

# Online Dating Association

Welcome to the first edition of the **Online Dating Association's Industry Update**, where we will bring you an overview of what the ODA has been up to in the last quarter, and a briefing on recent Public Relations and Government Affairs activities.

## Online Dating Association Update

Hannah, our Comms and Policy Director, will be in New York City in a few weeks presenting at the GDI conference, where she will be presenting a 'forward look' of the policy landscape, highlighting what the sector can expect from the 'Digital Regulation Decade'. If you will also be in New York City for the conference and would like to meet, please do not hesitate to get in touch.

The first ODA event of 2022 will be a webinar on the 26th of April, which will focus on new developments in moderation technologies and legal and regulatory regimes in which these technologies operate. We look forward to welcoming the wider sector to this webinar - look out for booking details soon!

We hope you are all enjoying the new website and utilising the best practice resources for the sector and the safe dating resources for the public. Over the next year the ODA will be making regular updates to the website, the standards and guidance, and the safe dating education and resources for the public. If you'd like to be involved in this important work, please do **consider becoming a member of the ODA**. Please reach out to [Ann](#) if you are interested in joining us, we'd love to have you!

We hope you have all seen our recent activity on Twitter and LinkedIn; Make sure to follow [@odassociation](#) on Twitter and [Online Dating Association](#) on LinkedIn to get all our news as it happens.

## Public Relations Update

With the release of the Tinder Swindler, and the usual Valentine's Day interest in dating, the media focus is squarely on romance fraud. We undertook an awareness campaign with the [City of London Police](#) in January, with significant [media pick-up](#), as well as a joint-campaign with [UK Finance for Valentines' Day](#). You may have seen Hannah representing the ODA on the ITV lunchtime news Friday the 11th February, or some of the [print media pick up](#). We expect romance fraud to continue to be a top story in the media; the significant increase in fraud over the pandemic shows no signs of abating and there are new elements emerging too - including relationships started on dating apps leading crypto-currency investment scams, as described in this recent [New York Times article](#). Outside the UK, we supported a romance fraud awareness [campaign in the Netherlands](#) over Christmas, and the FTC in the US is also regularly running [media engagement on romance scams](#). We think this illustrates

a continuing interest in romance fraud across global jurisdictions and something ODA and the sector need to monitor. Up next, keep an eye out for the ODA on the upcoming BBC series For Love or Money, likely to broadcast in May.

The ODA intends to keep working with partners to educate the public on romance fraud; in our public engagement work we always highlight the importance of users remaining on the dating service which allows us the opportunity to illustrate the hard work the sector does to combat scammers and fraudsters. Continued PR and public engagement improves the public's opinion of dating apps, and we intend to do more positive PR, highlighting the wonderful relationships formed from online dating and the role of trust and safety on our platforms. Good PR, and positive public opinion, is beneficial in our advocacy in relation to the Online Safety Bill and other new legislation in other jurisdictions.

In other PR activities, the ODA has also joined the [Coalition for App Fairness](#), which advocates for 'freedom of choice and fair competition across the app ecosystem.' We will be supporting CAF's public and media engagement, including commenting on the on-going [Dutch ACM decision against Apple](#), which relates to alternative payment systems in dating apps. We'll be making the case publicly for pro-competition regimes, like the EU Digital Markets Act, alongside other members of CAF.

Finally, we are regularly approached by Government and stakeholder agencies to support campaigns relevant to dating services. You will have seen the successful ['Booster' campaign](#) in the UK, and we are grateful for those in the sector who engaged; we are now supporting an awareness campaign focused on Violence Against Women and Girls (VAWG). This is particularly important in light of programmes such as last week's BBC programme ['Dating's Dangerous Secrets'](#), highlighting sexual harassment, abuse and assault as a result of 'online dating'; the article is [here](#). These types of exposés are a challenge to the perception of the sector, and we must work together to address them. Working with Governments and other public bodies raises our profile and helps build awareness of the trust and safety work we take seriously in the industry. **Please join the ODA to get involved with these campaigns and public engagement - we cannot deliver this work without the support of members.**

## Policy and Advocacy Update

It has been very busy for the ODA, and the members of the ODA, on the policy front. The 2020s is being touted as the 'Digital Regulation Decade' and it is essential the ODA and the voice of the online dating sector are heard while regulation is designed. TechUK has a [solid overview](#) of the 'digital decade', which is worth a read, as well as [Ofcom's predictions](#). The ODA has joined [TechUK](#), the trade association for the wider technology sector in the UK. Through TechUK, we have the opportunity to engage with multiple government departments and input into sector white papers. The next white paper published by TechUK will be on *'Digital ID'*, and we are collating feedback from ODA members ([read their current position here](#)). With TechUK we have also met with DCMS about the Online Safety Bill, addressing key concerns from the online dating sector, including the recent inclusion of a 'fraud' offence in the Bill. We have also begun meeting with Ofcom, who will be the regulator for the online safety regime and put forward both concerns and opportunities for our sector in

the new regime. Ofcom were particularly interested in speaking to our sector about fraud, including our frameworks for tackling frauds and scams. **I would urge any organisations concerned about new digital regulation and its impact on their businesses to consider joining the ODA for the latest updates on policy and regulation, and the chance to make their voice heard with Government, stakeholders and regulators.**

### Online Safety Legislation

If you would like to read more about the Online Safety Bill in the UK, TechUK has done an excellent [synopsis of the Joint Committee report](#) in December; we are still expecting the new Bill in mid-March. Since the original draft of the Bill was published, a further list of [priority illegal harms](#) has appeared, which will be added to the Bill. In scope companies will be required to proactively tackle these offences through risk assessments, and firms will need to make sure the features, functionalities and algorithms of their services are designed to prevent their users encountering them and minimise the length of time this content is available. Having these processes will be essential to the risk assessment performed as required by Ofcom's codes of conduct. These new offenses include online drug and weapons dealing, people smuggling, revenge porn, fraud, promoting suicide and inciting or controlling prostitution for gain as well as three new Communications Offences recommended by the Law Commission which are:

- A 'genuinely threatening' communications offence, where communications are sent or posted to convey a threat of serious harm
- A harm-based communications offence to capture communications sent to cause harm without a reasonable excuse
- An offence for when a person sends a communication they know to be false with the intention to cause non-trivial emotional, psychological or physical harm.

There will also be a new offence of 'cyberflashing', for which dating app Bumble has been advocating. Cyberflashing can be either the sending of unwanted sexual images over free public wifi (for instance on a bus) or the sending of unwanted sexual images through a messaging service. You may also have seen an addition to the Online Safety Bill requiring [age-verification for pornographic sites and apps](#) – we will be keeping an eye on this development, as it could set the precedent for other services which children are not meant to access.

In Europe on the 20th of January, The Digital Services Act (DSA), was passed by the European Parliament. Parliament introduced several changes to the Commission proposal, including imposing more stringent content moderation rules, exempting micro and small enterprises from certain obligations, and strengthening transparency and consent requirements for targeted advertising. The European Council had agreed its position on the proposal for a Digital Services Act in November 2021 and the trilogues (an equally composite tripartite meeting between those involved in the legislative process of the EU institutions) continue. A good overview of both the DSA and DMA (Digital Markets Act) can be found [here](#), and [this is an excellent analysis](#) of how the DSA will be enforced. Once the DSA has passed, it is likely each member country will draft specific Online Regulation Bills to deal with elements of the DSA for individual countries, much like Ireland's [Online Safety and Media Regulation Bill](#).

In the USA, two senators introduced [KOSA, the Kids Online Safety Act](#), which would apply to entities that are likely 'to be used by a minor', and would require entities to have a duty of care towards minors in their products and services as well as an opt-out recommendation on minor's personal data. Another online safety bill, [the EARN IT Act](#), was again before the Senate Judiciary Committee, where it was unanimously passed. It will amend Section 230 to allow lawsuits against internet companies that advertise, promote, present, distribute or solicit material depicting the sexual abuse of children. However, there is significant opposition to this amendment by privacy, human rights and freedom of speech groups in the USA.

Overall, you can see online safety is at the top of the agenda for a number of jurisdictions, and it is likely online dating services will be caught by legislation and regulation in some way. It is the ODA's role to both advocate on behalf of the sector, and to work with Governments for sensible regulation beneficial to all.

### Pro-Competition in Digital Markets

As mentioned earlier, the ODA has joined CAF, the [Coalition for App Fairness](#), which advocates for fair competition in digital markets and for all developers. This movement is particularly important in light of the recent decision in the Netherlands by the Dutch Competition Authority (ACM), that Apple must allow dating apps to use other payment providers. Prior to this decision, there was a pro-competition decision in South Korea, and the Government there has been working to make [big tech comply](#).

In Europe, the Digital Markets Act is in trilogue, and is likely to be finalised this year. The DMA will create a pro-competition regime in the EU and label certain companies with a 'core platform service' with gatekeeper status; these companies will have to comply with further regulations. The DMA may overtake the Dutch ACM decision and change the landscape for big tech across Europe. In the UK, the [mobile ecosystems market study](#) is the first step by the Competitions and Markets Authority to investigate pro-competition regimes in digital markets, and the CMA has set up the Digital Markets Unit, which will soon become statutory. We expect to see a Bill later this year, and the DMU will have the power to oversee entities with 'strategic market status', which is similar to the 'gatekeeper' status in the EU. TechUK has a [review of UK proposals](#) to increase competition in digital markets which is a useful read

In the USA, there are two major bills in the Senate - [Open App Markets Act](#) and the [American Innovation and Choice Online Act](#) - that deal with pro-competition regulation, and echo much of the Digital Markets Act. The OAMA and AICOA have both passed the Senate Judiciary Committee, though the proposals raised questions about moderation and security alongside praise from anti-monopoly watchdogs

### Data Protection & Privacy

In the UK, the government is reviewing GDPR with the [National Data Strategy Update](#), in which the Government has published frameworks for a future data strategy for the UK. There is also movement on the global flow of data through the [International Data Transfer Expert](#)

[Council](#) and the [International Data Transfer Agreement \(IDTA\) laid before Parliament by DCMS](#). The aim of this work is to help organisations ensure they have the correct protections when transferring people's data outside of the UK to countries not covered by adequacy decisions.

The European Commission rolled out [the EU Data Act](#) , a new proposal regulating the extent tech platforms can use or share consumer data. The EU and the US are also working on finalising a data adequacy agreement, the 'Privacy Shield' issue, in the EU-US Trade and Technology Council, with a likely announcement in May.

In the USA, is it likely at some point the Federal Government will need to pass a data protection Bill, as the 'patchwork' of privacy laws that are slightly different across the nation could lead to compliance costs exceeding \$1 trillion, [according to the Information Technology and Innovation Foundation](#). Last month also saw the unexpected failure of the Arizona bill that would have given developers a way to avoid fees imposed by Apple and Google's app stores. This bodes poorly for state efforts elsewhere, as 'big tech' becomes more aggressive in their lobbying.

### Cyber Security and Artificial Intelligence

The UK Government has announced its [Cyber Strategy for 2022](#), which includes funding for the National Cyber Security Programme and £2.6billion investment across 5 key pillars, including training for young people in cyber skills and the establishment of a National Cyber Advisory Board to bring together senior leaders across Government, the public and private sectors to discuss approaches to cyber resilience. The UK [Government's AI Strategy](#) has also been published.

In the EU, a joint committee of IMCO and LIBE launched Parliament's work on the [Artificial Intelligence Act](#) with an exchange of views. Introduced in April 2021 and currently under consideration in the European Parliament, the EU's AI Act looks to assess and label potential risks posed by aspects of AI tech. In the USA, Democrats are looking for stronger legislation to empower the FTC to mandate transparency of AI algorithms, with the [Algorithmic Accountability Act](#). Both cyber strategy and AI are important for the dating sector to monitor, as some changes may impact our platforms and services.

## Conclusion

To reiterate, a big thank you to everyone who supports the Online Dating Association. Please follow [@odassociation](#) on Twitter and [Online Dating Association](#) on LinkedIn to get all our news as it happens, and consider joining us as a Member or an Associate to make your voice heard.

We look forward to working with you all in future, whether as members or across the wider community. Please do not hesitate to get in touch with me to discuss anything further.

**Dr Hannah Shimko**  
**Comms and Policy Director**  
**[hannah@onlinedatingassociation.org.uk](mailto:hannah@onlinedatingassociation.org.uk)**