[00:00:00.410] - Introduction

In this recording from our seminar on the 18 May 2023 on Digital Reform: Insights and Regulators Perspectives', Olivia Mullooly, Partner in the Technology and Innovation Group and Head of the Intellectual Property Group at Arthur Cox, opens the event with some scene setting, providing a brief overview of the legislative landscape for digital content and services.

[00:00:22.850] - Olivia Mullooly, Partner

So start with a brief overview of the legislative landscape and we'll start at the beginning, which was the E-commerce Directive and the E-commerce Act. As you can see, this legislation is now 23 years old and it provided for safe harbour exemptions from liability for intermediaries, intermediaries being hosting providers, providers engaged in transmission and caching services so a mere conduit and any storage that would be necessary in the course of the transmission of a communication and that was subject to the conditions that they weren't liable for the content like as publishers, until such time as they were put on notice of that and acted expeditiously to remove it and in recent years the EU has decided that there needs to be more responsibility and liability on these platforms so the platforms that connect users with third parties and third party content, particularly in respect of illegal and harmful content and misinformation and in terms of how they have tackled that, the first of the Acts I'm going to cover today on the digital agenda is a Digital Markets Act. So this applies to the gatekeepers that sit between consumers and business users and basically would cover search engines, social media platforms, online marketplaces, app stores, so anyone who gets in the middle of a consumer who's wanting to connect with a business online.

[00:01:47.250] - Olivia Mullooly, Partner

In basic terms, the Act establishes a list of dos and don'ts for that platform and the idea of this is to open up the connectivity and I suppose cross use of platforms online. So not forcing users to use a platform service that is associated with maybe perhaps a core platform service that they're using, not having so many restrictions in relation to app stores. There's also going to be restrictions in terms of how the gatekeepers can use end user data for online advertising and target advertising and if they do they would need to get a quite high threshold of explicit consent in order to do so. In terms of when this comes into effect, so potential gatekeepers that meet the quantitative thresholds, so there are thresholds before you can be designated as such and they are quite high so we are talking about the large providers have until the 3 July to notify their services to the commission and following the designation they will have six months to comply with the DMA requirements so really they're looking at next March in order to bring their

operations into compliance. Next up is the Digital Services Act. So this provides for measures to counter illegal goods, services or content online.

[00:02:56.070] - Olivia Mullooly, Partner

There's new obligations on the “traceability of business users” who advertise their products and services online, more safeguards for users. There's a ban on certain types of targeted ads, on how ads are presented, like dark patterns, recommender systems are now regulated in a specific way. There's transparency measures in terms of how content gets regulated, how ads are presented and so forth. There's specific obligations for very large online platforms and very large online search engines which are basically service providers who have users of 45 million minimum per month in the European Union. Just in the last week or so, the European Commission has published the designated list of what we're going to call VLOPs and VLOSEs for the purpose of today's discussion. There's going to be provisions for researchers to get access to key data and generally there's going to be new compliance structures that will need to be set up within the VLOPs and VLOSEs to establish compliance with these new obligations. Then we have some domestic legislation, the Online Safety and Media Regulation Act was signed into law in December, updated the Broadcasting Act, and this was enacted as a response to changes in how content is now consumed as a result of the digital economy.

[00:04:10.710] - Olivia Mullooly, Partner

So this implemented the Audio-visual Media Services Directive. It was a few years late in doing so, but anyway, we got there in the end and it brings into scope of regulation video service providers in terms of audio-visual services on demand and video sharing platforms. It established the basis for creating and enforcing online safety codes against relevant service providers and online service providers. So again, you're talking about the video sharing platforms and any other service on which user generated content is made available. There is a process under which those services that provide user generated content online will be designated by the Media Commission and will be subject to online safety codes and there will be regulation and enforcement around that. For our purposes today, it established the Coimisiún na Meán to replace the Broadcasting Authority of Ireland and within that we have the role of the Online Safety Commissioner. Then we have the Artificial Intelligence Act. This is not yet enacted, so it is currently within the European Parliament. They're due to publish their proposal and then it will go to European Commission negotiations. And then there's like a 24 to 36 month period before it comes into force.

[00:05:27.440] - Olivia Mullooly, Partner

So this is like two and a half years away at least but the proposal is that it will address the risks created by artificial intelligence applications, propose a risk of what's high risk and at its core, there's a classification system for classifying whether an AI system poses a risk or not. Does it pose a risk to safety, does it pose a risk to fundamental rights of users and so forth. So this will be regulated going forward, but we're not there yet. Then we have a child sexual abuse, material regulation. Again, this is somewhat in its infancy, but back in 2021, the Commission introduced this proposal whereby interpersonal messaging services could detect and report and remove child sexual abuse material that was being transmitted through its services and do so on a voluntary basis without affecting its safe harbour exemptions. They're going to formalise that into a more permanent footing because this was only intended to be an interim measure and under this we providers will have to assess and mitigate the risks of misuse of their services and must take measures that are proportionate and subject to robust conditions and safeguards. So here's something that gives us a specific monitoring obligation that will come into effect in the future.

[00:06:40.430] - Olivia Mullooly, Partner

Then we have the Terrorist Content Regulation. This came into force last year, last June, and it's directly applicable in all member states. This applies to all hosting service providers and has a wide range of obligations in respect of the removal, reporting information, notification of content online and setting up again transparency around the measures it takes to comply and also setting up a complaint mechanism for users who object to the fact that their content has been removed on the basis that it has been designated as terrorist content. The sanctions may vary, however, the financial penalties of up to 4% of a provider's annual global revenue generated in the financial year can be imposed. So we're back to kind of GDPR levels of sanctions under this regulation. Just briefly, I'm going to touch on the Data Governance Act and the proposed Data Act. They're not terribly relevant for the purposes of our discussion today, but they will likely have some application in the future and relevance. The Data Governance Act will apply from this September. And basically it sets up a system whereby data intermediation services will have obligations that they will need to comply with by September 2025.

[00:07:48.810] - Olivia Mullooly, Partner

And it basically allows for the reuse of public sector data, so it will harmonise the conditions under which public sector bodies may make their content available. There's no particular obligation on them to do so, but it does set up a framework for that to happen and for the concept of data altruism for people to participate and support research initiatives. Then we have

the proposed Data Act. This is relatively controversial because it is intended to facilitate access to and use of data by consumers and businesses and business to business sharing of data. And there is going to be some, there's continuing, I suppose, controversy about this in terms of the extent to which it will affect or protect trade secrets and so forth but again, this is just a proposal at the moment. The Directive on Copyright in the Digital Single Market, it's a few years old now and it was transposed in 2021 and when I mentioned that the Safe harbour exemptions provided for a notice and takedown regime so you're not liable until you're put on notice and then you take it down for copyright it's notice and stay down. So there's two aspects to this once you're put on notice of something, you must remove it and you must use measures to prevent it being re uploaded again if the platform doesn't have a licence to use it.

[00:09:05.910] - Olivia Mullooly, Partner

There's also an obligation on the platform to use best efforts to get a licence for any copyrighted content that's made available on its platform. In simple terms, it's meant that a lot of online platforms and social media platforms have had to get licences and authorisations from the likes of record companies and so forth to cover any use of, we'll say, music on their platform and that kind of thing so this is a tweak to the notice and takedown regime. In terms of other legislation that's relevant, we have our old friend, the GDPR. This regulates the use of personal data for the purpose of AI, for example, including for direct marketing and advertising and selecting what content is presented to users, and we'll explore that a little further in the next session. E-privacy legislation regulates the use of cookies for behavioural advertising. We have the Unfair Commercial Practises Directive, which prohibits unfair advertising, so including advertising that's misleading or aggressive. And we have the Consumer Rights Directive which was enacted last year under the Consumer Rights Act and this, for example, sets out minimum information that must be presented to a consumer, including whether the pricing was based on automated decision making.

[00:10:15.970] - Olivia Mullooly, Partner

In terms of the key terminology that we're going to be using today, as I say, an intermediary service provider is a hosting mere conduit or a caching provider. An online platform is a hosting service that stores and disseminates user information to the public, not the platforms own content. It's user content and it must be made available to the public. So a private discussion board, a private group, is not an online platform because it's not being disseminated to the public online. An online search engine is what it is. It's an intermediary service that enables users to perform searches of websites and then, as I say, a very large online platform and a very large online service. Or a VLOP or VLOSE is for those entities that have been designated by the European Commission on the basis of the number of users that they have in terms of

harmful content online. This is a concept that exists in the Online Safety and Media Regulation Act. So there's two categories. The first is specific categories that are set out in schedule three, which basically relate to criminal offences. So issues such as restrictions on reporting on criminal trials, so people who may be identified on online platforms or online discussion boards where there's a restriction in place content that itself constitutes a criminal offence, like sexual offences, child exploitation, hate speech, grossly offensive communications and so forth.

[00:11:39.940] - Olivia Mullooly, Partner

Then you have a second category which are specified by law, and currently the categories are bullying or humiliation of a person, promotion of eating disorders, self-harm or suicide, and that's subject to a risk test. So that constitutes harmful content online if it gives rise to a risk to a person's life or significant harm to the person's physical or mental health, where that risk is reasonably foreseeable. So these will be the subject of online safety codes. Illegal content then is a concept under the Digital Services Act. One of the principles of this was that any information that's illegal offline is going to be illegal online. So this is in basic terms, it's information which is not in compliance with EU or member state law either by itself or in relation to an activity such as the sale of a product or service and we're going to explain in our panel discussion with the associates what that will actually mean in practice. What it means for all of you in the room is that any entity that is providing content to an intermediary provider such as a social media or other online platform that hasn't been checked for compliance with law runs the risk of that content being flagged, reported and ultimately demoted, demonetised or removed from the platform.

[00:12:56.500] - Olivia Mullooly, Partner

It will also give you the rights that if you're seeing something that has been said in relation to or let's say unfair comparative advertising and so forth, you do have the rights then to be able to a channel to have that content removed. So hopefully that's given you a sense of the complexity of this area, the various legislative obligations that apply, the different enforcement regimes, regulations are involved.