to energy consumption.

Meta is not alone in needing to take greater responsibility for energy use, and the American Clean Power Association finds that 48% of all clean energy is consumed by the tech industry. Sector wide realignment from power purchase agreements to restoration and generation is required if carbon neutrality is to be legitimately achieved. Silicon Valley sustainability narratives lack impression, even without considering the energy habits of transformative emergent technology.

The metaverse, AI, and energy consumption – is it an issue?

Looking at the metaverse, it is difficult ascertain energy usage data because it remains in embryonic form. Yet, if we consider that in 2011 Meta was using 0.53 terawatt-hours compared to 11.51 in 2022, it is reasonable to assume that introducing a vastly more immersive technology than the current Web2 will cause energy consumption to skyrocket.

Moreover, the Metaverse is intended to reach a plateau not unlike the fictional Ready Player One. Chip producer Intel thinks a 1000 fold increase in computing power will be required, no doubt having a commensurate uptake in energy demand. This means that in terms of powering the technology, and the sheer scale of its inevitable popularity, energy consumption will be gargantuan. Efficiency gains in hardware might negate some of this demand, and arguments have been put forward that the metaverse will be responsible for a drop in vehicle emissions. Yet, these arguments remain speculative and unreliable as a means of mitigation.

Where AI is concerned, the evidence surrounding its energy use is more readily visible. Training an AI model in 2019 generated 626,000 pounds of CO2, about five times more than that generated by a car over its lifetime. A ChatGPT prompt uses 2.9 watt-hours of electricity, compared to a standard google search that uses 0.3 watt-hours. Cloud data centres are predicted to double their energy consumption to 1000 terawatts by 2026, in part because of the increased use of AI. The cooling of these datacentres is also problematic, with Google, for instance, already using 25% of the water supply of the city of Dallas to cool its databanks.

Staggering as they are, these figures may just be the tip of the iceberg. It remains challenging

to attribute accurate greenhouse gas emissions to the use of AI due to an absence of regulatory oversight, allowing tech corporations to select what they report in terms of energy use and emissions. This gap led to the European Union adopting the Regulation on Artificial Intelligence Act 2024 that aims to put reporting and calculation models in place for the consumption of energy related to AI. While this step is welcomed, discussions must be had at the global level.

Responsible practice through a global charter

AI, the metaverse and any other emergent technology requires a set of foundational principles to regulate their impact upon the climate and wider environment. We need an international technology charter, one that is agreed upon universally and given resources and scope to be effective.

A charter is distinguishable from treaties which come with the trappings of consent, sovereignty, and endless political sabotage. Also, treaties are state orientated, and while governments have a role to play, the tech world is perhaps more influential than ever before, so the big players in the sector should not be absolved from involvement.

A charter can reflect this reality, placing the technology sector front and centre of the creation process. That does not mean allowing corporations to draft it themselves, that lesson is poignantly brought to life in Orwell's Animal Farm. But it does mean bringing their expertise to bear in the drafting alongside climate, environmental and energy specialists.

This charter must come from informed dialogue and good faith cooperation between relevant stakeholders. Yet, there are some core principles that would be reasonable from the outset.

First, emergent technology must be energy positive and not deplete clean power. It must be completely reliant on renewable energy streams distinct from the primary power grid.

Second, emergent technology in its operation must not harm the environment. Datacentres and infrastructure must be located in brownfield sites, not situated in leafy green areas where development damages the natural environment. Alongside, use of resources, like water for cooling, must come from dedicated recycling activities.

Third, emergent technology, and particularly the metaverse, must in good spirit seek to promote environmental protection through education. It must not become a substitute for the real world, but an advocate for advancing knowledge and preservation.

From these central principles, others must drive the discussion for a charter that ensures the future impact of emergent technology is positive. For it is a bleak tomorrow where humanity retreats to a digital world in search of green spaces and climate stability. The time to act is now, before one avatar says to another, "where were your parents when the climate collapsed?"

Ash Murphy

Ash Murphy is a Senior Lecturer at Manchester Law School (MMU), researching in the field of international climate, energy, security and technology law. The lens through which this research is conducted is always planetary protection and climate security, using innovative solutions to solve problems.

accenture

Learn how to apply generative AI to maximize efficiency and drive competitive advantage.

A new era of generative AI for everyone

http://accenture.com/total-enterprise-reinvention

Digital transformation: the risks of providing non-digitally accessible products in the EU and UK

A team from Hogan Lovells consider the regulatory regimes governing digital accessibility in the UK and EU.

In the era of digital transformation, the need to ensure products and services are accessible to all, including those who experience some form of disability, is greater than ever. While there is not (yet) a global uniform approach to governing the digital accessibility requirements of products and services, certain countries have developed fairly articulate and progressive legal frameworks in this respect. Even in countries where such legislation does not yet exist, consumer expectations have grown, leading to products and services that do offer accessibility features having a unique selling point over those that do not. As a result, potential risks have developed for economic operators who make available non-digitally accessible products and services. With digital accessibility at the forefront of the minds of legislators, regulators and consumers alike, such risks are only expected to increase as time goes by. Companies should therefore start considering how to safeguard themselves accordingly now – putting digital accessibility front and centre of all they do.

At its core, digital accessibility aims to ensure that digital products and services are accessible to all, including those who experience physical, hearing, vision, speech or physical disabilities. Whether driven by government policy, regulatory frameworks, consumer expectations, or even a company's own drive to "do better", digital accessibility aims to guarantee non-discriminating user experience at a visual, auditory, motor and cognitive level.

Although there is not (yet) a global uniform approach to the governance of digitally accessible products and services, certain countries have developed fairly articulate and progressive legal frameworks in this respect. These countries are most notably within the European Union, take for example Italy, which now has an array of digital accessibility-focused regulations to consider. On the other hand, countries like the United Kingdom have taken a more "light touch" approach, focusing instead on industry self-regulation.

The legal framework at a glance

- Both Italy and the UK are signatories to the UN Convention on the Rights of Persons with Disabilities. The Convention is the first international, legally binding instrument setting minimum standards for the rights of people with disabilities. It broadly categorizes the term "persons with disabilities" and reaffirms that all persons with all types of disabilities have a right to enjoy all human rights and fundamental freedoms. In addition, it identifies areas where adaptations must be made for persons with disabilities to allow them to effectively exercise their rights, which is something that is further reflected within the EU's 2021 – 2030 Strategy for the rights of persons with disabilities.
- There is also specific EU-level legislation at play. The key EU-level laws that introduce some form of digital accessibility governance currently include:
  - The Web Accessibility Directive: which aims to provide people with disabilities[1] with better access to the websites and mobile applications of public services. To do so, the WAD, which has been implemented in Italy by the "Stanca Law"[2] and is also retained legislation in the UK[3], introduces a duty for public sector bodies to make their websites and apps accessible by reference to specific standards, notably harmonised standard "EN 301 549 V3.2.1 (2021-03) Accessibility requirements for ICT products and services", which is in line with the most recent Web Content

[1] *WAD is stated to be, in particular, for "persons with disabilities", which it defines in accordance with the UN Convention as those people having "long-term physical, mental, intellectual or sensory impairments which may, in conjunction with other barriers, hinder their full and effective participation in social on an equal basis with others". It does not specify any particular types of disability*

[2] *Law no. 4/2004, as amended.*

[3] *The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.*

Accessibility Guidelines: WCAG 2.1.

- The Audiovisual Media Services Directive, the European Electronics Communications Code and the Citizens' Rights Directive: which have all been implemented in Italy and are also retained legislation in the UK[4], provide for certain accessibility requirements applicable to audiovisual media (i.e. traditional TV broadcasts, on-demand services as well as video-sharing platforms) and the broader telecoms framework.
- And perhaps most crucially, the European Accessibility Act: which was introduced in April 2019 to harmonise legislation and set new EU-wide minimum accessibility requirements for certain products and services. The EAA, which has been implemented in Italy[5] but, as a result of Brexit, has not been adopted in the UK, focuses specifically on enhancing the accessibility of digital products and services for people with disabilities or other functional limitations, such as the elderly.

Using this legislation, one of the driving messages EU legislature have attempted to deliver to economic operators that manufacture digital products or provide digital services is that the starting point is accessible design. Although, as briefly outlined above, EU legislation on digital accessibility has so far has been patchy, limiting its scope to e.g. public sector services or covering only specific categories such as electronic communications or audio media services, thinking about accessibility from the outset is something that is a clear expectation under the EAA, which is set to fill the gap and cover all aspects of making products and services accessible in a consistent manner across the EU Member States.

"Although the EAA is not applicable in the UK as it was enacted after Brexit, that does not mean that digital accessibility can simply be ignored when supplying digital products and services on the UK market.

To do so, the EAA, which will enter into force on 28 June 2025, focuses on digital products and services (e.g. computers and operating systems, ATMs, banking services, e-books, e-commerce and smartphones, to name just a few!) with the aim of improving the accessibility of technologies for persons with disabilities or functional limitations. In an EU first, the EAA sets out various requirements, including that economic operators must only place products and only provide services on the EU market that comply with specific accessibility requirements set out in Annex I of the EAA, and that consumers must be provided with certain accessibility information. The EAA will therefore require certain hardware (e.g. smartphones and computers) and software (e.g. audio-visual media services apps) to be accessible by design, with its requirements applicable to both public and private entities supplying in-scope products and services in

[4] *The Audiovisual Media Services Regulations 2020 ("AVMS Regulations"), implementing the Audiovisual Media Services Directive ("AVMSD"), the Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020 ("ECWT Regulations"), implementing Directive (EU) 2018/1972 establishing the European Electronic Communications Code ("EECC"), and the Communications Act 2003 ("Communications Act").*

[5] *Legislative Decree of 27 May 2022, no. 82, as amended by Law of 10 August 2023, no. 103.*

the EU, regardless of their size (except for microenterprises).

Although the EAA is not applicable in the UK as it was enacted after Brexit, that does not mean that digital accessibility can simply be ignored when supplying digital products and services on the UK market. This is because the UK does have legislation that is wide enough to be interpreted as introducing accessibility requirements for digital products and services, namely the Equality Act 2010, which requires service providers to make "reasonable adjustments" for people with disabilities both online and offline. This obligation requires such providers to proactively anticipate the needs of disabled persons, including by providing information in accessible formats.

It is against this backdrop that economic operators across the EU and UK should be alive to the potential risks that making available non-accessible products and services may entail, including the risk of not telling consumers just how non-digitally accessible their products or services are.

Providing non-digitally accessible products and services – what are the risks?

It should have become clear by now that accessibility, and specifically digital accessibility, has become a key agenda item for governments across the globe, and most notably in the EU, a scenario that won't likely change in the foreseeable future. As such, in-scope economic operators need to not only be aware of how to comply with their explicit digital accessibility-related obligations (as outlined in, among others, the legislation noted above), but also the more indirect obligations that may now arise.

One example of such 'indirect' obligation relates to the provision of information as to the digital accessibility features of an economic operator's products and/or services. Omitting to include what could be considered to be 'material' information of a product or service (i.e. its (non) digital accessibility capabilities), regardless of whether such product or service is in scope of specific digital accessibility legislation (such as the EAA), could lead to a consumer with a disability purchasing a particular digital product or service only to later discover that it is not accessible and, thus, not usable by that particular user. In turn, this may lead to consumer complaints or claims (under digital accessibility legislation, or more widely, under general consumer law), as well as potential enforcement action, with the relevant regulatory authorities possibly deeming such practices as misleading or unfair to consumers.

In Italy, not including an indication that a product or a service is not accessible, thus indirectly inducing a consumer with a disability to make a commercial decision that they would not otherwise have taken, could be construed as a misleading commercial practice in violation of the Italian Consumer Code.[6] Article 20, par. 3 of the Italian Consumer Code takes this point further, governing the scenario where a commercial practice – while reaching many groups of consumers

> **"In the UK, although digital accessibility is a key item on the UK Government's agenda, specific accessibility requirements for products and services are not yet at play**

[6] *Under Article 22 of the Italian Consumer Code, a misleading commercial practice is defined as the conduct of a person who: (i) omits, or presents in an obscure or untimely manner, material information that the average consumer needs in order to make an informed commercial decision; or who (ii) induces the average consumer to make a commercial decision that he or she would not otherwise have taken.*

Using this legislation, one of the driving messages EU legislature have attempted to deliver to economic operators that manufacture digital products or provide digital services is that the starting point is accessible design

– distorts the economic behaviour of only one group of consumers who are particularly vulnerable on account of, *inter alia*, their mental or physical disability. In such scenario, the "*average consumer*", through the lens of which the unfairness of the practice itself is to be assessed, will be the average consumer with a disability.

Once an unfair commercial practice has been established, the Italian Antitrust Authority ("*Autorità Garante della Concorrenza e del Mercato*") may impose an administrative fine of up to EUR 10 million, taking into account the seriousness and duration of the violation and also the economic conditions of the operator.[7] Additional legal risks also derive from the fact that persons with disabilities (including those represented by equal opportunity organisations or associations) are permitted to represent themselves in front of judicial authorities following discriminatory acts, even if such act was 'indirect' – i.e. when "apparently neutral conduct (such as the omission of information on e.g. the digital accessibility features of a product or service, even if not explicitly required by any law) puts a person with a disability at a disadvantage compared to other persons".[8] Such court proceedings (similarly as proceedings before the AGCM) not only carry with them legal risks for a company, but may also generate considerable media coverage that can damage a company's reputation and irreparably undermine consumer trust.

In the UK, although digital accessibility is a key item on the UK Government's agenda (reflected in its National Disability Strategy and the Disability Action Plan for 2024), specific accessibility requirements for products and services are not yet at play (and it looks to remain this way for the near future). As a result, while similarly to Italy, failure to provide consumers with the material information they need to make informed purchasing decisions may be deemed an unfair commercial practice[9], the more prominent risks in the UK are likely to stem from economic operators claiming that their products and services are accessible without that being the case (e.g. risk of making a misleading claim that may influence a consumer to make a transactional decision they would not have made otherwise), and less so from failing to state that their products or services are not accessible.

That said, increased risks in this regard are likely to arise later down the line, especially once the EAA comes into effect. This is because looking to what must be offered to EU consumers (i.e. digitally accessible products and services from 2025), UK consumers may well begin to expect "more" from their products and services, even if this is not explicitly required by UK legislation. As a result, scenarios can easily be envisaged where current UK legislation begins to be interpreted in creative ways by consumers, consumer groups, or even regulators in order to bring claims and actions against economic operators for making

[7] *Article 27, par. 9 of the Italian Consumer Code.*

[8] *Law No. 67 of 1 March 2006, see Article 2, para. 3*

[9] *The Consumer Protection from Unfair Trading Regulations 2008, see Regulations 3, 5 and 6.*

available non-digitally accessible products and/or services on the UK market.

For example, arguments may develop that a failure to state that a product or service is not accessible should be construed as a misleading omission, given this should (now) be considered as an 'essential characteristic / restriction' of a product or service. Alternatively, the requirements of the Equality Act could be interpreted in new, all-encompassing ways which require product manufacturers and service providers to do "more" to make their products and services accessible to all (with 'reasonable adjustments' potentially being interpreted as having a wider meaning than ever before). While this may seem theoretical, the same was initially said for greenwashing claims, but one only needs to look at the headlines nowadays to see the expansion of claims in this arena despite there being no specific laws in the UK governing green claims, showcasing how the interpretation of 'old' legislation can be widened to fit with the times.

The direction of travel and how to safeguard?

While it is correct that digital accessibility legislation, where this does exist, is far from mature and that – even with the entering into force of the EAA – there will be no general obligation for economic operators to market only digitally accessible products and services in the EU, it is also correct that explicit digital accessibility requirements are on the rise. This, in turn, increases the risks surrounding non-digitally accessible products and services, regardless of whether or not they are within the scope of such legislation, particularly when taking into account ever-growing consumer (and regulator) expectations. Further, these risks are in no way limited to potential claims before the courts or potential proceedings by regulatory authorities either, and it is likely that businesses will begin to receive consumer complaints, bad media coverage and general reputational damage for failing to provide accessible products and services, or at least for failing to notifying consumers that the product or service in question is not accessible.

In light of these risks, economic operators are strongly recommended to take a proactive approach to digital accessibility at all stages of the lifecycle, i.e. by implementing inclusive design processes when developing their products and services, all the way through to training their staff on accessibility best practices. Taking this a step further, companies should also carefully begin to consider how best to communicate the possible lack of accessibility of their digital product or service, for example, by way of explicit on-the-label information or via the use of pragmatic alternative solutions (e.g. webpages and/or QR codes). Such transparency and clarity in consumer communication will likely go a long way in demonstrating a real respect for the rights of people with disabilities.

To put it simply: this is a last call to economic operators dealing with digital products and services, with digital accessibility no longer being a "nice to have" but slowly becoming a non-negotiable endgame destination. The time to act is now.

This article was first published on the Hogan Lovells Engage portal and is reproduced with permission

Christian Di Mauro, Valerie Kenyon, Vicki Kooner, Lorena Baltazar & Guido Di Stefano

Hogan Lovells

The UK's Automated Vehicles Act – Unlocking Opportunities for UK Investment and Innovation in the Automotive Sector

A team from Bird & Bird precis the key points of the Automated Vehicles Act, which received Royal Assent just before Parliament was dissolved.

The Automated Vehicles Act 2024 received Royal Assent on 20 May 2024. Its swift motion through parliament in an election year has been a relief to many, having been first introduced to the House of Lords in November 2023. It provides a framework for the safe integration of autonomous vehicles (AVs) into society (potentially as early as 2026) and paves the way for further investment opportunities in the UK market alongside growing public support and consumer optimism.

The UK already has a strong reputation for self-driving technologies. According to the Government, approximately 70% of global automotive sector companies that source self-driving technologies do so from the UK market. It is hoped that the Act will build further confidence in the UK as a global leader in this high-growth industry.

Scope

The Act has three main aims with regards to self-driving vehicles:

- to create a rigorous safety framework;
- to clarify legal liability; and
- to protect consumers.

Safety framework and standards

The Act introduces an authorisation process for self-driving vehicles. AVs will be required to undergo a self-driving test to ensure safety benchmarks are met. These will be outlined in the Secretary of State's Statement on Safety Principles.

Crucially, AVs must enhance road safety, instead of contributing to current safety standards. The safety principles that will be included in the Statement on Safety Principles will be centred around "securing that authorised automated vehicles will achieve a level of safety equivalent to, or higher than, that of careful and competent human drivers". They also require the Secretary of State to consult organisations that appear to them to represent the interests of AV manufacturers, road users, and road safety. The Act also gives the Secretary of State powers to amend existing legislative regimes (such as type approval legislation) to achieve the aims of the framework legislation.

Legal liability

New concepts are incorporated in the Act which address the delineation of legal liability. These are outlined below.

Authorised self-driving entities (ASDEs):

Once a vehicle successfully passes the self-driving test, it will be classified as an 'authorised automated vehicle'. For every authorisation granted, there must be a designated entity known as the 'authorised self-driving entity' (ASDE). This entity has ultimate responsibility for ensuring the AV consistently complies with the requirements of the self-driving test and any accompanying requirements that the Secretary of State imposes. These entities will be the companies developing the cars (or potentially the software suppliers) and not individual users.

User-in-charge (UiC):

The Act makes a distinction between authorised AVs equipped with 'user-in-charge' (UiC) features and those that do not. UiC features mean those where a user can intervene during a journey. When a vehicle has these features there will be specific authorisation criteria around the requests that trigger user intervention and the transition periods during which intervention is required. How the transition requests are delivered, the duration of transition periods, and how the vehicle safely handles situations where a user fails to intervene are addressed in the Act.

A non-UiC journey is one where the AV drives itself for the whole or any part of a journey. In these cases, the ASDE will be legally liable in the case of an incident. AVs that undertake no-UiC journeys will need a licensed operator. The licensed operator's role will be to ensure the safe operation of the vehicle. They will be responsible for matters like ensuring the vehicle is insured and detecting and resolving issues during the journey, for example responding to breakdowns. Ultimately, however,

the ASDE retains responsibility for how the vehicle drives.

The Act grants immunity from liability to UiCs in specific circumstances, outlines exceptions to immunity, and establishes when a user will be liable as the legal driver of the vehicle. To avoid unfair responsibility being placed on UiCs, ultimate responsibility for automated driving behaviour (when the non-UiC feature is engaged, or the engaged UiC feature fails to alert the UiC to take control) lies with the ASDE. This grants the UiC immunity from road traffic offences when the vehicle is driving itself. When the vehicle is being driven by the UiC, it is treated as a conventional vehicle. The liability position as regards drive assist features (for example cruise control) remains the same, meaning the driver will continue to be liable for incidents that arise while using those features.

Consumer protection

Marketing

The Secretary of State has the power to regulate how self-driving cars are marketed. This is aimed at preventing consumers from being misled into believing a vehicle is fully self-driving when it actually just includes driver assistance features.

There is an outright prohibition on using specific terms, expressions, symbols, and marks other than for marketing authorised automated vehicles. There are also restrictions on the overall presentation of marketing communications to limit confusion regarding the varying degrees of autonomous capabilities.

Investigations

The Act provides the government with regulatory and enforcement powers – including the ability to conduct broad investigations if a self-driving car is found to be involved in a road traffic incident. The Act further provides for the modification of road traffic offences, so that they apply to the context of self-driving vehicles as they would apply to the driver of a standard car.

Sanctions

There will be new sanctions and penalties, including fines, requirements to take corrective action, suspension of operation and criminal offenses in serious cases.

Automated Passenger Services

AVs that carry passengers (for example, taxis), will need a permit from the Secretary of State.

What's next?

The Act is a framework piece of legislation which will be further developed through secondary legislation. Consultations are due to commence this year with the view to regulations being finalised in 2025 and 2026. However, with the next general election being tabled for 4 July 2024, the precise timetable may be subject to change.

George Mason

Partner at Bird & Bird.

Jonathan Speed

Partner at Bird & Bird.

Russell Williamson

Senior Associate at Bird & Bird.

EU AI Act Finalised

The team from the Technology & Innovation Group at Matheson pick out the key points from the now final EU AI Act which will be in force this Summer.

On 21 May 2024, the EU Council approved the EU Artificial Intelligence Regulation (the "AI Act"). This marks the final step in the legislative process, following the European Parliament's approval of the landmark law on 13 March 2024 after extensive negotiations with EU Member States. The final text of the AI Act will be published in the coming weeks in the Official Journal of the EU.

What is being regulated?

The AI Act defines an "AI System" as "a machine-based system designed to operate with varying levels of autonomy and may exhibit adaptiveness after deployment and that, for a given set of explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence real or virtual environments."

The AI Act also introduces dedicated rules for general purpose AI ("GPAI") Models, which are models that display significant generality, are capable of performing a wide range of distinct tasks, and can be integrated into a variety of downstream systems or applications.

Scope of the AI Act - who is impacted?

The AI Act will apply to different players across the AI distribution chain, including the following:

- AI providers – those who develop AI systems or have them developed for them;
- AI deployers – those who use AI systems (except personal use);
- Importers and distributors of AI;
- AI product manufacturers;

> **The AI Act has extra-territorial scope, and may apply to businesses not established in the EU**

- Authorised representatives of AI providers who are not established in the EU; and
- Affected persons located in the EU.

The AI Act has extra-territorial scope, and may apply to businesses not established in the EU. The AI Act will apply to providers located within the EU or in a third country, in circumstances where they make an AI system or GPAI model available on the EU market. In addition, where only the output generated by the AI system is used in the EU, the AI Act will apply to the provider and deployer of the AI system.

Non-EU providers of GPAI models and high-risk AI systems are required to appoint an AI representative in the EU to act as a contact point for EU regulators.

Risk-based approach

The EU has taken a risk-based approach to the regulation of AI. The higher the risk of harm to society, the stricter the rules. The AI Act establishes four categories of AI systems based on the probability of an occurrence of harm and the severity of that harm:

Prohibited AI Systems – These are AI systems that pose an unacceptable level of risk to individuals' safety, rights, or fundamental values. These systems are banned for use in the EU under the AI Act. Examples include social scoring, compiling facial recognition databases, and real-time biometric identification in publicly accessible spaces (subject to certain exceptions).

High-Risk AI Systems – AI systems that fall under this category have a high potential to cause significant harm or infringement of rights. They require strict regulation and oversight to mitigate risks. They include AI systems used in critical infrastructures, education, employment, essential private and public services, law enforcement, border control management and administration of justice.

Limited Risk AI Systems – These AI systems present lower risks. They still need to adhere to certain safeguards, however, the regulatory requirements for these systems are less stringent. An example of a limited risk AI system is an AI-powered customer service chatbot used to provide automated responses to customer questions.

Minimal Risk AI Systems – The AI systems in this category pose minimal risks to individuals' rights, safety, or societal values and are therefore subject to lighter regulatory burdens. For example, basic email filters that classify messages as spam, with a low likelihood of negative impact.

GPAI models

The AI Act provides specific rules for (i) GPAI models and for (ii) GPAI models that pose "systemic risk". GPAI models not posing systemic risks will be subject to limited requirements, such as with regard to transparency. However, providers of GPAI models that pose systemic risk will be subject to increased obligations, including performing model evaluation, assessing and mitigating possible systemic risks, ensuring an adequate level of cybersecurity protection, and reporting serious incidents to the AI Office and, as appropriate, national authorities.

A new governance structure

To ensure proper enforcement of the new rules, several governing bodies are being established, including:

- An EU AI Office within the EU Commission to enforce the common rules across the EU. The EU Commission has confirmed that this AI Office will not affect the powers of the relevant

national authorities and other EU bodies responsible for supervising AI systems;
- A scientific panel of independent experts to support the enforcement activities;
- An AI Board with Member States' representatives to advise and assist the EU Commission and Member States on consistent and effective application of the AI Act; and
- An advisory forum for stakeholders to provide technical expertise to the AI Board and the EU Commission.

Provider obligations

Providers of high-risk AI systems must, among other things:
- ensure the AI systems are compliant with the AI Act;
- have a quality management system in place;
- keep specific documentation;
- keep the logs automatically generated by the high-risk AI system;
- carry out conformity assessments and prepare declarations of conformity for each high-risk AI system; and
- comply with registration obligations.

Deployer obligations

Where businesses are acting as deployers of high-risk AI systems, they are subject to the following obligations:
- take appropriate technical and organisational measures to ensure compliance with provider instructions;
- allocate human oversight to natural persons who are competent, properly qualified and resourced;
- ensure input data is relevant and sufficiently representative (to the extent the deployer exercises control over it);
- monitor the operation of the high-risk AI system and report incidents to the provider and relevant national supervisory authorities;
- keep records of logs generated by the high-risk AI system (if under the deployer's control) for at least six months;
- cooperate with relevant national competent authorities; and
- complete a fundamental rights impact assessment before using a high-risk AI system.

"The AI Act imposes fines for non-compliance with its obligations, which are split into three tiers

Transparency obligations

Providers and deployers of certain AI systems and GPAI models are also subject to transparency obligations to:
- ensure that users are aware that they are interacting with AI;
- inform users when emotion recognition and biometric categorisation systems are being used; and
- label AI-generated content as such.

Penalties

The AI Act imposes significant fines for non-compliance with its obligations, which are split into three tiers:
- up to €35 million or 7% of total worldwide turnover, whichever is higher, for non-compliance with the provisions on prohibited AI practices;
- up to €15 million or 3% of total worldwide turnover, whichever is higher, for non-compliance with specified obligations of various operators of AI systems and infringements of the AI Act (including infringement of the rules on GPAI); and
- up to €7.5 million or 1% of total worldwide turnover, whichever is higher, for the supply of incorrect, incomplete or misleading information to notified bodies and national

competent authorities.

However, for small and medium-sized enterprises ("SMEs"), including start-ups, the AI Act allows for the lower scale of penalties to be applied and requires that the interests of SMEs and their economic viability be taken into account when imposing fines.

When will the AI Act come into force?

The AI Act will be published in the Official Journal of the EU in the coming weeks, and will enter into force 20 days after publication. The AI Act will be fully applicable 24 months after entry into force, with a graduated approach as follows:

- Prohibition on certain unacceptable uses of AI – applicable 6 months after entry into force (late 2024 / early 2025)
- Rules on GPAI Models – applicable 12 months after entry into force (mid-2025)
- Penalties for breaching obligations (with the exception of fines for providers of GPAI models) – applicable 12 months after entry into force (mid-2025)
- The AI Act in general, including for high-risk AI systems (see Annex III for the list of systems) – applicable 24 months after entry into force (mid-2026)
- High-risk AI systems as part of safety components in regulated products (see Annex I for the list of laws governing these products) – applicable 36 months after entry into force (mid-2027)

Systems placed on the market or put into service before the AI Act enters into force

There are some further exceptions to the 24 month timeline for full applicability of the AI Act, specifically for systems that have been placed on the market or put into service before the end of this period. Providers of GPAI models that have been placed on the market before 12 months from the AI Act's entry into force will have 36 months from the date of entry into force by which to comply.

Operators of AI systems that are part of large-scale IT systems used in the areas of freedom, security and justice, and are on the market or put into service no later than three years after the AI Act enters into force, have until 31 December 2030 to comply with the AI Act. However, the prohibition on certain AI systems still applies, whereby these systems must no longer be used after six months of the AI Act's entry into force.

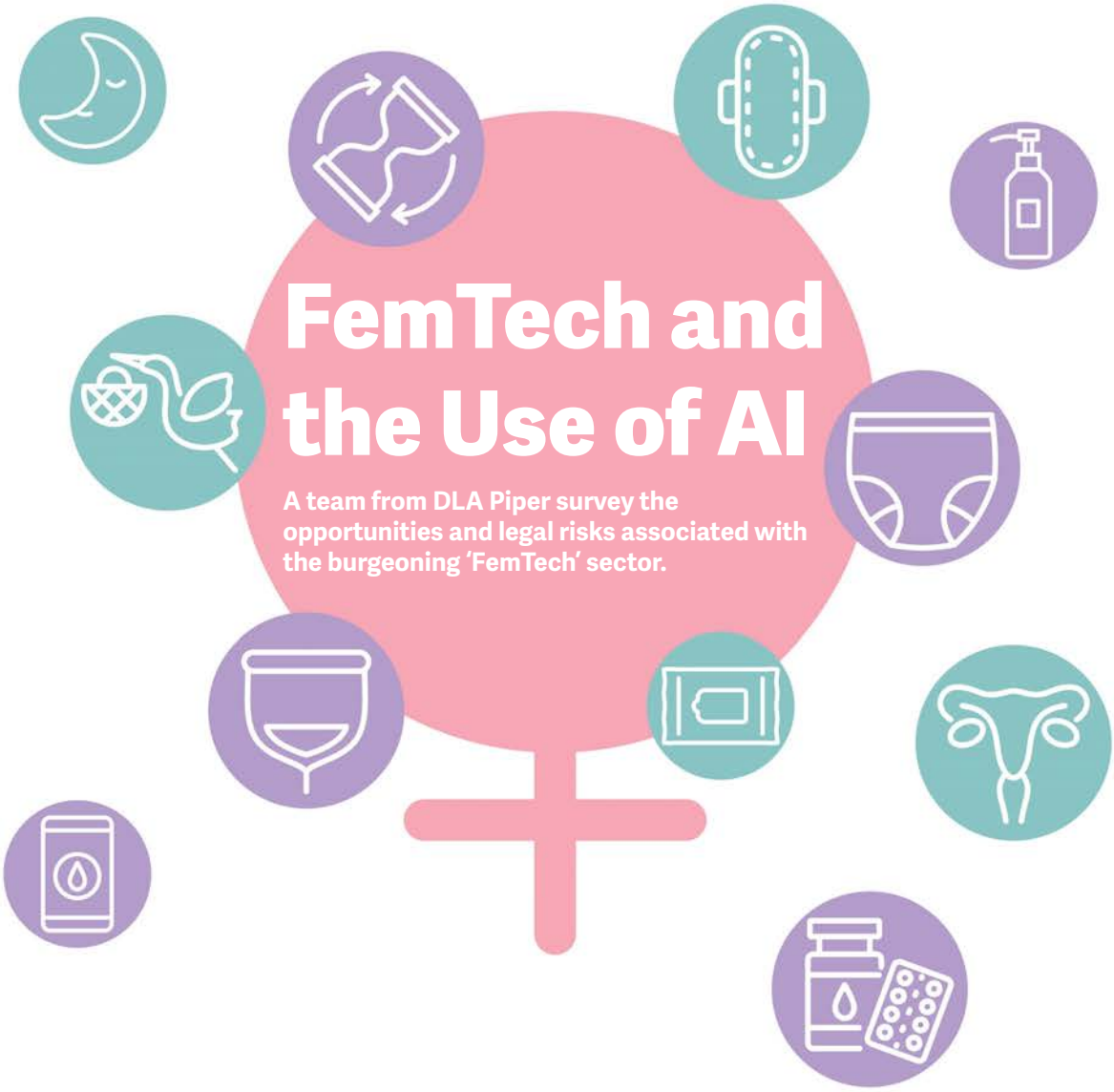
Providers and deployers of high-risk AI systems that are intended to be used by public authorities have six years after the AI Act's entry into force to be compliant. Operators of high-risk AI systems that are on the market or put into service before the general 24 month timeframe will only be regulated under the AI Act if the systems are subject to significant changes in their designs after this timeframe. Again, however, with the exception of prohibited systems.

How to prepare?

While the AI Act has yet to enter into force, it would be prudent for businesses that use and develop AI to start taking active steps to prepare for the new legislative regime and its onerous obligations. Companies should undergo a complete review of their practices to identify any existing or proposed AI elements and ensure that the procedures and measures implemented align with the requirements of the AI Act.

Davinia Brennan, Anne-Marie Bohan, Carlo Salizzo, Deirdre Crowley & Sarah Jayne Janna

Members of the Technology & Innovation Group at Matheson.



FemTech and the Use of AI

A team from DLA Piper survey the opportunities and legal risks associated with the burgeoning 'FemTech' sector.

Due to an exponential growth in the investment in female health and wellbeing, Forbes and Dealroom reported that 2023 saw $1.14bn raised collectively across 120 deals in 'FemTech'. The phrase refers to technology products and services that help to solve the health needs and concerns suffered disproportionately or solely by females. With an increased awareness of women's health issues, evolving societal perspectives and the development of artificial intelligence, the FemTech Landscape Report estimates that the industry will be worth over a trillion dollars by the end of 2027.

Several household global brands and emerging growth companies are looking to empower female users with data and technology to make more informed choices about their health and remove barriers to accessing appropriate healthcare e.g., due to gender biases, stigma, and a lack of funding. Less than 5% of public funded research in the UK is dedicated to the subject of reproductive health, despite it being the cause of health issues for a third of women. Part of this systemic issue may be attributed to a lack of insight or awareness, as women have previously been excluded from clinical trials due to fluctuations in their hormones.

FemTech is helping to address these challenges by providing either free or low-cost subscription-based access to female health and wellbeing information. Examples include period-tracking apps, such as Clue; virtual online clinics like Maven; and fertility-tracking bracelets such as Ava. Some of these technologies can measure and track stress levels, weight, hormonal changes, and menstrual cycles. This generates a lot of data which could help to rebalance the legacy impact of female health being comparatively under-researched. Of course, this data is generally considered "special category" or "sensitive" and is therefore subject to enhanced data protection requirements.

A poll conducted by the UK's data regulator, the Information Commissioner's Office in September 2023 revealed that more than 50% of the women surveyed said that:

- transparency about how their data is used; and
- the security of their data,

are of greater concern than the cost or ease of use of FemTech apps. As an example, it has been reported that some women attempt to conceal their pregnancies from their phones by not buying baby clothes online or using pregnancy apps to avoid being monitored and potentially subject to direct targeted marketing. As such, companies in this space have a significant trust gap to overcome in encouraging women to continue using their online services. The ICO is investigating technologies in this space to identify whether the services are negatively impacting users from a privacy perspective, for example by incorporating confusing privacy policies, storing unnecessary volumes of data, or targeting distressing advertising at users without valid consent.

> **"Less than 5% of public funded research in the UK is dedicated to the subject of reproductive health**

Statistics published by Google Ads showed that conversion rates are typically up to 5 times higher for consented users, which FemTech companies ought to be aware of. This emphasizes the importance of a user-centric design by, for example, embedding legal privacy language in user journeys at the point of data capture which clearly outlines what data will be collected, what it will be used for and whether it will be fed to data brokers in the advertising ecosystem. The idea of sexual health being labelled is uncomfortable, so companies might also consider whether they can conduct advertising without analysing sensitive personal data; recognising there is

a balance between brand loyalty and revenue driven from ads. Period-tracking app Flo appears to be alert to these issues and recently launched an 'anonymous mode' feature. This allows individuals to access the app without inputting personal data such as their name, email address or other identifiers after the topic of reproductive privacy gained global attention following the landmark US Supreme Court case decision to overturn Roe v Wade in 2022.

The UK Government appreciates the need to boost consumer confidence in buying and using tech products. On 29 April 2024, the UK Product Security and Telecommunications Infrastructure Act 2022) came into effect, requiring manufacturers, importers, and distributors of UK consumer connectable, "smart" products to meet minimum security requirements. It applies UK-wide. Many FemTech products are likely to be captured by this new law in one way or another, particularly given the number of FemTech applications available for use via internet-connected smartphones. The Act aims to reduce potential vulnerabilities in security that may result in cyber-attacks; it introduces requirements regarding the complexity of passwords, minimum security update periods, and closer engagement between users and manufacturers on the reporting of any security issues.

Meanwhile, generative artificial intelligence is an unescapable buzzword. In the FemTech space, it is poised to reinvent the industry, as it can analyse vast amounts of unstructured data and identify patterns. One of the more prominent use cases of artificial intelligence is chatbots. Whilst chatbots have been used since the 1960s, with ELIZA being one of the first to pass the Turing test, GenAI can "create new content" and could be leveraged – for example – by AI-virtual health advisors to provide increased awareness of female health concerns. There are unprecedented opportunities for this technology to increase health equity, particularly as the UK government rejected the proposal to roll out mandatory menopause training for GPs last year – despite it being estimated to cost billions annually in productivity loss and healthcare costs.

Some companies are already exploring the use of large/small language models in this space. Any company looking to fine-tune the model would have to ensure that they had permission to use the health data that they input. The model itself is unlikely to constitute personal data; however, to fully leverage AI-powered solutions companies are likely to add wider datasets to improve the accuracy and efficiency of the solution. The solution could be leveraged by individuals who could potentially input their own data and receive personalised recommendations that adapt to the needs of each female throughout the distinct stages of her life. For women suffering from conditions such as polycystic ovary syndrome, a widely reported but underfunded health issue, the predictive capabilities of data-driven systems could forecast risks and empower women to take more proactive responses to their healthcare based on convenient access to real-time insights provided through an app. Importantly, FemTech does not just revolve around menstruation and family planning. AI analysis of mammograms can help with the early detection of breast cancer; personal nutrition plans can be created that are specifically tailored to a woman's health and nutrition needs; and the technology can also help to predict the risk of diseases and genetic

> **"Some women attempt to conceal their pregnancies from their phones by not buying baby clothes online or using pregnancy**

Historically, women have been erased (or incorrectly accounted for) in medical studies and, as a result, this has impacted the extent of medical advice

issues predominately faced by women.

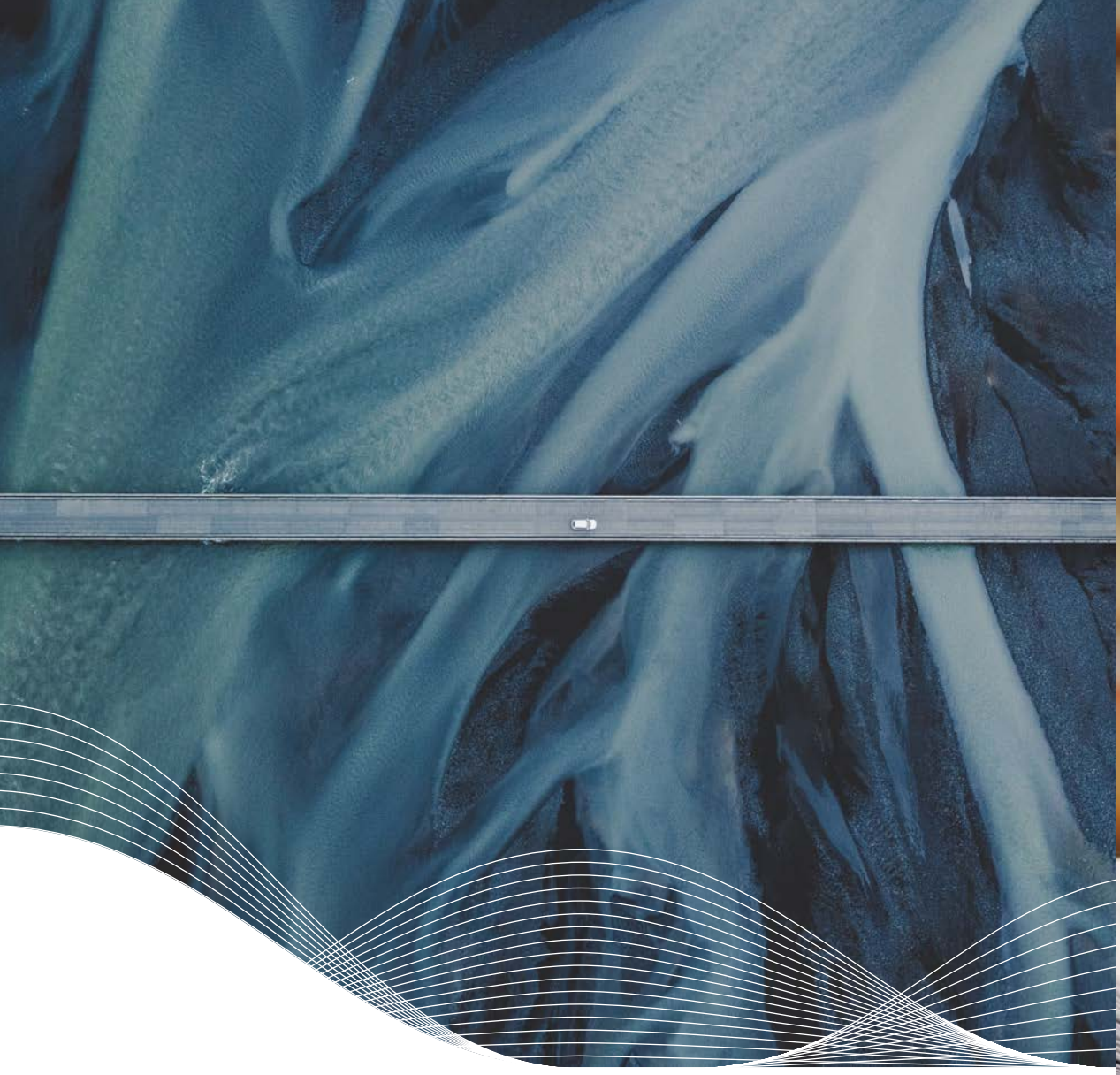
Of course, ensuring accountability, transparency and safeguarding fundamental rights (including privacy) from an ethical standpoint is critical. This processing would certainly require a data protection impact assessment. For FemTech AI solutions that incorporate medical devices or in vitro diagnostics and are deployed in the EU, additional obligations will apply under the EU AI Act – as these are considered 'high-risk." Historically, women have been erased (or incorrectly accounted for) in medical studies and, as a result, this has impacted the extent of medical advice which can be provided around female health issues. For FemTech products to avoid similar, restrictive, outcomes, and thus falling foul of the EU AI Act, manufacturers must ensure that such products are free from bias (or are clear on what bias may remain).

Bias is not limited to gender. Bias can be present in relation to race, ethnicity, religion, sexual orientation, socioeconomic and educational backgrounds. The medical advice received by one woman will not necessarily be relevant for another whose background differs in one (or more) of these respects. Avoiding bias is no mean feat. Data is king – or perhaps that should be "queen." Extensive, diverse, and informative data sets will be required to feed any FemTech solution incorporating AI and educate how to account for potential bias. That will require sufficient funding to allow the data to be properly obtained, assessed, and utilised; as the results are only ever as good as the data inputted. Done correctly, a well-funded FemTech industry demonstrating to consumers that products can help achieve health equity could hugely benefit the wider economy.

The opportunities in this sector are rapidly evolving, and deployed correctly, artificial intelligence can accelerate progress in bridging disparities and improving equal access to healthcare and education. However, the regulations in this space are complex and emerging on a global basis so care must be taken to ensure that data processed is adequately safeguarded.

This article was first published on the DLA Piper blog – Technology's Leading Edge – and is reproduced here with permission.

Linzi Penman, Naomi Pryde, Kirsty McKay & Sarah Cunningham



From garage to global

You can call on our top-ranked team to advise throughout your entire business lifecycle. We meet you where you are, from garage to global. We understand the technology you own and use. And we're where you need us to be – in the world's largest tech hubs. We spot opportunities, track best practices and regulatory trends, and help you succeed.

DLA PIPER

BOOK REVIEWS

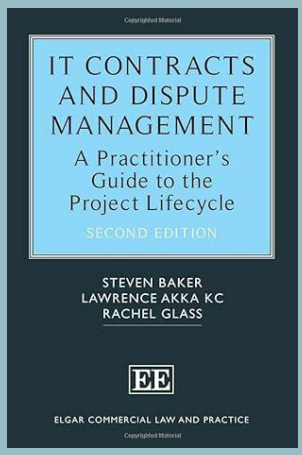
IT Contracts and Dispute Management: A Practitioner's Guide to the Project Lifecycle (2nd Edition)

There are many kinds of books on IT contracts out there. The ones that I came across early in my career contained checklists and sample clauses for a wide range of contracts. Mid-career, I found a 600+ page commentary on standard clauses in IT contracts, contracts for common services like cloud and consultancy, and particular issues such as escrow services and business continuity. These books certainly levelled me up, but I felt like something was missing. Being more a business partner to departments than assigned to churn out individual IT contracts, I wanted to learn more about legal considerations at each stage of the IT project lifecycle.

IT Contracts and Dispute Management: A Practitioner's Guide to the Project Lifecycle is the book that fills this gap for me, a book I wish I had then.

Twenty-one chapters in the book provide guidance on each stage of a technology contract in the form of commentary, from pre-contract to contract negotiation and execution, performance (or non-performance), termination, enforcement, and dispute resolution. In addition it takes into account the latest judicial decisions in relation to technology projects, providing justification for its guidance.

Chapters One, Two and Three discuss the selection of contracting partners, pre-contractual documents such as tenders and letters of intent, project methodology, contract negotiation, as well as types of liability for false pre-contractual statements. Some people may think that it is taboo or negative at this stage to talk about court cases. However I found it helpful that the authors brought in relevant ones



IT Contracts and Dispute Management: A Practitioner's Guide to the Project Lifecycle (2nd Edition) by Steven Baker, Lawrence Akka, Rachel Glass

- **Published July 2023**
- **Hardback, 530 pages**
- **ISBN: 9781839107955**
- **£190.00**
- **Available as an ebook from £152 as well as from Amazon.**

to expand on or illustrate certain points made.

Chapter Four touches lightly on the structure of tech contracts. Chapter Five, on breach of contract, estoppel, waiver, acquiescence, and variation. Interestingly it is titled "Housekeeping", with the authors saying that good project housekeeping will help limit the scope for operational disputes, delays, and a breakdown in the parties' relationship.

In some companies, project management is left completely to the project team to carry out. Nevertheless I suggest that lawyers still go through Chapter Six, which provides guidance on legal issues that may arise such as in relation to change control, and what kind of records ought to be kept.

Delivery and acceptance, testing, benchmarking, service credits, and delay are covered in Chapters Seven to Ten. Chapter Eleven contains a decent number of pages on project rescue which I savoured, as the other books on IT contracts that I read were light on project failure. The chapter talks about common approaches to resolving disputes mid-project, including de-scoping problematic areas, entering into 'heads of terms' or standstill agreements, step-in, and audit, and associated legal issues. My first project failure case was a monster and I could have used this chapter back then in generating options.

Chapters Twelve to Sixteen cover representations when re-baselining, termination rights, settlement considerations, interim dispute resolution, and enforcement of contract. Chapter Seventeen fearlessly tackles the issue of quantification of claims. The usual is covered: the rule against penalties, burden of proof, causation, remoteness. Then the chapter goes more in-depth into possible types of claims on a lost benefit basis, down to whether you can claim expenses incurred in preserving customers' goodwill, say through an improved customer warranty.

It also goes more in-depth into claims on a wasted expenditure basis, monies paid to the supplier for example, and it suggests that claims for out-of-pocket expenditure and consultants' fees which were incurred in reliance on the contract, and which were wasted due to the breach, can be recovered. Other topics covered are claims by the supplier, global claims, suing the tortious measure of damages, particular challenges with long-running disputes, and enforcement of indemnities.

Chapter Eighteen covers exemption and limitation clauses, and the last three chapters discuss dispute resolution forums, disclosure and document preservation, and factual and expert witnesses.

On the whole, this book is a solid reference suitable for newbies to the IT project lifecycle, as well as experienced lawyers given its consideration of recent court decisions. One thing to note is that the book is written from this lens. It does not examine the granular components of IT contracts, and so should be seen as a complement to other kinds of IT contract books not a one-stop shop.

Darren Grayson Chng

Darren Grayson Chng is a data and tech lawyer in Singapore.

High Wire: How China regulates Big Tech and Governs its Economy

Darren Grayson Chng delves into a book examining the peculiar nature of Chinese tech regulation.

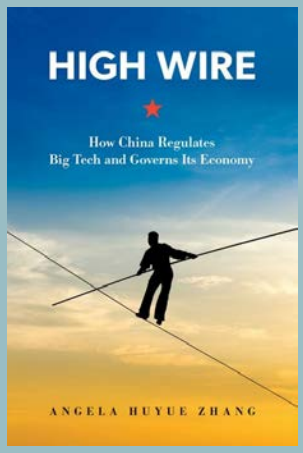
Imagine seven acrobats standing in a line forming a human pyramid – four at the base, two in the middle and one on top. Now imagine them walking a tightrope at height, in that formation. Each needs to maintain his or her own balance. Each needs to synchronise his or her moves with the others. If any one of them sways too much or falls, the entire pyramid will collapse.

The book High Wire says that Chinese regulation shares three similarities with this "pyramid on high wire" act: hierarchy (the structure of regulatory institutions), volatility (the regulatory process' erratic nature), and fragility (the outcome of the regulations). In this book about the intricacies of Chinese tech policy, the "dynamic pyramid model" is used as a framework for analysing China's regulatory system.

Chapter 1 elaborates on "hierarchy" and its four tiers comprising the top leaders, regulatory agencies, firms, and platform participants. The value of the book shines through even at this early stage – readers are not given a Who's Who list with a meek and politically correct analysis of how the Chinese government works. Instead the book discusses the fragmentation of power within the Chinese bureaucracy, the "relentless competition among Chinese regulators vying for policy control" in order to rise to the top level of the Chinese Communist Party and avoid political risk, and how this means that Chinese regulators are inclined towards prioritising their short-term and narrow bureaucratic interests without necessarily considering the broader implications for the whole society..

Chapter 2 discusses the sources of volatility in Chinese tech regulation, walking readers through the 2020-2022 tech crackdown as a case study. Chapter 3 says that the dynamic pyramid model is inherently fragile, primarily due to its tendency for inducing strong side effects and long information lag. Four severe policy challenges that the Chinese leadership faced in recent years, including China's response to Covid-19, are raised as examples.

In the next Part of the book, the dynamic pyramid model is applied to the three major



High Wire by Angela Huyue Zhang

- **Published June 2024**
- **Hardback, 432 pages**
- **ISBN: 9780197682258**
- **£25.99**

pillars of Chinese tech regulation: antitrust, data, and labour regulation. Readers are given information on the landscape in each of these three areas, how it was shaped by the tech companies, and the challenges faced by the government. The book then examines how interactions between the four key actors in the regulatory process led to the regulatory cycles experienced by Chinese tech companies, and offers predictions on the future trajectory of enforcement.

Chapters 7 and 8 examine how Chinese tech companies self-regulate in the shadow of the dynamic pyramid model. Chapters 9 and 10 compare China's crackdown on tech with the approaches of the US and Europe, and assess the impact to China. The last chapter discusses China's regulation of generative AI, using the dynamic pyramid model to analyse the key actors' involvement in the policymaking process.

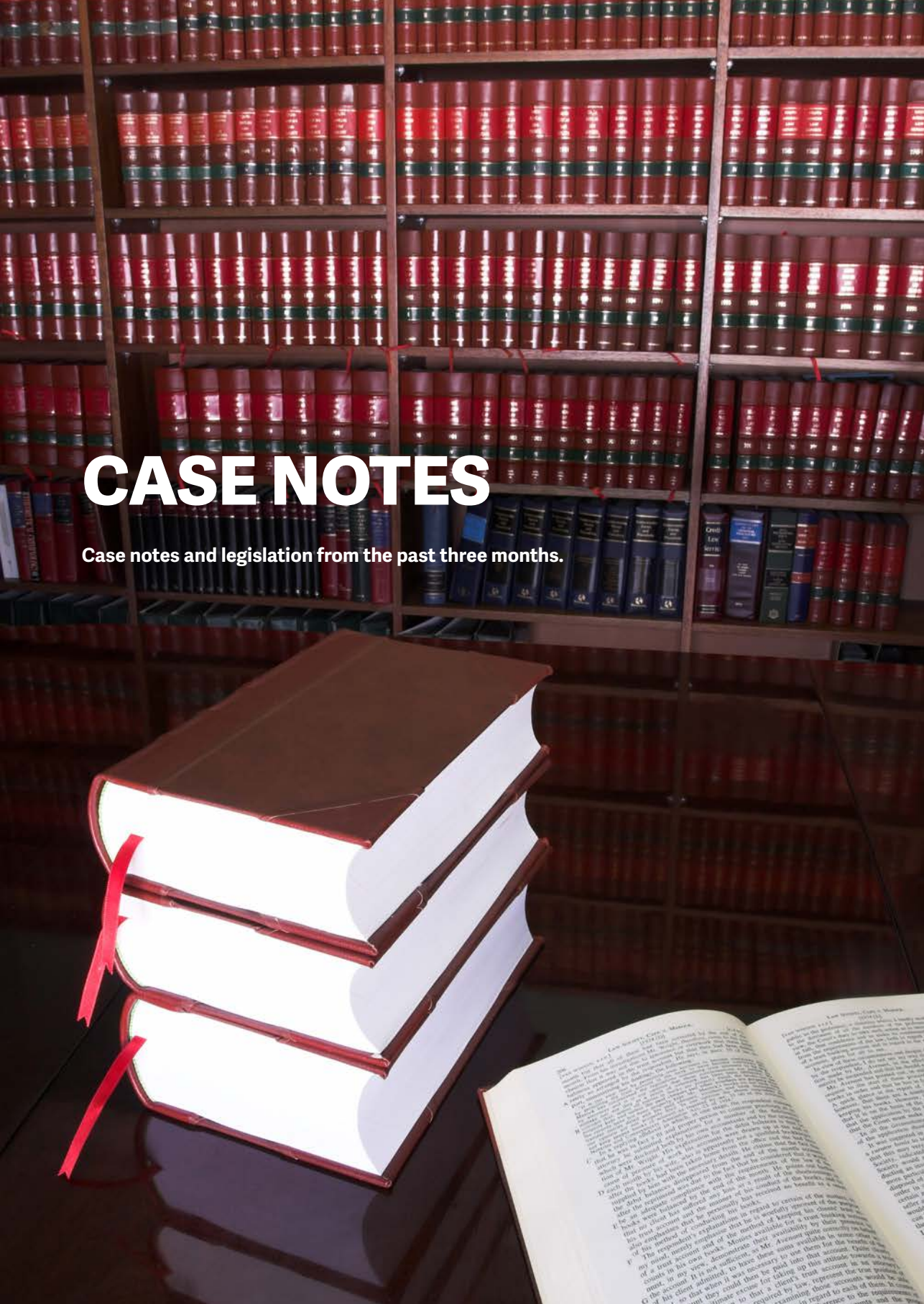
China is an enigma. Anyone who has been trying to crack it and understand policymaking in China and its regulatory approach, including its swings between onerous and lenient, should experience several "aha" moments while reading High Wire. The writing is clear and simple. You do not need much prior knowledge of China in order to appreciate the analysis. I really enjoyed reading this book.

Darren Grayson Chng

Darren Grayson Chng is a data and tech lawyer in Singapore.

CASE NOTES

Case notes and legislation from the past three months.



Advocate General gives opinion on scope of Software Directive's computer program protection

Advocate General Szpunar (AG) has issued an Opinion in *Case C-159/23: Sony Computer Entertainment Europe Ltd v Datel Design and Development Ltd and others*.

The Advocate General has expressed the opinion that Article 1(1) to (3) of Directive 2009/24/EC on the legal protection of computer programs (Software Directive) must be interpreted as meaning that the protection conferred by the Directive does not extend to the content of the variables which the protected computer program has transferred to the RAM of the computer and uses in running it, in the situation in which another program operating at the same time as the protected computer program changes that content, without, however, the object code or the source code of the latter program being changed.

The German courts had referred the following questions to the CJEU in the context of Sony's proceedings against Datel, who developed and distributed software and add-on devices to Sony consoles, which allowed the user to use both the console and the games in ways not intended by Sony. Among others, they allowed interference with the gameplay:

- Is there an interference with the protection afforded to a computer program under Article 1(1) to (3) of Directive 2009/24/EC in the case where it is not the object code or the source code of a computer program, or the reproduction thereof, that is changed, but instead another program running at the same time as the protected computer program changes the content of variables which the protected computer program has transferred to the working memory and uses in the running of the program?
- Is an alteration within the meaning of Article 4(1)(b) of Directive 2009/24 present in the case where it is not the object code or the source code of a computer program, or the reproduction thereof, that is changed, but instead another program running at the same time as the protected computer program changes the content of variables which the protected computer program has transferred to the working memory and uses in the running of the program?

The AG said that:

- the value of the variables is not an element of a computer program's code. They are merely data, external to the code, which the computer produces and reuses when running the program. The data does not exist at the moment that the program is created by its author or when it is loaded into the computer's memory, as it is only generated while the program is running. Therefore, it does not enable the program, or even a part of it, to be reproduced. The Software Directive only protects computer program code, as it is the code, both the source code and the object code, that enables the program to be reproduced.
- the value of the variables does not satisfy the criterion of originality set out in Article 1(3) in the Software Directive, as it is not the program author's own intellectual creation. With regards to Sony's video games, the value of the variables at issue was the result of the progress in the game and, ultimately, the result of the player's behaviour. The author designed the categories of the variables that are recorded as well as the rules whereby their value is determined in the course of the game. However, that value itself escapes the author's creative control, since it depends on factors which cannot be foreseen in advance, such as the player's behaviour. Therefore, it cannot enjoy copyright protection.
- the value of the variables generated by the program is merely transitory, temporary and provisional, since it can change while the program is running and is often reset to zero when that program is next run. In addition, an element such as the value of the variables

generated by a computer program when it is running, which is not only ephemeral but also constantly changing, both while that program is running and upon each subsequent time that it is run, cannot be identified with sufficient objectivity and precision, especially as those changes are determined not by the author's creation but by external factors, such as the actions of the users of the work.

Upper Tribunal issues ruling in ICO Experian case

The Upper Tribunal has dismissed the ICO's appeal in *ICO v Experian [2024] UKUT 105 (AAC)*.

Experian is a well-known credit reference agency. It holds and processes data relating to over 51 million people living in the UK (effectively the entire adult population). It also processes the data of UK residents to provide marketing services which it sells to its third-party clients.

The ICO was concerned about the extent and nature of Experian's data processing in the light of the transparency requirements of the GDPR and issued Experian with an enforcement notice. Experian appealed to the First Tier Tribunal, which allowed large parts of its appeal and the enforcement notice was scaled back. The ICO in turn appealed to the Upper Tribunal, which has now issued its ruling.

The appeal was primarily concerned with the principle of transparency, both the overarching duty in Article 5(1)(a) and the more detailed obligations in Article 14 GDPR. It was common ground between the parties that the provision of transparency in the processing of personal data is foundational to data subjects' rights. The transparency principle has not been the subject of any detailed judicial consideration by the Upper Tribunal or by the appellate courts to date.

The ICO alleged that the FTT's decision involved multiple errors of law and that it failed to address, or adequately address, several relevant issues. Experian contended that the FTT's decision should be upheld and that the appeal essentially sought to re-litigate unassailable findings of primary fact and evaluative assessments.

The Upper Tribunal dismissed the ICO's appeal.

It rejected each of the alleged errors of law that the ICO argued had been made. It said that the FTT's decision was neither well-structured nor particularly well-reasoned, but the Upper Tribunal was satisfied that, applying the approach that the appellate authorities required it to take, there was no error of law in the FTT's approach.

The Upper Tribunal also decided that, whether the ability to access the information prescribed by Article 14 via a series of hyperlinks was sufficient to satisfy the exception in Article 14(5)(a) that applies where a data subject already "has" that information, was a question of fact and degree. In doing so, the panel addressed the secondary basis on which the ICO put its case, that is, that the FTT's decision was inadequately reasoned. Having undertaken a significant amount of inferential work, the panel was satisfied that the FTT's reasons were not so inadequate as to amount to an error of law.

The Upper Tribunal rejected the ICO's submission that the FTT did not have regard to or determine the ICO's concerns regarding the layering of the information provided on Experian's Consumer Information PortaI. It was for the FTT to make its own evaluative assessment as to whether information about Experian's processing was sufficiently prominently displayed on the Portal; it did make that assessment and decided that it was sufficiently prominently displayed.

The Upper Tribunal also said that it was apparent from the terms of the enforcement notice that the ICO thought that the legitimate

interest assessments should be reconsidered because it believed that Experian's processing was intrusive, non-transparent and harmful. However, the FTT had rejected each of these propositions and there was no challenge to their conclusion in terms of the relatively innocuous nature of the processing involved. Moreover, the Upper Tribunal dismissed the grounds of appeal that challenged the FTT's findings on intrusiveness and on transparency. It followed that the FTT's decision contained a reasoned rejection of the ICO's case, although it could have been clearer.

The ICO has published a statement on the decision, saying it will "take stock of [the] judgment and carefully consider our next steps, including whether to appeal".

High Court considers whether cap on liability was single, aggregate cap or multiple caps

High Court considers whether cap on liability was single, aggregate cap or multiple caps

The High Court has issued its judgment in the case of *Tata Consultancy Services Ltd v Disclosure and Barring Service [2024] EWHC 1185 (TCC)*.

The case arose in the context of a contract for the digital transformation of the services of a public body. As is often the case with digital projects, it did not go well. There were immediate challenges with transition, leading to delay and revision of milestones. DBS said the system had significant defects, and each party blamed the other for delays.

The liability clause provided that its "aggregate liability":

"in respect of all other claims, losses or damages, shall in no event exceed £10,000,000 (subject to indexation) or, if greater, an amount equivalent to 100% of the Charges paid under this Agreement during the 12 month period immediately preceding the date of the event giving rise to the claim under consideration less in all circumstances any amounts previously paid (as at the date of satisfaction of such liability) by the CONTRACTOR to the AUTHORITY in satisfaction of any liability under this Agreement."

The court had to decide if the limitation of liability clause provided a single, aggregate cap that applied to all claims rather than multiple, separate caps.

The court's decision

The High Court said "Clause 52.2.6 is far from a model of clarity" and held that it provided for a single cap rather than multiple caps. This was because:

- the words 'the aggregate liability … in respect of all other claims, losses or damages, shall in no event exceed' were a clear indicator that the clause was setting out the total liability notwithstanding however many claims, losses or damages might exist;
- the simple language of 'per claim' was absent;
- whilst the 'claim under consideration' within the alternative (if greater) to the figure of £10,000,000 suggested that more than one claim may be under consideration, the clause then sought to net off sums previously paid. This meant that the capped sums calculated in accordance with the clause were not intended to be additive (although it might have been that a later claim considered would give rise to a larger overall cap being applied than had previously been calculated by reference to an earlier claim).
- even without the express 'netting off' process, the court favoured a construction which implied a reference to the first claim because the clause was intended to provide an aggregate liability figure for all other claims. However, this was not necessary, and it might have been that a later claim than the first would set the cap. The effect of this

would be that the alternative cap would be, in effect, the charges under the contract in 12 months before any claim brought giving rise to the greatest cap. However, the court said that determining the precise mechanics of this was unnecessary because DBS had not brought a claim by reference to a cap calculated in accordance with the alternative possibility.

Last year the court considered a similarly unclear clause in *Drax Energy Solutions Ltd v Wipro Ltd [2023] EWHC 1342 (TCC)* and decided that similarly unclear drafting should be interpreted as a single cap. In that case, the contract had included drafting often encountered in IT contracts whereby the liability cap would flex, up and down, to match the delivery risk profile and charges received over time, with charges being assessed over a rolling period rather than the whole term.

In addition, in the Tata case, the limitation clause sought to exclude liability for loss of profits. Tata had claimed for loss of revenue. It argued that anticipated cost savings were not realised because of customer delays and so net revenue was reduced. On the other hand, DBS argued that this claim was actually a claim for loss of profits by another name and consequently was excluded by the contract. The court agreed with DBS and referred to the Court of Appeal's judgment in *Soteria Insurance Ltd v IBM United Kingdom Ltd [2022] EWCA Civ 440*, where it found that an exclusion of loss of profit, revenue and savings did not exclude a claim for wasted expenditure.

Court authorising access to telephone records must have discretion to refuse such access

The Court of Justice of the EU has recently ruled in *Case C-178/22 | Procura della Repubblica presso il Tribunale di Bolzano*. Under Italian law, the offence of aggravated theft is one of the offences that may justify obtaining telephone records from a provider of electronic communications services if a court authorises it. The Court of Justice considers that access to such records can be granted only to the data of individuals suspected of being implicated in a serious offence, and says that member states must define "serious offences". However, the court responsible for authorising that access must be entitled to refuse or restrict that access where it finds that the interference with the fundamental rights to private life and to the protection of personal data which such access would constitute is serious, while it is clear that the offence at issue is not a serious offence in the light of the societal conditions prevailing in the member state concerned.

National authority can access civil identity data linked to IP addresses to investigate online copyright infringement

In *La Quadrature du Net and others v Premier Ministre, Ministère de la Culture (Case C-470/21)*, the Court of Justice of the EU ruled that in certain circumstances a national public authority responsible for combating online counterfeiting may access civil identification data based on an IP address without previously seeking approval from a court or independent authority. The French

courts referred a question on identifying those suspected of online copyright infringement. The CJEU considered if Article 15(1) of the E-Privacy Directive (2002/58/EC) (alongside the Charter of Fundamental Human Rights) prevented a French decree claimed to authorise disproportionate access to connection data in relation to suspected online copyright offences that are not serious, without being first reviewed by a judge or independent authority.

Patents Court considers scope of FRAND licence and termination of obligation of full and frank disclosure

In *Lenovo Group Ltd and others v InterDigital Technology Corporation and others (Re Applications) [2024] EWHC 1036 (Pat)* the Patent Court considered a new phase of the continuing litigation between InterDigital and Lenovo about a licence for Standard Essential Patents (SEPs) Lenovo had obtained leave to serve out on InterDigital. InterDigital applied to have the service out set aside. It said that Lenovo's statement of claim appeared to include a claim to a FRAND licence which would cover non-SEP patents (Portfolio Licence). Interdigital said this lacked merit as it had no legal obligation to grant such a licence. The court said that InterDigital has made several detailed criticisms of drafting of the pleadings, but many of those were just drafting criticisms that overlooked the fact that the pleading as a whole disclosed a claim for a Portfolio Licence which had a reasonable prospect of success. The court rejected the argument that a claim for a Portfolio Licence failed the merits test. Interdigital also argued that the application to serve out lacked the required full and fair disclosure but the court said that while Lenovo could be criticised for not notifying the court of the relevant breaches earlier than it did, it did not agree that the appropriate sanction was to set aside the order for service out.

High Court rules on Bitcoin identity issue

The High Court has ruled in *Crypto Open Patent Alliance v Wright [2024] EWHC 1198 (Ch)* that the defendant Dr Wright was not: the author of the Bitcoin White Paper (which described the Bitcoin system and was in October 2008). The court also ruled that Dr Wright was neither the author of the initial versions of the Bitcoin software; nor the person who adopted or operated under the pseudonym Satoshi Nakamoto in the period between 2008 and 2011. Finaly, he was not the person who created the Bitcoin system. The judge said "I am entirely satisfied that Dr Wright lied to the Court extensively and repeatedly. Most of his lies related to the documents he had forged which purported to support his claim. All his lies and forged documents were in support of his biggest lie: his claim to be Satoshi Nakamoto." The judgment also notes that remote links to the proceedings had been provided (on individual request) to over 400 people from all over the world. By the conclusion of the trial, that number had risen to over 1100, reflecting the wide interest.

Amazon's request to suspend its obligation to make an advertisement repository publicly available is rejected

The Vice President of the Court of Justice has ruled in *Case C-639/23 P(R) European Commission v Amazon Services Europe Sàrl*.

In April 2023 the Commission adopted a decision under the Digital Services Act which designated Amazon Store as a very large online platform. Among other things, this meant that Amazon Store is obliged to make publicly available a repository containing detailed information on its online advertising under Article 39 of the DSA.

Amazon sought the annulment of that decision before the General Court of the EU. It had also made an application for interim measures. In September 2023, the President of the General Court ordered that the Commission's decision be suspended to the extent that Amazon Store was required to make the advertisement repository publicly available.

The Commission appealed.

The Vice-President of the Court of Justice has set aside the part of the General Court order suspending the Commission's decision in so far as it concerns the advertisement repository. He said that the Commission had not had the opportunity to comment on the arguments Amazon had made to the General Court which was in breach of the principles that the parties should be heard. The Commission did present its arguments to the Court of Justice so the Vice President of the Court of Justice has given final judgment in the dispute and dismissed the application for interim measures.

The Vice-President of the Court considered that Amazon's argument that the obligation introduced by the EU legislature to make an advertisement repository publicly available unlawfully limited its fundamental rights to respect for private life and the freedom to conduct a business, could not be regarded as irrelevant or lacking in seriousness.

Furthermore, in the absence of a suspension, it was likely that Amazon would suffer serious and irreparable harm before the intervention of any judgment annulling the Commission's decision.

However, he also said that those findings are not decisive in themselves., concluding that the Commission's interests in the full implementation of the DSA outweighed Amazon's interests. Applying Article 39 in the interim would not have an adverse effect Amazon's existence or long-term development. Amazon's revenue from advertising represented only 7% of its overall revenue. Contrasting with this, the DSA is a central element of EU policy in the digital sector. If its rules were not applied, this would delay achieving the DSA's objectives and could affect competition by making Amazon subject to different rules than other players in the digital sector.

Public statement by social network user about sexual orientation means data is public but that does not mean it can be used for personalised advertising

The Advocate General has delivered his opinion in *Case C-446/21 | Schrems*.

In 2018, Meta Platforms Ireland started using new Facebook terms of service in the EU. Consent to those terms is required to sign up for, or access, Facebook's accounts and services. Mr Maximilian Schrems (S) a Facebook user and well-known activist in the field of data protection, accepted these terms.

Following that, he said he had regularly

received advertisements directed at homosexuals and invitations to corresponding events. He argued that those advertisements were not based directly on his sexual orientation, but were based on an analysis of his particular interests.

S was dissatisfied with the processing of his data which he considered to be unlawful and so brought an action before the Austrian courts. Subsequently, during a panel discussion, he publicly referred to his homosexuality, but did not publish anything on his Facebook profile.

The Austrian Supreme Court referred the issue to the CJEU, asking if:

- a network such a Facebook may analyse and process all the personal data available to it for an indefinite period to produce targeted advertising; and
- if a statement made by a person about their sexual orientation as part of a panel discussion permits the processing of other data concerning that topic to offer that person targeted advertising.

First question: Advocate General Athanasios Rantos proposes that the Court should rule that the GDPR prohibits the processing of personal data for targeted advertising without a time restriction. The national court should consider the principle of proportionality and assess the extent to which the data retention period and the amount of data processed are justified having regard to the legitimate aim of processing that data for personalised advertising.

Second question: The Advocate General takes the view, subject to the findings of fact to be made by the Austrian Supreme Court, that the fact that S has made a statement concerning his own sexual orientation during a panel discussion open to the public may constitute an act by which he 'manifestly made public' that information under the GDPR. While data concerning sexual orientation falls into the category of data that enjoys special protection and the processing of which is prohibited, that prohibition does not apply when the information is manifestly made public by the data subject. Nevertheless, this does not in itself permit the processing of that data for personalised advertising.

Patents Court refuses interim declaration that draft licence is FRAND

The Patents Court has recently issued its judgment in the case of *Lenovo Group Limited and others v Interdigital Technology Corporation and others* [2024] EWHC 596 (Ch). It refused Lenovo's application for a declaration that a proposed draft interim licence of various cellular standard essential patents (SEPs) would be fair, reasonable and non-discriminatory (FRAND). The judge saw "real difficulties in determining on an interim basis that the Interim Licence is FRAND. I consider that question likely to be capable of determination only on a final basis. That in itself is a strong indication that the Interim Declaration should not be made. Even if that objection can be overcome, I consider I should make the Interim Declaration only if I have a high degree of assurance that the Interim Licence is FRAND…I do not have that high degree of assurance." The court also refused Interdigital's application to stay part of the proceedings which were argued to overlap with German proceedings with respect to its various SEPs.

Patents Court rules on consequential matters following FRAND judgment

The Patents Court has ruled in the case of Optis Cellular Technology LLC and others v Apple Retail UK Ltd and others [2024] EWHC 197 (Ch). This follows judgment in the trial relating to the terms of a FRAND licence to Apple for Standard Essential Patents (SEPs) owned by Optis. In a further trial the court considered issues consequential to the judgment. The court had to consider the degree of redaction required in the public version of the judgment for reasons of confidentiality. A balancing approach was appropriate between "trade secrets" and open justice and some issues were trade secrets. However, other provisions in lump sum licences for which redactions had been sought did not come within definition of trade secrets and so the court refused the redactions. In addition, "non-discriminatory" implied a degree of transparency. People who were not currently party to the proceedings could apply to have the redactions in the judgment lifted. The judge also made it clear that the SEP owner cannot hedge its bets by commencing parallel proceedings and hoping to then choose the outcome most favourable to it.

CJEU issues ruling in IAB Europe referral about auctioning of personal data for advertising purposes

The CJEU has issued its ruling in Case C-604/22 | IAB Europe.

Companies, brokers and advertising platforms, which represent thousands of advertisers, can bid in real time, behind the scenes, to acquire online advertising space to display advertisements which are tailored to a user's profile. However, before such targeted advertisements can be displayed, it is necessary to obtain the user's prior consent to the collection and processing of their personal data (concerning, for example, their location, age and search and recent purchase history) for purposes such as marketing or advertising, or with a view to sharing the personal information with certain providers. The user can also object to that collection and processing.

IAB Europe is a Belgian non-profit association which represents undertakings in the digital advertising and marketing sector at European level. IAB Europe has created a solution which it argues is compliant with the GDPR. Users' preferences are encoded and stored in a string composed of a combination of letters and characters referred to as the Transparency and Consent String (TC String), which is shared with personal data brokers and advertising platforms so that they know what the user has consented or objected to. A cookie is also placed on the user's device. When they are combined, the TC String and the cookie can be linked to that user's IP address.

In 2022, the Belgian Data Protection Authority ruled that the TC String constitutes personal data under the GDPR and that IAB Europe had been acting as data controller without fully complying with the GDPR. The Belgian regulator imposed various corrective measures as well as an administrative fine. IAB Europe appealed that decision to the Belgian courts, which referred the case to the Court of Justice for a preliminary ruling.

In its judgment, the Court of Justice confirmed that the TC String contains information concerning an identifiable user and therefore constitutes personal data under

the GDPR. Where the information contained in a TC String is associated with an identifier, such as the IP address of the user's device, that information may make it possible to create a profile of that user and to identify him or her. The CJEU also said that IAB Europe must be regarded as a 'joint controller' under the GDPR. Subject to the verifications which are for the Belgian courts to carry out, IAB Europe appears to exert influence over data processing operations when the consent preferences of users are recorded in a TC String, and to determine, jointly with its members, both the purposes of those operations and the means behind them. However, the CJEU also said that without prejudice to any civil liability provided for under national law, IAB Europe cannot be regarded as a controller under the GDPR, in respect of data processing operations occurring after the consent preferences of users are recorded in a TC String, unless it can be established that IAB Europe has exerted an influence over the determination of the purposes and means of those subsequent operations.

Court of Appeal confirms terms of lottery instant win game were enforceable

The Court of Appeal has issued its ruling in the long-running saga of Ms Parker Grennan v Camelot UK Lotteries Ltd [2024] EWCA Civ 185.

Facts of case

The appellant P played an instant win game on the National Lottery website, which was operated by Camelot at the time. The game display screen displayed the message 'match any of the WINNING NUMBERS to any of "YOUR NUMBERS" to win PRIZE'.

When P opened the account, she was required to accept various terms and conditions, which she did by clicking to tick a box to 'accept terms and conditions' and clicking 'confirm'. There was a link to the account terms at the bottom of the page, which in turn contained hyperlinks to other terms and conditions and resources.

A random number generator pre-determined the outcome of the game. The pre-determined outcome in this case was a win of £10. The software included animations, which, if enabled, meant that the winning pair of numbers would turn white and flash in a green circle.

P played the game with the animations enabled. The random number generator selected a number corresponding with prize tier 27, which meant that her ticket had won her £10. After the final number was clicked, her screen came up with an image with two flashing number 15s (the bottom one displayed a prize of £10 underneath it) and a message at the top of the screen saying "CONGRATULATIONS! You have won £10". However, she noticed that there also appeared to be two matching number 1s in the upper and lower sections of the screen (although they were not flashing), and 1 was the number to which the top prize of £1 million was ascribed. She took a screenshot.

The cause of the display of the matching number 1s was a coding error in the Java software responsible for the animations. Camelot's database recorded a win of £10; Camelot credited the account with £10 and told P that she had won £10. P applied for summary judgment, claiming £1m.

First instance decision

The first instance court held that:

- The terms were properly incorporated;
- None of the terms was contrary to the Unfair Terms In Consumer Contracts Regulations 1999 (the predecessor legislation to the

Consumer Rights Act 2015).

- P's arguments as to the proper construction of the terms were rejected.

P appealed the first instance decision.

Court of Appeal decision

The Court of Appeal unanimously dismissed the appeal. It said that when a court is considering the incorporation of contractual terms, it needs to consider if the operator has carried out reasonable steps to adequately bring the various terms and conditions to the player's attention. There was no necessity for the operator do "everything in its power" to require a user to read the terms.

Consumers can be given sufficient opportunity to read the terms by providing hyperlinks to the terms or a drop-down menu. P had argued that consumers should be forced to scroll through the terms before being able to click "accept" but the Court of Appeal said that this was likely to cause the player to give up, or scroll to the end and accept without reading the terms.

The first instance court was correct to find that anyone playing an instant win game would expect there to be rules governing how the game was played and how a win was determined. These were in the Game procedures, which explained that the outcome of a play was pre-determined. There was nothing in Camelot's terms which was unduly onerous or unusual. Therefore, there was no requirement for Camelot to specifically signpost any of the terms to incorporate them.

The court also considered if, contrary to the requirement of good faith, any term caused "a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer". According to the Court of Appeal, Camelot's terms were clearly drafted and well signposted through hyperlinks. Its rules made clear that the prize was the one that showed in Camelot's database. The Court did note that the dispute resolution clause, which provided that Camelot could conduct a validation exercise in relation to claimed prizes, did create an imbalance between the parties, but this was not contrary to the requirement of good faith. Anyway, Camelot did not need to rely on this clause because P had not won £1 million under its rules.

P tried to rely on the phrase 'Match any of the WINNING NUMBERS to any of YOUR NUMBERS to win PRIZE' as the only relevant contractual term. The Court of Appeal disagreed. It said that if P had read the game procedures, it would have been clear to her that to win the prize, the matching numbers had to turn white and flash, the amount of the win would be displayed. In any event, this should have been obvious to a player even without reading the game procedures.

The rules of the game set out that the outcome of the play was that recorded in Camelot's database, which was a win of £10. Therefore, P did not win £1 million.

NEWS REVIEWS

Missing your news hit? Catch up with all the news reported on scl.org by reading our monthly news reviews available to download on the site now.

SCL Events Diary 2024

JULY

- **Generative AI and Deepfakes: Understanding the Illusion**
  Tuesday 2 July , 4.00 - 6.30pm. Herbert Smith Freehills.
- **SCL AI Group Webinar: EU AI Act Contractual Clauses**
  Wednesday 10 July , 1.00 - 2.00pm. Online.

OCTOBER

- **Annual AI Conference**
  Tuesday 8 October, 9.30 - 5.00pm. Central London.

NOVEMBER

- **Tech Fundamentals: a structured primer on core tech for tech lawyers**
  Wednesday 6 November, 9.30 - 5.00pm. Bristows LLP.

SCL Corporate Supporter Scheme

The Society for Computers and Law (SCL) is a registered educational charity. We receive no grants or subsidies but rely on the support and engagement of our members and the wider tech law community in order to fulfil our mission of delivering 'tech law for everyone'.

Your support of SCL means that the Society can meet its charitable objectives, maintain its student schemes, and continue to educate and support our community.

In return you receive top notch tech law training, access to our ever-growing online resources and expert opinion and the opportunity to share ideas with peers and thought-leaders and help shape the future of your sector.

SCL continues to go from strength to strength with the dedication and hard work of all involved and the tremendous support of the membership and community. To help the Society grow and continue to serve the tech law sector we are introducing the ***"SCL Corporate Supporter Scheme"***.

Why should you become an SCL Corporate Supporter?

As an SCL Corporate Supporter you will be helping the Society fulfil its charitable aims by funding our initiatives to educate lawyers and the wider public about computer law and legal technology.

Our Supporters are organisations with strong links to the sector and a track record in developing relevant ideas and services and so it is a prestigious badge for you at a time when regulation of the sector has never been so important.

What you get as a Supporter?

You will also be able to work with us to increase the awareness of your organisation as a thought leader in the sector through these channels:

- Acknowledgement as a Supporter on the SCL website including 200 words on what you offer, a contact link and links to your website. The page is signposted from the homepage of the website and on all our update emails.
- A listing in the "Supporters" pages of our online magazine, Computers & Law
- Distribution of promotional materials free of charge at SCL events on a first come first served basis. Details will be emailed when events are organised.
- First choice to exhibit at/ sponsor selected SCL events (there may be an additional event related cost) on a first come first service basis where exhibition places are limited
- The ability to book places for clients on SCL events at member rates
- An announcement on scl.org of your status when you take up or renew your support linking to a chosen product news story placed on our Supporters blog
- A 'Supporter's message' to all members when you take up / renew your support
- Attendance at the Supporters event held each year

How much does it cost?

We have four levels of support available:
Platinum Supporter = £10,000 pa
Gold Supporters = £5000 pa
Silver Supporters = £3000 pa
Bronze Supporters = £1000 pa

If you are interested in becoming an SCL Corporate Supporter please contact
Maddie Southorn
maddie.southorn@scl.org.

Society for Computers & Law
The leading educational charity for the tech law community
www.scl.org

SCL Tech Law Essentials Programme: T2

All modules online and on-demand. Delivered to your desktop in 2024 – available to pre-order now.

Are you ready to supercharge your IT Law career? Join SCL for a transformative journey with the all-new Tech Law Essentials Programme and stay ahead in the dynamic world of tech law.

A Decade of Excellence:

It's been 10 incredible years since the introduction of the SCL Tech Law Essentials programme, an innovative training course that has shaped the careers of countless SCL members. We can now proudly share the next evolution of this programme – T2.

What to Expect:

T2 is designed to equip you with the latest insights and skills, addressing new legal challenges and offering solutions to emerging issues. We've preserved the essential knowledge while infusing fresh perspectives, making this programme indispensable at every stage in your tech law career, either as an introduction or a refresher.

What Makes T2 Stand Out:

- **Expert faculty:** Each event is shaped and delivered by experts in the field, thought-leaders who have a thorough understanding of the topic and passion for sharing their knowledge and experience. Speakers are carefully chosen to ensure a balanced viewpoint covering legal and commercial perspectives.
- **Keeping it Relevant** - The programme is consistently reviewed and updated to make sure we offer you the very latest in tech law training.
- **Flexible and available on-demand** - in 2024 and beyond. You choose how to engage with the events and design a curriculum that suits you and your practice. The modules can be purchased individually or as a complete package so you can take the course in your own time, in any order and wherever you are.
- **Comprehensive content:** Covering crucial aspects of IT Law Practice, T2 ensures you're well-versed in the essentials.
- **Ongoing access:** Stay connected with the course material even after completion. Once you have purchased a module or modules you have permanent access to the materials and can view them at any time.
- **Certificate of achievement:** Validate your expertise with an official certificate of completion from SCL.
- **Exceptional value:** Top-notch education at an unbeatable price.

The Modules:

The Context of Tech Law

Module 1. Commercial Context of IT Law Practice - Advising Tech Customers.

Module 2. What is "Cloud"?

Module 3. Navigating Cyber Risk

The Tech Law Legal Environment

Module 4. IP in IT Law: IP rights in technology and data

Module 5. Online Trading, Digital Media & Internet Law

Module 6. Data Protection and IT

Module 7. UK Internet and telecoms regulation.

Module 8. EU Regulated Tech Environment

Module 9. The International – Multi Jurisdictional IT Law:

Module 10. ESG

Tech Law Contracts and Practice

Module 11. Introduction to the most common technology agreements

Module 12. Outsourcing

Module 13. IT Disputes Law and Practice

Module 14. IT Corporate Transactions and IT Law in Corporate Transactions

Module 15. Projects, Public Sector and Procurement

Module 16. Soft Skills

Module 17. The Annual Zeitgeist

Ready to Elevate Your Career?

Don't miss your chance to be part of the future of tech law. Join the SCL T2 Programme today and become the legal expert that tech companies rely on! Your journey to tech law excellence begins here with SCL T2.

Learning and Development organisation level course roll out available for organisations. Please email the SCL Team at hello@scl.org to discuss this in more detail..

Please email the SCL Team at hello@scl.org to discuss this training programme in more detail.

SCL
Society for Computers & Law
The leading educational charity for the tech law community
www.scl.org