Online Dating Association

The Online Dating Association (ODA) welcomes the opportunity to comment on the White Paper.

Our response to the specific questions are set out below. We hope it is helpful also to share some general reflections which informed our answers to specific questions. Our top line messages are:

1. We agree further action is needed to address online harms.
2. Online harms, like harm in the physical world can take endless forms.
3. Regulation should only happen when and where necessary. It should, per Ofcom and other guidance, be objectively justified and the minimum necessary to achieve the goal set.
4. If any legislation and regulation is not to affect every provider of any kind of Information Society Services (ISS), the Government needs to focus down on the specific goals it wishes to achieve and on the hosting and other services that relate to these harms.
5. Online dating services have a single reference in the White Paper: reflecting the specific singular purpose services provide and their irrelevance to the harms highlighted in the White Paper.
6. We think the Government right not to propose regulation specific to dating services.
7. Dating service providers will continue on a voluntary basis to apply age rules to use of their services and will continue to develop mechanics for ensuring this policy is applied.
8. An approach that prioritises the risks to be addressed by any new regime should not reach into matters already addressed by existing law and existing regulators. Any new regulatory body should focus on social media providers that host, promote and accelerate content that could cause serious offence and encourage harmful actions.
9. Targeting is critical to adding value and delivering new protections without causing regulatory conflict, overlaps, inconsistences and an approach that is contrary to existing Community law relating to providers of ISS.
10. Proportionality matters. Most members of the ODA are UK based UK-focused entities of varied but unexceptional scale. Measures that seem proportionate to global social media providers could cause severe damage to UK businesses if applied to all and sundry and in a standard format

Scope

The first is that almost every entity, commercial, voluntary, regulatory or social is an internet entity to some degree: every neighbourhood or Allotment or PTA group - almost every trader. The White Paper references various harms but it is difficult to see how they relate to the vast majority of entities and, indeed, how far they practically extend beyond those who provide forms of social media and contact platforms that allow the publication, sharing and broad distribution of content.

The second is the need to explore whether the issues of concern are issues “everywhere” and not specific to the digital space. Most are, inviting us to reflect on if and why we see different behaviours online to those we experience “face-to-face”.

That, in turn, means taking proper account of the pre-existing legal frameworks around e-Commerce and the duties on providers of ISS and related law setting out the legal responsibilities on defined categories of providers.

Equally important is the need to recognise pre-existing legislation that addresses commercial and contractual practices. Care should be taken not to bring forward legislative and regulatory proposals in the name of "internet safety" that may overlap seriously or even conflict with existing law that addresses forms of activity that occur on and off-line and which are the subject of legislation with universal application. That is the case, for example, with consumer rights under Unfair Commercial Practices and other consumer protection legislation, rights to dispute resolutions mechanisms, and duties in relation to misleading advertising.

The White Paper recognises the need for proportionality of approach and for the targeting or prioritisation of action to address those harms of most concern that are not addressed by the EU and UK statute books today.

Definitions matter

We feel the White Paper is vague or inconsistent in some of the language used.

The reference to "companies" but not to other entities raises questions over coverage and ensuring duties and responsibilities sit as they should.

The references in Section 3 to "companies and their users" might be seen, understandably, to refer to Facebook and other recognised social media brands with a direct user base.

But what of other models? A company proving some social media hosting platform capacity to societal, faith, interest or other groups has responsibilities under existing law as a provider on an ISS. It can be argued that these duties could be added to. But is it appropriate to treat a technological "host" of ISS with little or no brand and no direct users or user interaction, as you treat Facebook and their like? If not, how should the regime address the individuals and entities that create and share or publish illegal or legal but hateful and unacceptable content? These are not "companies".

In terms of coverage, care is needed to clarify whether a proposal addressing "companies" (Section 3 Page 41), applies to all companies that provide ISS, to user-facing entities or to social media providers as "relevant companies".

We argue any binding Code that seeks to address the core harms flagged throughout the White paper (Child Sexual Exploitation and Abuse, terrorism, abuse related to race, faith, sexual orientation etc) should.

Consultation Questions:

Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

We believe the critical issues within the proposals for transparency reporting are coverage and proportionality. The references are to "companies" and then to "relevant companies". Limiting the coverage to companies as defined in law may lose entities that have a direct and substantial engagement in the issues that most concern the government and society.

Conversely, there is a need to look with care at which companies or entities are "relevant". The harms referenced and the activities described are quite specific to forms of social media that enable the sharing and potentially wide promotion or "acceleration" of content and opinion or victimisation of individuals or groups.

Other services such as dating services and online sale or auction services do not have these characteristics. They exist for a simple purpose: to allow individuals to post some form of profile online and to provide communications and other support to allow people to make one-to-one contact for whatever purpose the service exists to provide: new friendships, social interaction, romance and often marriage in the case of dating services.

Such services have no mechanic whatsoever for those with hateful or harmful content to pitch it to a community of users as can happen on an open social media platform.

This does not mean a dating service or other online service providers should not look carefully at how, where and when their service could expose a user to some form of risk that is different to those set out in the White paper or to some sub-set of those listed. It would be a retrograde step if harmonised rules designed for social media and equivalent platforms were to constrain the discretion dating and other online services have (and exercise) at their own discretion to remove individuals they thought posed a threat to others and to the online experience.

It is right to remind all ISS providers with a user/public interaction of the case for such an assessment, and to signpost good practice that might be followed by all in terms of clarity over terms and conditions of use, in giving users access to reporting mechanisms and in dealing with users concerns. But that does not mean it necessary to apply extensive regulation on each and every merchant, charity or other site simply because they operate an ISS.

In the case of dating services, the ODA has taken a lead in producing a set of standards and good practice guidance and links to advice from the Information Commissioners Office (ICO), Competitions and Markets Authority (CMA) and law enforcement bodies. This addresses our decision as a sector not to allow under 18s to use dating services, and the wish to give clarity over the costs and terms of use of services including personal behaviour. The standards address action that should be taken to block potential scammers and advice and guidance to users on how they themselves can minimise this risk and the possible risks that are there when any two people meet for a first time. And, consistent with the approach in the White Paper our standards and guidance refer to services having reporting mechanics and the ability to remove profiles of offenders.

We are sure similar mechanics are there on other services set up to allow this sort of one to one contact for whatever purpose. We believe our sector has taken a lead in showing this responsibility even though the very structure of services mean it is not a means by which child sexual exploitation, terrorism, race and other "hates", fake news and the other harms identified on social media can be advanced.

We would strongly encourage the Government to look both at the nature and functional structure of services when deciding how to define which "companies" or entities are relevant when targeting the regulatory requirements to the harms identified. In explaining why dating services are not "relevant" we are also saying it is right to take this opportunity to ask all digital businesses to give thought to when and how guidance and good practice for social media providers could help them identify and manages risks specific to their sector or activity.

Question 2: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

This question is impossible to address based on a single short paragraph in the White Paper. Box 24 refers both to "harmful online activity" and to many feeling "social media providers" do not take complaints seriously. If the relevant companies in this regard are social media providers, the concerns below over any extended liability may be mute.

There is reference to "redress" without comment on whether this is social (a public apology?) or financial or in some other form.

This goes to the need to the different roles of different entities and the duties and responsibilities appropriate to those roles. Profound differences exist between Instagram and Facebook as social media entities who host, generate and distribute content that may or may not offend, to the likes of eBay who facilitate offers and purchases between two individuals or entities, or a dating company that helps Person A find and engage with Person B.

In the case of dating services operators already take a package of actions that reflect their commitment to dealing responsibly with their customers. The standards and best practice that relates to these activities can be found at https://www.onlinedatingassociation.org.uk/standards-guidance.html. Operators have monitoring and reporting arrangements and the ability to remove a user/profile that is a threat to others. These exist to address the harms that might arise with one-to-one communications and then one-to-one meetings and dates. These are materially different from the social media risks and harms identified in the White Paper: see above.

The Government needs to distinguish clearly between the adequacy of complaint handing processes of relevant social media providers, and the limit to which the likes of a dating service or selling or auction site can be liable for events of any nature, which could take place between members or subscribers during online interactions with other members or subscribers, whether through the service itself or through Third Party channels of communication, or, in the case of dating, during actual dates.

The issue of designated bodies is raised but the White Paper offers little by way of examples or possible models. Designated bodies or "super-complainants" may have relevance where it is argued there is some form of widespread contravention of a statute or substantive procedure: as there is with financial services and consumer protection law where independent bodies such as PostWatch and Citizens Advice can make representations to the CMA.

Even with a narrow definition of "relevant social media companies and entities" it is difficult to see the fit between a structure for super-complainant bodies and the relatively narrow scope of the scope of the proposed regulation and the proposed Duties of Care.

We would argue that any mechanic for recognising super-complainant be as robust and challenging as exists under consumer protection law dating to the Enterprise Act 2002. This is reflected in the subsequent Treasury guidance on super-complainants and the Financial Conduct Authority (see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200454/guidance_for_super_complainants_120313.pdf). It is not clear that many or any of the associations, charities and interest groups in the social media field would meet these tests vis capacity, independence and objectivity.

We do not believe this approach is needed.

Question 2a: If your answer to question 2 is 'yes', in what circumstances should this happen?

Not Applicable.

Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

We would be wary of over-engineering here. We think it right that service providers own the relationship with their user/customer.

With dating services, we have found criminal actions, particularly the most serious, are generally reported to the police by users ahead of any referral to the service provider. We do ask that users report any action or concern to the service provider too as this allows them to remove profiles and potentially alert others who might be at risk. We signpost other agencies that can provide advice, guidance and support. We do not think it is healthy, however, to refer users with an issue away from the service provider unless there is clear cause.

Question 4: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

Others are better placed to reflect on the form and balance of governance and accountability. There is major understandable political interest in issues around internet safety and online harms, including harm to the democratic process. There is also, however, risks if issues start to be addressed based on populist behaviours and personal opinion rather than a robust dispassionate evidence-based assessment. Regulators and Departments that are open to judicial and other external review. Parliament would surely reserve the right to carry out Select Committee scrutiny if this seemed necessary. We do believe, however, that judicial review provisions help ensure balance and objectivity.

Question 5: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

We see a need to clarify the terms used in Section 4.2. Dating services allow users to post profiles in order to allow individuals then to engage in private one-to-one communications. This facility, as perhaps with a sales site like eBay, support bilateral contact for a singular purpose. They do not facilitate forms of sharing material or comment with any wider community.

We understand a government wish not to define coverage in ways that may leave gaps that may be problematic at a later date, but the definitions used, like those used by the ICO in relation to "Age Appropriate Codes" may end up capturing every provider of an ISS as already defined in EU law.

Assurances of a proportionate approach are welcomed given the seriously limited relevance of dating services to the harms the White Paper lists. It is not comfortable, however, for a large number of businesses and other entities to be in a state of uncertainty as to when, how and why they are subject to any new regulatory regime. Alongside proportionality the Better Regulation Principles stress the importance of "Targeting".

The White Paper does focus on proposals relating, in effect, to forms of "social media" while rehearsing worries over threats to child safety, bullying, political interference, terrorism, unhealthy level of use of online services/social media, eCommerce, crime, the promotion of gambling and more. This may help as an aggregation of issues from which to identify and prioritise actions. But that analysis and targeting is needed to avoid a "cover all: achieve less". In Section 3 (Box 24) there are proposals for new complaint handling responsibilities. The language references online harm but is silent on how specific or general the proposal is. Law and customer service arrangements already exist to deal with a misleading deal on an auction platform or a date that went badly after online communications. But the problems and exposure or uncertainty multiplies when a concern almost certainly anchored in social media behaviours translates into duties that are wholly imprecise that may or may not apply to online traders and service providers and communications businesses generally.

Dating services generally provide dedicated communications platforms as a measure of assurance and security against anyone seeking to perpetrate a fraud. Our understanding from work carried out by the National Fraud Intelligence Bureau (NFIB) is that one behaviour reported by victims of fraud is where a scammer persuades the victim to come off of these dedicated platforms and onto insecure and untraceable channels like WhatsApp.

Question 6 In developing a definition for private communications, what criteria should be considered?

The White Paper refers to addressing highly defined illegal behaviours. We agree the test must be this high one… forms of illegal content and activity defined in the statute or regulations.

Dating services provide communications platforms to deter those possibly intent on fraud. A set up that does enable correspondence to be examined and shared with law enforcement in the event of an incident is a valuable deterrent. It would be a large and contentious move for the Government to create a broad exemption to the current privacy rules surrounding personal communications in anything but the most severe circumstances.

Question 7: Which channels or forums that can be considered private should be in scope of the regulatory framework?

We look to privacy experts and legal agencies to address this question.

Question 7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

Others are better placed to respond. When issues have arisen over harms on a dating service the sector has been ready to cooperate with Court Orders and RIPA requests. Going forward there needs to be clarity over the legal powers that exist and the mechanics for their exercise. Companies holding possible sensitive personal data need the assurance those seeking this data are properly authorised to do so. They cannot otherwise be asked to support actions of uncertain provenance.

Question 8: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

No comment here.

Question 9: What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

No comment.

Question 10: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body? Question 10a: If your answer to question 10 is (ii), which body or bodies should it be?

There is no obvious and assuredly "right" answer to this question. If a new regulator is created there is a further need to clarify regulatory boundaries between this entity and those regulators and law enforcement agencies that already have a necessary and substantive interest in issues of online safety.

Indeed, it could very well be argued that any activity that is already criminal already has an agency with the duty to prevent or prosecute these crimes. That is true on some broadcast/publication/communications issues, of data protection, of action against unfair commercial practices and other matters.

If there is a concern already there it is over the apparent efforts of regulators with defined core duties seeking to use these to assume far broader social responsibilities. This would seem to be the case with the ICO if the Commissioner is seeking to give a lead in deciding when and how services can be offered to children, and when and how children should be refused access to pretty much any ISS.

Accordingly, we do not believe a new regulator with wide ranging responsibilities that include matters already addressed by existing agencies makes sense. If, as we would support, the regime brought forward after this process is specific to some identifiable community of social media and networking providers and harms not addressed elsewhere (the legal but potentially harmful category) then there is a case for a body specific to that activity.

Question 11: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

If a targeted regime (see 10 above) is introduced in relation to social activity that is unwanted but not contrary to any statute, there may be a case for saying this is a choice of the State with the costs met by the State.

If any form of levy or fee is required it should address the community the regime applies to directly and who generate the majority of reporting and regulatory activity required.

There is no reason why the generality of Internet sites that do not host or facilitate the harms identified should meet the costs of monitoring or policing the behaviours of others.

Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

We do not believe this regime should apply to dating sites given the wholly limited mechanics they provide for anything other than one-to-one communication for a single purpose.

If the regime fundamentally exists to encourage social media and similar providers to use systems, best endeavours and reporting and trend analysis in relation to user-based/user-generated activity and content there needs to be a real measure or test of practicality and proportionality in situations where entities may be unknowing hosts of material they did not produce, do not condone and will remove.

Any arrangements must be consistent with the terms in which the eCommerce and other directives address providers of ISS who purely host, or who publish or who "accelerate" content or allow such content to be distributed widely.

Question 13: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

No comment based on the interests of dating companies and the applicability of most proposed provisions.

Question 14: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

Yes, if the regulator's power to make decisions are wide and may directly affect the continuing ability of an entity to trade.

Question 14a: If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

See above: when a regulatory decision makes a material impact on the ability of a company to continue to offer its services.

There may also be circumstances where a regulatory decision could have profound impact on competition in a marketplace for digital services and, therefore, the risk that complaints are driven by some competitive agenda rather than an interest in the public good. That is certainly the case with matters before Ofcom Tribunals.

Question 14b: If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

An appeal to the regulator should be based on the Code, the actions and the merits of the case.

This as the primary mechanic may not remove the right a party has to seek a judicial review. At that point we assume the principles relating to a judicial review would apply.

Question 15: What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

Others with a wide and more substantial interest are better placed to respond to this question. So-called "big-data" and Artificial Intelligence or simply smarter analysis of data, trends and behaviours must be an aid to identifying and addressing harms faster. The Government must set out its top priorities and recognise when and why this means individual arms of Government must restrain their wish to apply "pure" interpretations of Statute.

We do not think it right and sensible for the ICO to be the agency that prescribes when and how forms of age verification or identity checking is done on digital services "off the back of" its general requirements over the security and use of personal information. Similarly, there are bound to be situations where government agencies, law enforcers and others should be able to share and process data to prevent harm.

In these circumstances it is important that any business that is required to share data they hold on individuals knows there is a robust and understandable basis for requesting such information. Entities should not feel or be at actual risk of being charged with a failure to co-operate where the duty to cooperate is not clearly communicated and understood. Equally entities should not be at risk of breaching data protection and privacy or other law by co-operating with requests from law enforcement agencies or others, when those requests do not have a legal footing and leave the entities in breach of data protection law.

Question 16: What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

This is not clear at this time. As the issue seldom relates to dating services our contribution may be limited. One issue which does relate to dating and must relate to some social harms reported in social media, concerns the privacy or otherwise of personal communications.

Dating services create communications platforms that allow users to "chat" in an environment where the activity has a digital fingerprint….where those intent on wrongdoing know they may be identified and their activities discovered. This is one core safety message we push: stay on the messaging site: it's safer; and be wary of anyone trying rapidly to shift you off such sites.

That is not the same as saying a service provider will use human or digital monitoring of private one-to-one communication as people seek new friends, dates and partners. Services cannot cross lines in existing privacy legislation. Any guidance must address where these boundaries are, how they are explained, and how they inform any liability on an entity related to private communications.

Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

Dating services are exclusively for over 18s. We are not best placed, therefore, to comment on how parents manage access to other online material or deal with physical or mental threats, bullying and other harms set out in the White Paper.

We recognise the value in teaching parents how they can manage access controls on smartphones and tablets as well as home computers and laptops. Internet Matters provides good guidance on this while recognising the answer is complex and goes beyond technological barriers.

Question 18: What, if any, role should the regulator have in relation to education and awareness activity?

See above. Educational issues do not fall with our remit and we defer to other respondents on this issue.

1 July 2019

Online Dating Association **Web:** www.onlinedatingassociation.org.uk
Email: info@onlinedatingassociation.org.uk