OLIVIA WHITCROFT

“It’s a good idea to keep an eye on the legal pipeline and start planning how it could impact you”

If there’s one thing that stays the same in law, it’s that the law is always changing. And that’s even more true if your specialism involves technology

Changes to the law can be annoying. You’ve just got your head round the rules, built them into your systems and are sitting back watching everything run smoothly. Then a new law comes along that pulls you back to square one.

A key driver for legal change is technology. Technological advances change the way in which we do stuff, and the roles and perspectives of the different players. Existing laws are not always equipped to address the challenges and uncertainties that arise.

Right now, I’m trying to keep track of several legal developments. Proposed new data protection laws aim to clarify provisions that are impeding the use of new technologies. Applying existing intellectual property law to the use and creation of content by AI is just messy, and the UK government is consulting on how to tackle this. And the Online Safety Act is kicking into gear to mitigate risks of harms that increase as the internet expands.

Data protection

Do you remember back in 2023 (*see issue 349, p116*) I was telling you about the Data Protection and Digital Information (No. 2) Bill (DPDI2), which had replaced 2022’s DPDI1 Bill? Well, that one didn’t work out either. With some stealthy renaming back to DPDI at the end of 2023, it looked set to be enacted in 2024. But then someone called a general election and the Bill was dropped.

With the new Labour government, there were musings of whether the reforms would stop in their tracks to stay aligned with EU legislation. But my ears pricked up at the announcement of the Digital Information and Smart Data Bill in the King’s Speech in July 2024. This didn’t emerge either. The House of Lords then put its own stamp on it and welcomed the Data (Use and Access) (DUA) Bill in October 2024.

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

“Right now, I’m trying to keep track of several legal developments”

One could be forgiven for thinking that the main debate so far has been over what the new law should be called. But there is some meat to the proposals, too.

The changes I’m talking about most are those impacting the right of access to personal data. A common query is: how far do you need to go to search for data in response to a subject access request? With organisations using ever-increasing amounts and varieties of technology, the potential sources of data are vast.

Let’s say you receive a request from a customer. At one extreme, you could halt all other operations in the organisation, and spend human and computing resources searching every system and device (and paper file) ever touched by anyone for any trace of personal data about the requestor. After all, it’s always possible a small piece of data is hidden at the back of a drawer somewhere. At the other extreme you could print out the customer’s entry in your main database, momentarily ponder as to whether you remember there being anything else, then give up and send the printout.

There tends to be a misconception that if the customer has said: “I want everything you have on me”, that you need to take the former approach. But there are limits to required searches. Currently, where an organisation holds a large quantity of data about the requestor, it can ask what information or activities their request relates to. This has always seemed odd to me, as if you need clarification to conduct a search, then why do you first have to demonstrate you hold a lot of data? Your customer may have contacted a particular department, where you can find their records within a limited range of systems. But you also have other teams and types of customer, and who’s to say they weren’t once your employee, too? Without conducting overly complex searches, you may not know whether you hold any information within other records, let alone large quantities.

The DUA Bill helps with this. It proposes a new rule, which allows an organisation to clarify a request where it “reasonably requires further information to identify the information or processing activities to which a request... relates”. This is not limited to where large quantities of data are held. Seeking clarification should also help the individual to get what they actually want, rather than being swamped with irrelevant information.

The DUA Bill also says an individual is only entitled to personal data based on a reasonable and proportionate search (which reflects existing case law and guidance). So you can leave some stones unturned in your search for data. What this means will depend on the context, including whether the individual has been clear on what they are looking for, what significance the data has to them, and what the burdens and costs are in locating and retrieving the data. If the request is unreasonable, there is also an exemption for “manifestly unfounded or excessive” requests.

BELOW Data transfers between the UK, the EU and the US are currently in flux

I’m also keeping an eye on the long-running international data transfer saga. I told you about the EU-US data protection framework (and related UK-US Data Bridge) in issue 359, and that it was already facing challenges. It may be wise to have another plan in your back pocket for data transfers to the US,

particularly now President Trump is giving Executive Orders an overhaul (including reviewing those that form the foundation for adequacy of the framework). Standard contractual clauses may seem an obvious solution, but these also require a transfer risk assessment, which could be impacted by changes to the US regime.

Plus there are rumblings of whether the DUA Bill could impact the EU's determination of adequacy for transfers *into* the UK.

AI and copyright

Intellectual property (IP) rights holders and those training, developing and deploying AI models are struggling to navigate how the law applies to the use and creation of content by AI. There are issues in the use of creative content to train AI, whether AI outputs may infringe others' IP, whether AI outputs can attract intellectual property protection (and, if so, who owns that IP), how consumers can spot that a work is AI-generated, and how individuals can address the risks of deepfakes. There are lots of questions where I don't have a clear answer. This is not because I'm a lawyer and prone to giving cryptic advice, but because the law itself was not drafted with AI in mind.

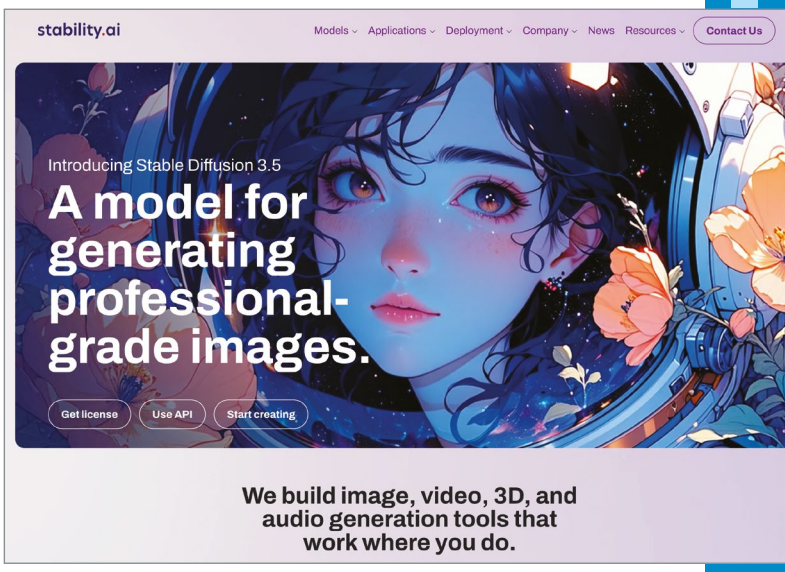
The government opened a consultation on AI and copyright at the end of last year, and the consultation closed on 25 February. An area of focus is the use of works protected by copyright (or related rights, such as database rights) for training AI models.

One option proposed by the government is that AI developers would be able to train on material to which they have lawful access (such as publicly available content), but only where rights holders have not expressly reserved their rights (in which case licences would be needed). This is much wider than the existing exception to copyright infringement under UK law covering data mining for non-commercial research. Mechanisms to support this may include standard tools to reserve rights, individual or collective licensing agreements for payments, and transparency of AI training sources.

I spoke with a company in the publishing industry that thinks this proposal is crazy and doesn't do enough to protect rights holders. In practice, how can they challenge the use of unlawful training material, as it will be too late to back-track? One question posed by the consultation is what the consequences should be of using material where a rights reservation is ignored. Other challenges include limitations on technical controls, concerns over unclear rights reservations, and impracticalities in listing vast quantities of training sources. Indeed, the creative industries have been campaigning against the "opt-out" approach, and in February more than 1,000 musicians released a silent album, *Is This What We Want?*, in protest, with empty studios and performance spaces.

On the other side of the coin, another company I spoke to is desperately looking for clarity on what is permitted so it can make lawful use of publications. It has no intention of depriving authors and publishers of their rights, and is happy to sign up to a licensing model if that is what's needed. But it doesn't want to be taken for a ride by licensing agencies claiming full control of works and charging arbitrary amounts.

Alongside this consultation, the courts are facing the challenge of applying existing copyright law to disputes between copyright holders and AI developers. In the UK, there's a pending High Court case: *Getty Images vs Stability AI*. Getty Images is claiming Stability AI is infringing its copyright (and copyright of its licensors) by using images without authorisation to train its generative AI model, Stable Diffusion. The case started in 2023 and is set for a first trial to determine liability in June 2025.



ABOVE **Stability AI is being taken to court by Getty Images over alleged copyright violations**

"The creative industries are campaigning against the 'opt-out' approach"

Online safety

I've filled up my word count with names of data protection law, so am in rather a rush to discuss online safety. The Online Safety Bill I wrote about in 2023 (*see issue 345, p116*) became an Act in October 2023. As a quick recap, you're caught by the rules if you offer user-to-user services (which means users can share content or communicate with each other) or are an online search provider.

Just over a year ago I drafted terms of service for two new online platforms, enabling messaging between individual users. We envisaged illegal content and age assurance issues, but the finer details were parked pending more information from Ofcom. And now it's here! Ofcom has published codes of practice and guidance to implement the rules, and tools to assist organisations.

Illegal content risk assessments should have been completed by now, and an assessment on whether children are likely to access to the service by April 2025. Where such access is likely, a children's risk assessment should be carried out by July 2025. Age-check methods suggested by Ofcom include photo ID matching, facial age estimation, credit card checks, digital identity services and email-based age estimation.

Another action for providers (which should already be on track) is to ensure terms of service address protection from illegal content, complaints procedures, and rights of users to take action for breach of contract relating to the removal of material, as well as other terms to protect children.

BELOW **Musicians including Kate Bush and Damon Albarn protested against the government's AI plans**

Planning ahead

It's a good idea to keep an eye on the legal pipeline and start planning how it could impact you. There's always a risk that Bills won't become Acts or cases won't be decided as expected, though. If you plan too much too soon, you may need to backtrack. If, following my article in issue 349 (on then-current data protection proposals), you scrapped your process for data protection impact assessments and fired your data protection officer then... oops. I'm afraid these changes didn't make it into the DUA Bill. That must be annoying.

olivia.whitcroft@obep.uk