COMPUTERS & LAW

NEWS REVIEW

MARCH 2024

» **Computers & Law News Review**
Computers & Law News Review is published monthly and brings together the news reported on scl.org over the previous month.

» **Join SCL**
Join online at www.scl.org, email hello@scl.org or ring 07948 517049. For £155 you get full membership, including six copies of the magazine. Academic concession rate: £52 Concessionary/low income (6 months): £25

» **Contributing to Computers & Law**
Computers & Law relies on our members and readers for much of our content. If you have an idea for an article or wish to submit a news piece, event report or anything else, in the first instance please email David Chaplin: david.chaplin@scl.org.

» **Disclaimer**
The views expressed in the articles, reports, reviews and other contributions to Computers & Law are those of the authors and do not necessarily reflect the views of the officers, Council or any member of the Society for Computers and Law.

ISSN: 0140-3249

Published by the Society for Computers and Law.

Contents

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

NEWS FROM THE UK

House of Lords Communications and Digital Committee publishes report about LLMs and generative AI

The House of Lords Communications and Digital Committee has published its report on large language models and generative AI.

It says that the UK government's approach to AI and large language models (LLMs) has become too focused on a narrow view of AI safety. The UK must rebalance towards boosting opportunities while tackling near-term security and societal risks. Otherwise, it will fail to keep pace with competitors, lose international influence and become strategically dependent on overseas tech firms for a critical technology.

The report warns about the "real and growing" risk of regulatory capture, as a multi-billion pound race to dominate the market deepens. Without action to prioritise open competition and transparency, a small number of tech firms may rapidly consolidate control of a critical market and stifle new players, mirroring the challenges seen elsewhere in internet services.

The Committee welcomes the UK government's work on positioning the UK as an AI leader, but says a more positive vision for LLMs is needed to reap the social and economic benefits, and enable the UK to compete globally. Key measures include more support for AI start-ups, boosting computing infrastructure, improving skills, and exploring options for an 'in-house' sovereign UK large language model.

The Committee considered the risks around LLMs and says the apocalyptic concerns about threats to human existence are exaggerated and must not distract policy makers from responding to more immediate issues.

The report found there were more limited near-term security risks including cyber attacks, child sexual exploitation material, terrorist content and disinformation. The Committee says catastrophic risks are less likely but cannot be ruled out, noting the possibility of a rapid and uncontrollable proliferation of dangerous capabilities and the lack of early warning indicators. The report called for mandatory safety tests for high-risk models and more focus on safety by design.

The Committee calls on the government to support copyright holders, saying the government "cannot sit on its hands" while LLM developers exploit the works of rightsholders. It rebukes tech firms for using data without permission or compensation, and says the government should resolve the copyright dispute "definitively" including through legislation if necessary. The report calls for a suite of measures including a way for rights-holders to check training data for copyright breaches, investment in new datasets to encourage tech firms to pay for licensed content, and a requirement for tech firms to declare what their web crawlers are being used for.

The Committee has made ten core recommendations. These include measures to boost opportunities, address risks, support effective regulatory oversight – including to ensure open competition and avoid market dominance by established technology giants – achieve the aims set out in the AI White Paper, introduce new standards, and resolve copyright disputes.

Guidance published on upcoming connectable product security regime

The Department for Science, Innovation and Technology has published updated guidance on the UK Product Security and Telecommunications Infrastructure (Product Security) regime for connectable product security, which comes into effect on 29 April 2024. Manufacturers of UK consumer connectable products will be required to ensure that their products meet the relevant minimum security requirements. The guidance sets out how businesses should comply with the regime, such as who is subject to the duties under the regime, duties of relevant parties, security requirements and enforcement. In addition, the Office for Product Safety & Standards (OPSS) has updated its guidance. It explains the enforcement powers that are available to the OPSS when addressing non-compliance with the legislation. These relate to the service of a compliance, stop or recall notice, the imposition of monetary penalties, and application for a forfeiture order.

UK government publishes response to AI White Paper

The UK government has published its response to its AI White Paper, which was published last year. It set out initial proposals to develop a "pro-innovation regulatory framework" for AI. The proposed framework outlined five cross-sectoral principles for the UK's regulators to interpret and apply within their remits. The government also proposed a new central function to bring coherence to the regime and address regulatory gaps.

The five principles were:

- Safety, security and robustness.
- Appropriate transparency and explainability.
- Fairness.
- Accountability and governance.
- Contestability and redress.

The government says there was strong support for these principles. It says that it remains "committed to a context-based approach that avoids unnecessary blanket rules that apply to all AI technologies, regardless of how they are used. This is the best way to ensure an agile approach that stands the test of time."

Since the publication of the White Paper, the CMA has published a review of foundation models to understand the opportunities and risks for competition and consumer protection and the ICO updated its guidance on how data protection laws apply to AI systems to include fairness.

The government has written to several regulators affected by AI to ask them to publish an update outlining their strategic approach to AI by 30 April. It is encouraging regulators to include:

- An outline of the steps they are taking in line with the expectations set out in the white paper.
- Analysis of AI-related risks in the sectors and activities they regulate and the actions they are taking to address these.
- An explanation of their current capability to address AI as compared with their assessment of requirements, and the actions they are taking to ensure they have the right structures and skills in place.
- A forward look of plans and activities over the coming 12 months.

The government also proposed an AI central function. It says it has started developing the central function to support effective risk monitoring, regulator coordination, and knowledge exchange. It has also published guidance to support regulators to implement the principles effectively.

The government highlights three broad categories of AI risk: societal harms; misuse risks; and autonomy risks.

Societal harms

- Preparing UK workers for an AI enabled economy – there will be guidance on the use of AI in HR and recruitment. In addition, it will publish a skills framework later this year, as well as funding AI-related courses.
- Enabling AI innovation and protecting intellectual property – creative industries and media organisations have particular concerns regarding copyright protections in the era of generative AI. The Intellectual Property Office convened a working group made up of rights holders and AI developers on the interaction between copyright and AI. However, it is now clear that the working group will not be able to agree an effective voluntary code. The government intends to do further research and engagement in this area.
- Protecting UK citizens from AI-related bias and discrimination – regulators such as the ICO have updated guidance.
- Reforming data protection law to support innovation and privacy – the Data Protection and Digital Information Bill will expand the lawful bases on which solely automated decisions that have significant effects on individuals can take place.
- Ensuring AI driven digital markets are competitive – the CMA has carried out an initial study and the Digital Markets, Competition and Consumers Bill aims to give it the tools it needs to regulate digital markets.
- Ensuring AI best practice in the public sector.

Misuse risks

Safeguarding democracy from electoral interference – among other things, the Online Safety Act 2023 will capture specific activity aimed at disrupting elections where it is a criminal offence in scope of the regulatory framework.

Preventing the misuse of AI technologies – the NCSC published guidelines for secure AI system development in November 2023. The Online Safety Act and the Product Security and Telecommunications Infrastructure Act also aim to provide regulation in this area.

Autonomy risks

- The government has examined the case for new responsibilities for developers of highly capable general-purpose AI system. It says that while voluntary measures are a useful tool to address risks today, it anticipates that all jurisdictions will, in time, want to place targeted mandatory interventions on the design, development, and deployment of such systems to ensure risks are adequately addressed.
- It is also working with international partners on AI governance.

Ofcom issues roadmap to regulating new Media Bill

Ofcom has published a roadmap to regulating the new Media Bill, which is currently passing through the UK parliament. This article considers the aspects of most interest to SCL readers.

The measures in the Bill include:

- Amending a simplifying the requirements of public service broadcasters, including protecting listed events (i.e. events of national interest such as sporting events), requiring them to be free to watch.
- An Ofcom-regulated video-on-demand code for major streaming platforms such as Netflix, Amazon Prime and Disney+. This will impose editorial standards like those applying to broadcast TV. Streaming services will also be subject to accessibility requirements, such as subtitling.
- New rules to make sure public service content is available, prominent, and easily accessible on connected TV platforms, such as smart TVs and streaming sticks. This requires Ofcom to establish new codes, guidance and dispute resolution processes.
- The Bill gives Channel 4 the ability to produce and monetise more of its own programming.
- Removing outdates regulatory burdens on radio services, while protecting and strengthening the provision of local news. This includes ensuring that BBC, commercial and community stations are accessible to listeners via smart speakers.

The Bill will require changes to the Ofcom fee structures for many services that it currently regulates, as well as bringing new services into scope of its regulation (including connected TV platforms, voice-activated services and some non-UK based VoD services). A revised fee regime is expected to be in place before April 2026.

Listed events

Following Royal Assent, Ofcom will draft regulations to define the meaning of certain terms used in the listed events regime, including 'adequate live coverage' and 'adequate alternative coverage'. It will call for evidence in the summer ahead of consultation. It will consult fully in 2025, with the revised Code and regulations to follow later that year.

Ofcom's roadmap – VOD providers

Shortly after Royal Assent, Ofcom expects the government to formally request a report from Ofcom on the state of the VoD market in the UK. This will be considered by the Secretary of State when deciding which services will be designated as 'Tier 1' services and therefore subject to the new VoD Code and the new accessibility requirements. Ofcom expects to submit this report around the end of 2024.

It will also work on the VoD Code and accompanying guidance, due to come into effect in 2025 following consultation. There will be a 12 month grace period from publication of the Code (or their designation as a Tier 1 service, whichever is later) before they are required to comply. Ofcom will also consult on and finalise new procedures for handling and resolving complaints.

The Bill also requires Ofcom to review the audience protection measures implemented by VoD providers (both existing and new) to protect audiences from harm. This will begin shortly after Royal Assent.

Ofcom also expects to consult on a new VoD Accessibility Code around the beginning of 2025. The first set of accessibility quotas is likely to come into effect around the middle of 2027 of 24 months after a provider is designated as Tier 1, whichever is later. However, there will be interim quotas and reporting requirements in force from 2026.

Radio code

Ofcom will also produce a Code of Practice that will set out Ofcom's expectations on both designated platforms and radio services that have opted into the regime. The Code of Practice will, among other things, explain the steps platforms can take to ensure compliance with their duties as well as clarifying the technical and other requirements which will apply to internet radio services. Ofcom plans to launch a consultation on the draft code around the end of 2025 alongside a consultation on draft enforcement guidance. It expects to publish final versions of these documents in 2026.

PSBs

Ofcom plans to focus first on the process designating the services in scope. Later in 2024, it will consult on how it intends to apply the criteria for the designation of PSB online players alongside its plans for running the application process. It will also consult on the methodology it will use to give advice to the Secretary of State about platform designation. It plans to issue final statements and its report by the middle of 2025.

It will then focus on drafting the codes and guidance. It will consult in 2025 on how Ofcom recommends regulated platforms can comply with their duties to give prominence to designated PSB players and content as well as securing the accessibility of their services to people with disabilities.

For the final stage of implementing the regime, it will consult on its enforcement and dispute resolution procedures – this is likely to be the end of 2025.

Law Commission calls for evidence on digital assets and consults on draft legislation

The Law Commission has launched a call for evidence to inform its project on private international law in the context of digital assets and electronic trade documents. It is also separately seeking views on draft legislation following its report on digital assets in June 2023.

Digital assets and electronic trade documents in private international law

The Law Commission seeks a better understanding of the most challenging and prevalent issues that digitisation, the internet, and distributed ledger technologies pose for private international law.

When parties to a private law dispute are based in different countries, or the facts and issues giving rise to the dispute cross national borders, questions of private international law arise: in which country's courts should the parties litigate their dispute, and which country's law should be applied to resolve it?

The project has a particular focus on crypto-tokens and electronic trade documents because these assets are prevalent in market practice, whilst also posing novel theoretical challenges to the traditional methods of private international law.

The Law Commission is specifically asking the following questions:

- To what extent can the existing methods and approaches of private international law be applied to the new digitised and decentralised contexts in which digital assets and electronic trade documents are used?
- How easily can the existing rules of private international law be applied to determine when the courts should accept jurisdiction over a dispute involving a digital asset or electronic trade document?
- How easily can the existing rules of private international law be applied to determine which country's laws should apply to resolve a dispute involving a digital asset or electronic trade document?
- What market practices have developed, and what challenges stakeholders have encountered in their dealings with either digital assets or electronic trade documents (under the Electronic Trade Documents Act 2023) in commercial and legal practice?

The deadline for responses is 16 May 2024.

Digital assets and personal property rights

The Law Commission is also consulting on draft legislation to confirm the existence of a third category of personal property into which crypto-tokens and other assets could fall.

Its June 2023 report concluded that certain digital assets, including crypto-tokens and non-fungible tokens (NFTs), can attract personal property rights. However, because digital assets differ significantly from physical assets, and from rights-based assets like debts and financial securities, they do not fit within traditional categories of personal property. In its report, the Commission said that the unique features of digital assets should be recognised as belonging to a separate category of personal property. Although the courts have been – expressly or impliedly – moving towards the recognition of a "third category" of personal property, the Commission recommended legislation to remove any uncertainty as it its existence. The prospect of this legislation was supported by a range of consultees, including members of the judiciary.

The Commission has now prepared draft legislation to reflect this recommendation, and is seeking consultees' views on the draft clauses including as to their potential impact.

The draft legislation deliberately does not attempt to define what will fall within the third category, leaving this open for common law development. As well as assets like crypto-tokens, it could potentially include other things such as voluntary carbon credits. Similarly, the consequences of being a "third category thing" will be for the courts to determine.

The consultation ends on 22 March 2024.

ICO issues guidance for platforms when moderating online content

The guidance aims to help organisations caught by the Online Safety Act to also comply with data protection laws.

The ICO has issued guidance to organisations that come within the scope of the Online Safety Act 2023 to help them comply with data protection law as they carry out content moderation to meet their online safety duties.

Content moderation is commonly used by organisations to analyse content generated by users to check if it is appropriate for publication on their platforms. This process involves using people's personal information and the ICO says that it can cause harm if incorrect decisions are made.

In the guidance on content moderation, the ICO outlines how data protection law applies to these processes and the impacts they can have on people's information rights.

It explains how data protection law applies when platforms use content moderation technologies and processes. It provides practical advice to help comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The ICO points out that if organisations are processing children's personal information, they should conform with the Children's code. The ICO uses "child" to refer to anyone under the age of 18. The Code is a statutory code of practice that sets out how internet society services likely to be accessed by children can protect children's information rights online. It sets out fifteen standards that platforms should implement if they are an internet society service.

The Data Protection and Digital Information Bill was reintroduced in the Houses of Parliament on 8 March 2023. Assuming it becomes law, it will amend elements of the DPA 2018 and the UK GDPR relevant to this guidance. The ICO has written this guidance in line with current law. This guidance on content moderation is the first in a series of products the ICO has planned about online safety technologies. The ICO says it is working with Ofcom on the project and will update the guidance when Ofcom's final codes of practice are published.

Public Accounts Committee issues report on preparedness for online safety regulation

The Public Accounts Committee has issued a report on Ofcom's preparedness for online safety regulation. It says that Ofcom has made a good start in preparing for its new role as the online safety regulator. It benefited from time to prepare while the Online Safety Bill was going through Parliament and so has been able to move swiftly since the Act became law. Ofcom has already acted against a suicide-promoting website, which is now blocked in the UK. However, the Committee says that it may be years until people notice a difference to the online experience. People may be further disappointed that Ofcom cannot act on individual complaints from the public and does not plan to inform complainants about any resulting action it takes where their complaints have helped it to identify a systemic issue with a service provider. Ofcom faces significant challenges about how it will engage with, supervise and regulate providers based overseas (which constitute the vast majority of regulated services), in particular smaller providers and those that may seek to avoid its attention. The Committee points out that over 100,000 service providers are covered by the Act and so Ofcom is reliant on large scale data collection and automated systems to regulate them all, which it has yet to develop. These systems will have to keep up with the fast-moving nature of online harms. The Committee says that this regulatory regime is at the forefront of online regulation globally. If Ofcom follows through on its positive start, then the establishment of the online safety regime has the potential to be a case example of good practice when setting up a new regulator, or significantly expanding its remit. However, Ofcom still has a lot to do to implement an effective regulatory regime and some of this work will take a long time. A key measure of success for the new regime will be whether Ofcom is able to meet the requirement in the Act to have regulation in place for illegal harms and protecting children by April 2025. The government has two months to respond to the report.

Bar Council issues guidance on AI

The Bar Council has issued new guidance for barristers navigating the growing use of ChatGPT, and other generative AI and large language model systems (LLMs). It concludes that there is nothing inherently improper about using reliable AI tools for augmenting legal services, but they must be properly understood by the individual practitioner and used responsibly. The guidance, available on the Bar Council ethics and practice hub, sets out the key risks with LLMs: anthropomorphism; hallucinations; information disorder; bias in data training; and mistakes and confidential data training. It explores the considerations for practitioners when using LLM systems: due to possible hallucinations and biases, it is important for barristers to verify the output of LLM software and maintain proper procedures for checking generative output; "black box syndrome"– LLMs should not be a substitute for the exercise of professional judgment, quality legal analysis and the expertise that clients, courts and society expect from barristers; barristers should be extremely vigilant not to share with an LLM system any legally privileged or confidential information; barristers should critically assess whether content generated by LLMs might violate intellectual property rights and be careful not to use words which may breach trademarks. It is important to keep abreast of relevant Civil Procedure Rules, which in the future may implement rules/practice directions on the use of LLMs, for example, requiring parties to disclose when they have used generative AI in the preparation of materials.

UK Voluntary Code of Good Practice on Transparency in Music Streaming published

The Intellectual Property Office has published the UK Code of Good Practice on Transparency in Music Streaming. The voluntary code has been developed and agreed by 12 music industry bodies representing music creators, record labels, publishers, digital service providers, distributors and collecting societies. It is part of the commitment made by the government in response to the recommendations of the Culture, Media and Sport Select Committee's Inquiry into Music Streaming. The IPO will have oversight of the Code and its implementation and will convene meetings of signatory organisations every six months to consider how the Code is working, with a formal review of the Code in 2026. It sets out agreed standards of good practice, forming part of a shared ambition across the music industry to build greater trust in music-maker contracts, streaming licensing deals, royalty payments, usage data, audit rights, and communication to music creators. This is part of the process to help improve creators' understanding of how their music is licensed, administered and used, helping build confidence and clarity that they are being paid correctly when their music is played via streaming services.

Ofcom consults on changes to digital television additional service licences

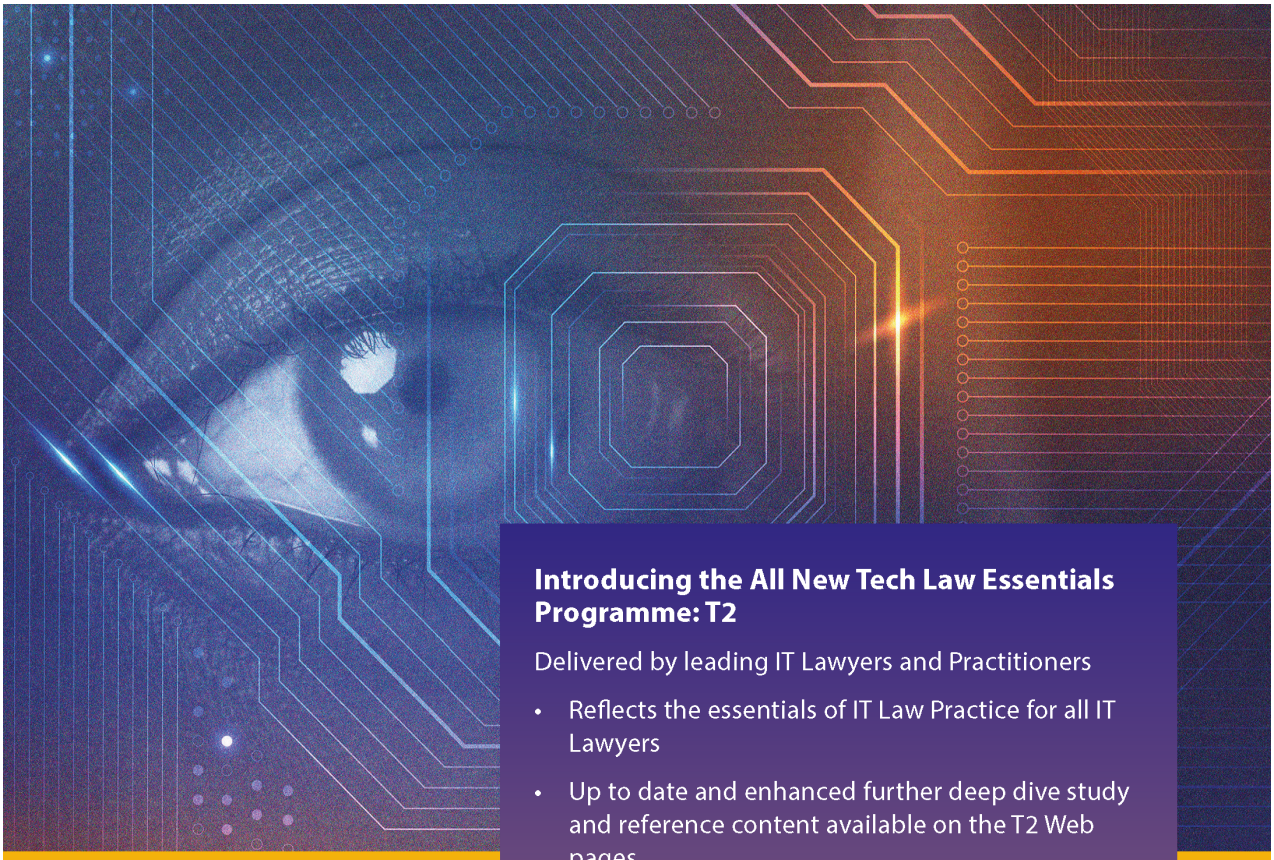
Ofcom is consulting on proposed changes to the conditions included in Digital Television Additional Service licences. These services are broadcast on Freeview and usually consist of text or data – for example, they are used to broadcast software that allows a viewer to watch channels delivered via the internet. Under the current licence conditions for these services, a warning must be displayed letting viewers know they are about to view material delivered over the internet, which may not be regulated in the same way as other television services. However, the current wording of the licence condition means that a warning must be displayed even if the service is licensed by Ofcom and therefore subject to its content standards rules. This could be confusing for viewers, so Ofcom is proposing to update the licence condition so that warnings are not required if the licensee holds an Ofcom broadcast licence. Ofcom also wishes to introduce some administrative changes. The consultation ends on 17 April 2024.

Digital Government (Disclosure of Information) (Identity Verification Service) Regulations 2024 made

The Digital Government (Disclosure of Information) (Identity Verification Service) Regulations 2024 (SI 2024/64) were made on 18 January 2024, and are scheduled to come into force on 8 February 2024. The purpose of the Regulations is to expressly allow specified public authorities to check and share government-held personal data to make it easier for individuals to prove their identity when seeking to access public services digitally.

Circular published about new offences under Online Safety Act

The UK government has published a circular to inform the police and other relevant public authorities of certain provisions of the Online Safety Act, in particular new criminal offences. There are offences relating to the new requirement to report Child Sexual Exploitation and Abuse (CSEA) content to the National Crime Agency (NCA) in section 69 of the Act – this offence is not yet in force. There are also offences in Part 7 of the Act, which relate to Ofcom's enforcement powers – these came into force on 10 January 2024; and offences in Part 10 of the Act (the communications offences) – these came into force on 31 January 2024.



SCL Tech Law Essentials: The Next Generation – Serious Content for Serious Times

Introducing the All New Tech Law Essentials Programme: T2

Delivered by leading IT Lawyers and Practitioners

- Reflects the essentials of IT Law Practice for all IT Lawyers
- Up to date and enhanced further deep dive study and reference content available on the T2 Web pages
- Ongoing access to course material
- Digital reference material
- Dovetails with Professional Standards Continuing Competence requirements and validation
- Certificate of completion
- Exceptional value for money!

Module 1

The Annual Zeitgeist - New issues and new areas of Tech Law and Tech Law Practice - "Tech and Abuse of Dominance, and Tech, Digital Assets and NFT - from cutting edge to mainstream"

Now available to purchase on the SCL website

SCL Members: Just £90 plus VAT (£108)

Non-SCL Members: £180 plus VAT (£216)

All T2 modules will be available to attend in person, online and will be recorded – for more details see: www.scl.org/about/T2

SCL 1973/2023 50th Anniversary
Tech Law for Everyone

NEWS FROM THE EU & OVERSEAS

European Data Protection Board holds latest plenary session

Among other things, the EDPB adopted an Opinion on the notion of main establishment.

During its latest plenary, the EDPB adopted an Opinion on the notion of main establishment and on the criteria for the application of the One-Stop-Shop mechanism, following a request under Article 64(2) GDPR by the French data protection authority. The Opinion clarifies the notion of a controller's "main establishment" in the EU, especially where decisions regarding the processing are taken outside the EU.

In its Opinion, the EDPB considers that a controller's "place of central administration" in the EU can only be considered as a main establishment under Article 4(16)(a) GDPR if it makes the decisions on the purposes and means of the processing of personal data and if it has the power to have such decisions implemented. The EDPB further explains that the One-Stop-Shop mechanism can only apply if there is evidence that one of the controller's establishments in the EU takes decisions on the purposes and means for the relevant processing operations and has the power to have these decisions implemented. This means that, when the decisions on the purposes and means of the processing are taken outside the EU, there is no main establishment of the controller in the EU, and therefore the One-Stop-Shop should not apply.

This Opinion follows the EDPB's Vienna Statement on cross-border enforcement, aiming to streamline enforcement and cooperation among data protection authorities.

In addition, the EDPB adopted a Statement on the legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse. The Statement follows the EDPB-EDPS Joint Opinion on the European Commission's Proposal for a Regulation and focuses on the latest legislative developments, in particular the position of the European Parliament of November 2023.

The EDPB welcomes the many improvements proposed by the Parliament, such as exempting end-to-end encrypted communications from detection orders. However, the EDPB says that the updated text does not fully resolve important issues flagged by the EDPB and the EDPS related to general and indiscriminate monitoring of private communications, especially regarding detection orders.

The EDPB stresses the importance of further limiting the risk that those orders could affect individuals who are unlikely to be involved in child sexual abuse-related crimes. Furthermore, the EDPB says that detection orders are not limited to child sexual abuse materials (CSAM) that are already known to authorities, despite the fact that the technologies used to detect new CSAM have proven in the past to have significant error rates. During the plenary, the EDPB also discussed the scope of the guidance related to the Consent or Pay model. In addition to the upcoming Article 64 (2) Opinion, which will address the Consent or Pay model in the context of large online platforms, it was agreed that there is a need to consecutively develop Guidelines with a broader scope.

EDPB launches website auditing tool to analyse legal compliance

The EDPB has launched a website auditing tool that can be used to analyse if websites comply with the law. The tool was developed in the context of the EDPB Support Pool of Experts and can be used by both legal and technical auditors at data protection authorities, as well as by controllers and processors who wish to test their own websites. The new tool allows preparing, carrying out and evaluating audits directly in the tool by a simple visit to the website in question. The tool is also compatible with other tools, such as the EDPS website evidence collector, and allows auditors to import and evaluate the results of audits carried out on those tools. Finally, the tool can generate reports. While several website auditing tools already exist, these usually require technical expertise. Therefore, the EDPB decided to develop a solution that would be easy to use to facilitate enforcement by national regulators and compliance checks by controllers. A second version with new features is planned for later this year.

European Commission and consumer authorities investigate online influencers

Only 20% of influencers disclose that their content is advertising.

The European Commission and national consumer protection authorities have issued the results of a sweep of social media posts by 572 influencers. The sweep found that 97% posted commercial content but only one in five systematically indicated that their content was advertising. The objective of the sweep was to verify whether influencers disclose their advertising activities as required by EU consumer law.

The main sectors of activity concerned were fashion, lifestyle, beauty, food, travel and fitness/sport. According to the Commission, 119 influencers were promoting unhealthy or hazardous activities, such as junk food, alcoholic beverages, medical or aesthetic treatments, gambling, or financial services such as crypto trading.

EU consumer law provides that commercial communications must be transparent. In their posts, influencers should not mislead consumers with false or untruthful information on the promoted products or services that fall under the Unfair Commercial Practices Directive. Any promotion of the products or services of a brand in a post that earns its influencer revenues or other types of benefits must be disclosed as an advertising activity.

In addition, influencers who sell products or services for their own account have the same legal obligations as online shops, such as providing consumers with legal guarantees or withdrawal rights as required by the Consumer Rights Directive.

On 17 February 2024, the Digital Services Act came into force in the EU. Among other things, the DSA requires influencers uploading content to declare whether such content contains commercial communications. In addition, influencers qualifying as traders now need to provide information to ensure their traceability before they use an online platform to promote or offer their products or services. These obligations already apply to the very large online platforms (such as Instagram, TikTok, Youtube, Facebook, X and Snapchat). Smaller platforms must comply from 17 February.

Finally, under the Audiovisual and Media Services Directive, influencers offering audiovisual content and meeting the criteria to be considered audiovisual media service providers need to comply with specific rules on audiovisual commercial communications, incitement to violence and hatred and harmful content for minors. For example, audiovisual commercial communications of influencers need to be readily recognisable and must not be prejudicial to health or safety; influencers' content must not exploit minors' inexperience or credulity, and must not unreasonably show minors in dangerous situations.

Findings of the sweep

- 97% of published posts included commercial content, but only 20% systematically disclosed this as advertising;
- 78% of the verified influencers were exercising a commercial activity, but only 36% were registered as traders at national level;
- 30% did not provide any company details on their posts, such as e-mail address, company name, postal address or registration number;
- 38% of them did not use the platform labels that serve to disclose commercial content, such as the "paid partnership" toggle on Instagram. They used different wording, such as "collaboration" (16%), "partnership" (15%) or generic "thanks to the partner brand" (11%,);
- 40% made the disclosure visible during the entire commercial communication. 34% of influencers' profiles made the disclosure immediately visible without needing additional steps, such as by clicking on "read more" or by scrolling down;
- 40% of influencers endorsed their own products, services, or brands. 60% of those did not consistently, or at all, disclose advertising; and
- 44% influencers had their own websites, from which a majority were able to sell directly.

Next steps

As a result of the sweep, there will be more investigation of 358 influencers. The Commission will analyse the results of the sweep in light of the legal obligations of the platforms under the DSA and will take the necessary enforcement action as appropriate. The results of the sweep will also feed into the Digital fairness fitness check of EU consumer law, which was launched in Spring 2022 by the European Commission. It covers the Unfair Commercial Practices Directive, the Consumer Rights Directive and the Unfair Contract Terms Directive and is considering if they effectively deal with consumer protection issues such as dark patterns, personalisation practices, influencer marketing, contract cancellations, marketing of virtual items, or the addictive use of digital products, amongst others.

Digital Services Act starts applying to all online platforms in the EU

The DSA started to apply on 17 February 2024.

On 17 February, the Digital Services Act (DSA), started to apply to online intermediaries in the EU with the exception of certain SMEs and micro-businesses.

The DSA aims to ensure that EU users are better protected against illegal goods and content and have their rights upheld on online platforms where they connect with other users, share information, or buy products.

New responsibilities for platforms and empowered users

All online platforms with users in the EU, with the exception of small and micro enterprises employing fewer than 50 people and with an annual turnover below €10 million, must implement measures to:

- Counter illegal content, goods, and services: online platforms must provide users with means to flag illegal content, including goods and services. In addition, online platforms are required to cooperate with 'trusted flaggers', specialised entities whose notices will have to be given priority by platforms.
- Protect minors: including a complete ban of targeting minors with ads based on profiling or on their personal data.
- Empower users with information about advertisements they see, such as why the ads are being shown to them and who paid for the advertisement.
- Ban advertisements that target users based on sensitive data, such as political or religious beliefs, sexual preferences, etc.
- Provide statements of reasons to a user affected by any content moderation decision, eg content removal, account suspension, etc and upload the statement of reasons to the DSA Transparency database.
- Provide users with access to a complaint mechanism to challenge content moderation decisions.
- Publish a report of their content moderation procedures at least once per year.
- Provide the user with clear terms and conditions, and include the main parameters based on which their content recommender systems work.
- Designate a point of contact for authorities, as well as users.

In addition to online platforms, the Digital Services Act also applies to hosting services (for example, cloud services or domain name systems, background services which connect users to requested website addresses), as well as to online intermediaries (eg internet service providers, or domain). Hosting services and online intermediaries are subject to a subset of obligations under the DSA.

Since August 2023, the DSA has applied to the 19 Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) designated in April 2023 (with more than 45 million monthly users on average). Three other platforms designated as VLOPs in December 2023 have until April to comply with the most stringent obligations under the DSA. However, they now have to comply with the general DSA obligations as of 17 February.

Digital Services coordinators in EU member states

Platforms not designated as VLOPs or VLOSEs are supervised at member state level by an independent regulator acting as the national Digital Services Coordinator (DSC). DSCs supervise and enforce the DSA for the platforms established on their territory. They:

Are the first port of call for complaints by users on infringements against the DSA by any platform, including VLOPs and VLOSEs. The DSC will, when appropriate, send the complaint to the DSC of the platform's member state of establishment, where appropriate, accompanied by an opinion.

Certify existing out-of-court appeal mechanisms for users to address complaints and challenge content moderation decisions.

Assess and award the status of trusted flaggers to suitable applicants, or independent entities that have demonstrated expertise in detecting, identifying, and notifying illegal content online.

Process researchers' requests for access to VLOPs and VLOSEs data for specific research. The DSCs will vet the researchers and request access to data on their behalf.

Have investigation and enforcement powers, to ensure compliance with the DSA by the providers established in their territory. They are able to order inspections following a suspected infringement of the DSA, impose fines on online platforms failing to comply with the DSA, and impose interim measures in case of serious harm to the public sphere.

The European Board for Digital Services

The Digital Services Coordinators and the Commission will form an independent advisory group, the European Board for Digital Services, with the aim of ensuring that the DSA is applied consistently, and that users across the EU enjoy the same rights, regardless of where the online

platforms are established.

The Board will be consulted on the enforcement of the DSA and advise on arising issues related to the DSA and can contribute to guidelines and analysis. It will also assist in the supervision of Very Large Online Platforms and Very Large Online Search Engines and will issue yearly reports on the prominent systemic risks and best practices in mitigating them.

The Board met for the first time on 19 February 2024.

What happens next?

In March 2024, the Commission intends to adopt Guidelines on risk mitigation measures for electoral processes. A consultation on the data access delegated act is expected in April with adoption by July and entry into force in October 2024. In May, the Commission plans to adopt an Implementing Act on transparency report templates.

European Commission opens formal DSA breach proceedings against TikTok

The European Commission has opened formal proceedings to assess whether TikTok may have breached the Digital Services Act (DSA) in areas linked to the protection of minors, advertising transparency, data access for researchers, as well as the risk management of addictive design and harmful content. Based on the preliminary investigation conducted so far, including an analysis of the risk assessment report sent by TikTok in September 2023, as well as TikTok's replies to the Commission's formal Requests for Information (on illegal content, protection of minors, and data access), the Commission has decided to open formal proceedings against TikTok under the Digital Services Act. The Commission will continue to gather evidence, for example by sending additional requests for information, conducting interviews or inspections. The opening of formal proceedings empowers the Commission to take further enforcement steps, such as interim measures, and non-compliance decisions. The Commission is also empowered to accept any commitment made by TikTok to remedy on the matters subject to the proceeding. The DSA does not set any legal deadline for bringing formal proceedings to an end. The duration of an in-depth investigation depends on several factors, including the complexity of the case, the extent to which the company concerned cooperates with the Commission and the exercise of the rights of defence.

CASES

Application by Bytedance seeking suspension of European Commission gatekeeper designation decision dismissed

In *Bytedance v Commission (Case T-1077/23 R)*, the General Court dismissed an application by Bytedance for interim measures in its appeal against the European Commission's September 2023 decision designating it a "gatekeeper" under Article 3 of the Digital Markets Act. According to the General Court, Bytedance had not shown that it is necessary to suspend the contested decision until the proceedings on the substance of the case are closed to avoid serious and irreparable harm to Bytedance. Bytedance argued that the immediate implementation of the contested decision risks causing the disclosure of highly strategic information concerning TikTok's user profiling practices, which is not otherwise in the public domain. That disclosure would enable TikTok's competitors and other third parties to obtain insight into TikTok's business strategies in a way that would significantly harm its business. The court rejected this.

ELSEWHERE

Catch up with some of the stories reported in the Editor's weekly newsletters.

The ICO used Data Protection Day to update on their campaign to regulate cookie pop-ups. In November 2023 the regulator wrote to 53 of the Top 100 websites and apparently 38 of them now have cookie banners complying with the law. The Commissioner himself followed up on that theme in late February in with a speech centred on adtech saying his message is clear; "it must be just as easy to reject all non-essential cookies, as it is to accept them". To that end, and acknowledging writing to just top 100 websites is not the answer, he announced moves to automate monitoring of cookie compliance at scale.

50m customer records from Europcar were breached in a hack but the car hire firm responded this was nonsense: the dataset had instead been generated by ChatGPT. Tell tale signs for Europcar were unknown place names and email addresses not in their systems, though the man behind HaveIBeenPwned, Troy Hunt, is not convinced about the use of ChatGPT saying fabricated breaches have been a problem for a long time.

Plans for a regular AI Safety Report have been announced. This new initiative, emerging from the Bletchley Summit, aims to "drive a shared, science-based, up-to-date understanding of the safety of advanced AI systems" by "producing reports which represent up-to-date syntheses of scientific literature on the capabilities and risks of these AI systems." The first report is due in Q2 of 2024.

The Post Office scandal continued to grow and Computer Weekly recounted the attempts by the PO lawyers to prevent the subpostmasters' expert witness, Jason Coyne, from inspecting one of the now infamous Horizon terminals.

The Bar Council issued new guidance on the use of AI at the Bar. The guidance does not say anything too startling (and is not even official "guidance") but damns with faint praise by stating there is nothing 'inherently improper' in using AI at the Bar. One thing struck me though: that poor New York lawyer who first came up with citations faked by ChatGPT is shouldering a lot of policy making.

Much comment was generated by the Government's response to the consultation on their pro-innovation AI white paper. Notable in the response were the gaps already identified by the Government, with the perhaps contradictory trumpeting of the Product Security and Telecommunications Infrastructure Act, scheduled to come into effect in 2024 and which imposes minimum security requirements for products made available to UK consumers, including AI powered smart speakers.

Perhaps our ancient tort laws can be invoked to protect us as suggested in a paper by Gabriel Weil, an assistant professor of Law in the US, and helpfully summarised on Vox. The underlying premise is that AI firms should be subject to strict liability but, given the harms of AI may take years to emerge, we should "pull forward" the cost of the potential harms so damages can be awarded before they arise.

A study undertaken by a team of US researchers, as reported on Gizmodo, looked at how different AIs responded as lead decision makers in a war simulation and found they have a tendency towards "arms-race dynamics" with sudden lurches to increased military investment and escalation. GPT-4 is the most aggressive, apparently using a desire to see peace in the world as justification for launching nuclear warfare.

The EU agreed on a new Platform Work Directive, which will introduce 'a presumption of an employment relationship (as opposed to self-employment)' and which the platforms in scope will have to rebut if they wish to absolve themselves of the need to pay workers properly.

Vox published a useful round-up - under the title *Your Brain Needs A Good Lawyer* - of what a small group of lawyers and activists are doing to create a right to mental privacy: their concern is primarily around technologies seeking to 'write' to the brain not those, such as Neuralink's current offering, which merely attempt to 'read' it.

The LockBit ransomware group had their entire operation hacked by a team from several international crime agencies including our own National Crime Agency but reemerged just a fortnight later.

Reddit announced a deal to licence their UGC for AI training. Perhaps surprisingly, the deal has been announced before the New York Times dispute with OpenAI has been resolved. Ars Technica published a piece about how the NYT's chances in that dispute may have improved, partly because of the Italian Plumber Problem. Ask a GPT to imagine an Italian plumber in a video game and an image surprisingly similar to Super Mario pops up. Likewise, the NYT has supplied 100 examples of almost verbatim reports generated by ChatGPT.

Avast, who sell themselves as the 'all-in-one solution for privacy, protection, and performance' were fined $16.5m by the FTC after the agency found out they have been selling user data since 2014 and for their sins have now been fined $16.5m by the FTC. An accompanying blog post about the fine the FTC uses some refreshingly colourful language.

That same week the FTC intervened in the bankruptcy proceedings of location data vacuum Near to prevent the sale of data assets to all and sundry which according to Near's privacy policy would have been enabled by listing 'Prospective Buyers of Our Business' as one of the parties

they can share data with. Now, buyers have to put in place sensitive location data programs (sic) before they can put in a bid.

Still, the expansion of data driven advertising shows no signs of slowing yet, as described on The Atlantic in a piece about the 'adpocalypse' which catalogues the increasingly inventive ways in which advertising is being insinuated into all our online interactions. Although written from a US perspective it is an eye-opening read - for example who knew that Uber expects to make $1bn in ad revenue this year.

Finally, bad press for AI chatbots in two doses. ChatGPT seemingly went rogue and started responding to questions with 'drivel'. At first the story amused me, but the more I think about it the less sanguine I become. Where GPT4 is underpinning more fundamental processes than simply organising a trip abroad then who knows where a similar 'bug' may lead us. Then came the chackhanded launch of Google's new version Gemini whose text to image generator had been tweaked to create racially diverse Nazis.

SCL Events Diary 2024/25

MARCH

- **SCL Annual Tech Disputes Masterclass**
  Wednesday 6 March 2024. Womble Bond Dickinson (UK) LLP, London, 1:30 – 5:30 pm.
  This year's annual SCL Tech Disputes Masterclass includes a traditional case law development update, which will be followed by a number of sessions focusing on issues arising from the use of emerging technologies.

- **SCL Tech of Tech Law Conference: Hands-on tech training for tech lawyers**
  In-person and recorded
  Tuesday 26 March. Macfarlanes, London, 9:00 – 5:00pm
  The two stalwarts of the SCL's monthly "Tea and Tech" series, Simon Forrester and Neil Brown, and their special guest speakers are delighted to be back with an all-new "Tech of Tech Law" Conference. Chaired by Elizabeth Fitzgerald, this is a unique event in the SCL's calendar, in that it focuses solely on helping you better understand the technology on which you are being asked to advise.