Submissions to the DRCF's 2023/24 Workplan – Call for Input D-N

Content

7. Dawes Centre for Future Crime at UCL

This submission outlines the views of the Dawes Centre for Future Crime at UCL (DCFC) about issues that the Digital Regulation Cooperation Forum (DRCF) should take into consideration as it develops its 2023/24 workplan.

The submission offers answers to all the questions included in DRCF's Call for Input, namely:

> *1. Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.*
> *2. In line with the 'factors we consider when prioritising work' (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan?*
> *3. Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?*

The Dawes Centre for Future Crime: background and expertise

The DCFC aims to forecast both the nature and spread of future crimes emerging from technological, social and environmental change and to propose methods for tackling them effectively before they become established. Research projects at the Centre aim to answer complex questions related to ground-breaking technologies, such as future crimes facilitated by the metaverse,[14] crime enabled by Artificial Intelligence (AI),[15] online fraud,[16] and cryptocurrency fraud and money laundering.[17]

To achieve these objectives, the Centre has, and works with, a team of researchers from different disciplinary backgrounds who have developed considerable experience in designing and employing innovative and collaborative methodologies, as well as working with a broad network of stakeholders. These include **two DRCF's member regulators** – namely, the **Financial Conduct Authority (FCA)** and **Ofcom**. Other stakeholders include organisations from **government** (e.g. Department of Culture Music and Sport, Home Office, Ministry of Justice, Defence and Science Technology Laboratory, National Cyber Security Centre), **law enforcement** (e.g., Action Fraud, CIFAS, City of London Police, College of Policing, Europol, Interpol, National Crime Agency, National Police Chief's Council), **industry** (e.g., British Retail Consortium, Instagram, Meta,

[14] https://www.ucl.ac.uk/future-crime/publications/2022/aug/scoping-study-future-crime-challenges-metaverse
[15] https://www.ucl.ac.uk/future-crime/publications/2021/may/future-crime-opportunities-arising-artificial-intelligence-ai
[16] Johnson, S.D. & Nikolovska, M. (2022) 'The Effect of COVID-19 Restrictions on Routine Activities and Online Crime'. *Journal of Quantitative Criminology*. Available at: https://link.springer.com/article/10.1007/s10940-022-09564-7
[17] Trozze, A., Kamps, J., Akartuna, E.A. *et al.* Cryptocurrencies and future financial crime. *Crime Science* 11, 1 (2022). Available at: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-021-00163-8

Elliptic, Tech UK, and the World Bank), and the **voluntary sector** (e.g., Age Concern, Age UK, Neighbourhood Watch, Suzy Lamplugh Trust, Worshipful Company of Information Technology).

The outputs of many projects conducted at the DCFC include not only academic publications but **policy briefs** seeking to inform the practice of policymakers, regulators, law enforcement agencies, and industry. A full overview of all the projects of the Centre and their policy briefs are available on our website.[18]

The DCFC also funds and supervises a wide variety of **PhD research[19]** and is committed to delivering **professional training** and promoting **knowledge exchanges** with relevant partners and stakeholders.

1. Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.

- **Crime-enabling technologies:** The 2021/22 and 2022/23 DRCF's workplans focused on the challenges of specific technologies such as design frameworks, algorithmic processing, digital advertising technologies, and end-to-end encryption. This **technology-specific focus** is very welcome as each of these technologies raises different issues and risks. It is advisable that in 2023/24 the DRCF expands this focus to other emerging technologies that, while promoting innovation and growth, can threaten individual and public interests. The DRCF's 'Joining up on future technologies' horizon scanning programme[20] has already identified some of these technologies, such as cloud computing, privacy enhancing, distributed ledger, Artificial Intelligence, quantum technologies, 'Internet of Things' (IoT), cybersecurity technologies, the metaverse and immersive technologies, and biometric technologies.

  Of course, focusing on all these technologies might be unfeasible and a selection based on a **prioritisation exercise** might be required. We suggest that the **prediction and prevention of crime risks** should be one of the criteria for prioritisation. Crime causes considerable societal and individual harms. Therefore, understanding, assessing and preventing crime risks should be a priority for all the DRCF's member regulators. The research conducted at the Dawes Centre can support such prioritisation exercise by identifying technologies which can produce such risks. These include:

a) **The metaverse:** The DRCF has already started addressing the regulatory implications of the metaverse. On 17 May 2022, as part of its horizon scanning programme, the DRCF brought together industry, analysts, academics, government and regulators at its 'Metaverse

[18] For our research projects, see: https://www.ucl.ac.uk/future-crime/research-0 . For the policy briefs, see: https://www.ucl.ac.uk/future-crime/policy-briefs

[19] For PhD research conducted at the Centre, see: https://www.ucl.ac.uk/future-crime/phd-research

[20] https://www.gov.uk/government/publications/joining-up-on-future-technologies-digital-regulation-cooperation-forum-technology-horizon-scanning-programme/joining-up-on-future-technologies

Symposium' to exchange ideas and perspectives on the potential implications of the metaverse and associated immersive technologies for people,[21] businesses and the wider economy.[22] A recent scoping study by the Dawes Centre including a systematic literature review and stakeholder workshops (involving academics, researchers, industry, government, and relevant professional bodies) mapped existing, emerging and future criminal threats of the metaverse and identified the most critical ones that require immediate attention. The study also showed that in order to address and prevent these threats a complex regulatory framework involving all the DRCF's member regulators is required. Therefore, metaverse technologies and their manifold crime risks should be a priority for the next DRCF's workplan.

b) **The Internet of Things (IoT):** IoT devices have the potential to transform society, but they also provide opportunities for crime. For example, some devices (including 'security' cameras) lack basic password functionality or allow the use of default passwords which can easily be guessed or even found in online forums. Many IoT devices sold to consumers lack basic cyber security provisions, leaving responsibility with the consumer to undertake tasks such as changing the default password and installing software updates. Research conducted at the Dawes Centre[23] explored how consumer IoT can be misused for crime, what security features are provided by manufacturers and what information is available to consumers, as well as relevant policy implications, including those related to the Department for Digital, Culture, Media and Sport (DCMS)'s Security by Design Code of Practice.[24] A 2021 report by UCL scholars commissioned by DCMS's Secure-by-Design team identified shortcomings of the current Code of Practice and recommended policy and regulatory measures to improve it.[25] As explained in DRCF's 2021/22 workplan, design frameworks and the Code of Practice are relevant to all DRCF's member regulators.[26] The pervasiveness and harmfulness of criminal threats enabled by IoT technologies suggest that these should be an area of priority in the next DRCF's workplan.

c) **Cryptocurrency:** This is another technology area that requires urgent attention. Studies conducted at the Dawes Centre identify cryptocurrency as an enabler of large-scale financial

[21] https://www.ucl.ac.uk/future-crime/publications/2022/aug/scoping-study-future-crime-challenges-metavers

[22] https://competitionandmarkets.blog.gov.uk/2022/06/22/the-metaverse-and-immersive-technologies-a-regulatory-perspective/

[23] Johnson, S.D., Blythe, J.M., Manning, M., & Wong, G.T.W. (2020). 'The impact of IoT security labelling on consumer product choice and willingness to pay'. *PLoS ONE*; Blythe, J.M., Sombatruang, N., & Johnson, S.D. (2019). 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?' *Journal of Cybersecurity*, 5(1); Blythe, J.M., Johnson, S.D. (2019). 'A systematic review of crime facilitated by consumer Internet of Things'. *Security Journal*; Blythe, J.M., & Johnson, S.D. (2018). 'The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. *IET Conference*; Blythe, J.M., & Johnson, S.D. (2018). 'Rapid evidence assessment on labelling schemes and implications for consumer IoT security'. DCMS: London; Blythe, J.M., Johnson, S.D., & Manning, M. (2019). 'What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices'. *Crime Science*.

[24] See: Johnson, S.D., Blythe, J.M., Manning, M., & Wong, G.T.W. (2020). *How Secure is IoT?* Available at: https://www.ucl.ac.uk/future-crime/policy-briefs/policy-brief-how-secure-consumer-iot

[25] Datta Burton, S., Tanczer, L.M., Vasudevan, S., Hailes, S., Carr, M. (2021*). The UK Code of Practice for Consumer IoT Security: 'where we are and what next'*. The PETRAS National Centre of Excellence for IoT Systems Cybersecurity. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978692/The_UK_code_of_practice_for_consumer_IoT_security_-_PETRAS_UCL_research_report.pdf

[26] https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022#the-2021-22-drcf-workplan

crimes, such as extortion, pump-and-dump schemes (a type of market manipulation), money laundering, crypto money mules, cryptocurrency theft, cryptojacking and investment scams.[27] Such crimes can harm a variety of public and private interests, from personal identity and property to financial stability and market integrity. As such, they require complex regulatory responses addressing the behaviour of various actors involved – from financial services providers to potential victims.[28] As a result, cryptocurrency crimes are relevant to all the DRCF's member regulators – especially FCA and CMA – and should be another priority in the next DRCF's workplan.

d) **Biotechnologies:** digital technologies are empowering considerable advances in biotechnologies, which integrate natural and engineering sciences to modify living organisms. For example, artificial intelligence allows the automation of laboratories, while the Internet allows such laboratories to be connected around the world. Research at the Dawes Centre shows that the complex integration of digital and biotechnologies can enable transformative research, but also harness considerable risk of harm and regulatory challenges.[29] For instance, fully automated and internet-connected laboratories can create opportunities for data exploitation across geographic boundaries, as well as the manipulation and misuse of biological material. Internet-connected laboratories could also be used to bypass regulations of a country to conduct experiments in a country which would allow these. Cyber-biotechnologies also entail crime risks, such as bio-discrimination, cyber-biocrime, bio-malware, bio-hacking, illicit drug manufacturing, illegal gene editing, genetic blackmail and neuro-hacking.[30]

Misuses of cyber-biotechnologies are of particular concern for both IMO and Ofcom, as they often exploit online services or gaps in cyber security and involve the use or manipulation of personal data. We advise therefore that the next DRF's workplan includes initiatives to develop an adequate awareness and understanding of the risks of cyber-biotechnologies to support the coordinated and collaborative design of appropriate regulatory solutions.

2. In line with the 'factors we consider when prioritising work' (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan?

- **A joined-up approach to future-proofing regulation:** one of the main objectives of the DRCF is to 'anticipate future developments by developing a shared understanding of emerging

[27] Trozze, A., Kamps, J., Akartuna, E.A. *et al.* Cryptocurrencies and future financial crime. *Crime Science* 11, 1 (2022). Available at: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-021-00163-8

[28] Akartuna, E.A., Hetzel, F. & Kleinberg, B. (2021) *Cryptocurrencies and future crime*. Available at: https://www.ucl.ac.uk/future-crime/sites/future_crime/files/ucl_cryptocurrencies_and_future_crime_policy_briefing_feb2021_compressed_1.pdf

[29] Elgabry, M., Nesbett, D. & Johnson, S.D. (2020) A Systematic Review of the Criminogenic Potential of Synthetic Biology and Routes to Future Crime Prevention. *Frontiers in bioengineering and biotechnology*, 8, p.1119. Available at: https://www.frontiersin.org/articles/10.3389/fbioe.2020.571672/full

[30] Elgabry, M. & Johnson, S.D. (2021) *Synthetic biology and future crime*. Available at: https://www.ucl.ac.uk/future-crime/sites/future_crime/files/synthetic_biology_and_future_crime_final_021221.pdf

digital trends, to enhance regulator effectiveness and inform strategy'.[31] The work of the DRCF in this respect is very timely and welcome. Foresight of future technological and social changes is paramount to develop future-proof regulation – that is, regulation that proactively anticipates change, prevents harms and promotes desirable outcomes.

- The DRCF has already taken some first steps in this area by promoting a joined-up approach on future tech which focuses on three initial priorities: improving awareness of and accessibility to DRCF members' digital research; jointly engaging with UK small to medium sized companies (SMEs), tech start-up community and academia; accelerate DRCF's knowledge building in new or rapidly developing subject areas, especially where there are important potential opportunities or risks. So far, this approach has resulted in a broad preliminary **horizon scanning** exercise.

- A priority for 2023 and 2024 should be to build on this joined-up approach to move from horizon scanning to a more **sophisticated and collaborative framework of methodologies and techniques** for DRCF's member regulators to:

    a) develop **rigorous and systematic evidence-based foresight** of possible and desirable futures;
    b) explore **shared policymaking and regulatory techniques** to future-proof regulation in the areas within the member regulators' remit**.**

Researchers at the Dawes Centre for Future Crime regularly employ **futures research methods** – that is, methods specifically designed to systematically identify possible and desirable futures[32] – to investigate the future crime risks of emerging technologies.[33] Such methods include **systematic reviews** of the existing literature which inform **sandpit events** intended to understand an issue and to map out possible solutions to them. **Systematic reviews** differ from typical (ad-hoc) literature reviews, as they rely on clear and predetermined search criteria that make them more exhaustive and less biased accounts of existing knowledge. **Sandpit events** are intensive and highly multidisciplinary interactive discussion forums designed to drive lateral thinking and innovative approaches to challenging issues. UKRI considers them one of the main examples of 'transformative research' that stimulates 'creativity and adventure'.[34] So far, the Centre has completed **11 sandpit events as well as other workshops**, and has evolved its approach over these iterations**.** For our sandpit events, we combine the approaches typically taken with a form of **Delphi study** to elicit knowledge, and seek consensus on priorities, from

[31] Objective 4 of DRCF's Terms of Reference: https://www.gov.uk/government/publications/drcf-terms-of-reference/terms-of-reference

[32] See, for instance, Fowles, J. (ed.) (1978). *The Handbook of Futures Research*. Westport-London: Greenwood Press; Gordon, T.J. (1992). 'The methods of futures research'. *The Annals of the American Academy*, vol. 552, 25-25

[33] https://www.ucl.ac.uk/future-crime/publications/2021/may/mapping-future-horizon-scanning-future-crime

[34] UKRI (2022) *Transformative research*. Available at: https://beta.ukri.org/councils/epsrc/guidance-for-applicants/types-of-funding-we-offer/transformative-research/

participants in a systematic way. Other approaches employed by the DCFC include **comparative and socio-legal** research, as well as more traditional quantitative and qualitative approaches.

Other than on research methods, a framework of methods and techniques to future-proof regulation could also rely on the **expertise, toolkits and guidance developed by national and supranational policy bodies**. These include, for instance, the Futures Toolkit and further guidance developed by the Government Office for Science's Futures, Foresight and Emerging Technologies team or the Fit for Future Platform (F4F) established by the EU Commission as part of the Regulatory fitness and performance programme (REFIT) to simplify EU laws and help them effectively address new challenges such as digitalisation.

The development of a joined-up framework of methods and techniques to future-proof regulation should be a collaborative endeavour involving all relevant stakeholders, including academia, industry, law enforcement, and government.

- **A joined-up approach to the unintended consequences and crime risks of regulation:** studies on regulation have long demonstrated that regulation can have unintended consequences, including criminal opportunities and motivations.[35] Recent research suggests that the **unintended and criminogenic effects of regulation** are especially caused by changes in legal and regulatory regimes.[36] Regulatory changes driven by emerging technologies – such as the Online Safety Bill – can be particularly insidious as such technologies evolve at a very fast pace and involve different areas of regulation. This can aggravate the problem, as the same research also suggests that unintended consequences and crime risks can be enabled not only by individual regulatory provisions and their wording but also by the **more complex interactions (and lack of coordination) between different areas of regulation**. Therefore, while targeted regulatory amendments can resolve the unintended effects of specific provisions, broader interventions applicable to any area of regulation and relying on the collaboration of different regulators are required. Such measures could include increased coherence between regulations, special training for regulators and policymakers, task forces or expert committees to advise on the design, implementation and evaluation of policy and regulation, as well as mechanisms to assess and mitigate the crime risks or other unintended consequences of proposed or enacted regulations.[37]

[35] See: Savona, E.U. (ed.) (2006). Double thematic issue 'Proofing EU Legislation against Crime.' *European Journal on Criminal Policy and Research*, 12(3–4): 177–397; Pasculli, L. (2017). 'Corruptio Legis: Law as a Cause of Systemic Corruption: Comparative Perspectives and Remedies Also for the Post-Brexit Commonwealth.' *Proceedings of 6th Annual International Conference on Law, Regulations and Public Policy (LRPP 2017), 5-6 June 2017, Singapore.* Singapore: GSTF, pp. 189-197. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216442

[36] Pasculli, L. & MacLennan, S. (forthcoming 2023) "The Producers" of Tax Abuse: The Corrupting Effects of Tax Law and Tax Reliefs in the U.K. Film Industry, *Law & Contemporary Problems*

[37] For an overview and other references see: Pasculli, L. (2021) 'The Responsibilization Paradox: The Legal Route from Deresponsibilization to Systemic Corruption in the Australian Financial Sector', 15 *Policing*, pp. 2114-2132. Available at: https://academic.oup.com/policing/article-abstract/15/4/2114/6424222

Regulatory coherence and effectiveness are amongst the primary objectives of the DRCF. The DRCF is particularly well-placed to promote dialogue and raise awareness on these issues amongst its members regulators, develop effective collaborative solutions and build the skills and capabilities required to implement them. We recommend that the 2023/24 workplan of DRCF includes initiatives for the understanding, detection, assessment and mitigation of the **risk of crime or any other unintended consequence of present and future regulation of digital technologies.**

- **Online anonymity:** There are growing concerns about how anonymity can easily act as a major enabler of online crime and misconduct by disinhibiting online behaviours and shielding offenders from enforcement. The UK government is considering including special measures against anonymous abuse on online platforms in the Online Safety Bill[38], which the House of Lords has recently asked Government to reintroduce to Parliament.[39] Online safety regulators overseas, such as the Australian e-Safety Commissioner, have also called for stronger and more transparent identity-related policies.[40] However, policymakers and lawmakers are very cautious about introducing more stringent online identity policies. Identification requirements might conflict with individual interests such as the right to define one's own self-sovereign identity (SSI), the protection of privacy and even the protection from possible victimisation. They might also conflict with industry interests in the broader commercialisation of online services and less burdensome obligations for providers of such services.

  A better dialogue and understanding of the competing interests surrounding online anonymity is crucial for all the DRCF's member regulators. With its collaborative approach the DRCF could play an important role in advancing the debate between regulators and relevant stakeholders on such issue to build the knowledge base and the consensus required to develop adequate regulatory solutions. These objectives can be addressed through a series of initiatives, including commissioned research, consultations, surveys, or stakeholder events. The inclusion of online of anonymity as an area of focus for the DRCF's workplan for 2023/24 would be therefore a great contribution to the effective regulation of digital technologies.

3. Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?

[38] DCMS (2022). *Press release: New plans to protect people from anonymous trolls online*. Available at: https://www.gov.uk/government/news/new-plans-to-protect-people-from-anonymous-trolls-online

[39] House of Lords (2022). *Fighting Fraud: Breaking the Chain*. Available at: https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf

[40] eSafety Commissioner (2022). *Anonymity and identity shielding online: Tech trends position statement*. Available at: https://www.esafety.gov.au/sites/default/files/2021-02/Anonymity%20and%20identity%20shielding%20online%20statement.pdf

- **Vulnerable users:** one of the priorities of the DRCF, as set out in the previous workplans, is the protection of children online. The DRCF could build and expand on the progress made and the experience developed in this area to focus also on the protection of **other groups of vulnerable users** of digital technologies. Such groups can include the elderly, adults with additional needs, adults with physical or mental difficulties, minority groups exposed to abuse, users lacking sufficient digital or financial literacy, young people in pupil referral units. The FCA rightly observes that in the context of online harms 'anyone can be vulnerable' – for instance, during elections prospective elected members who use social media as part of the campaign process are vulnerable to abuse, harassment and much more.[41]

  One of the priorities of DRCF for 2023/2024 could be to start a **mapping exercise** to identify groups of vulnerable users and understand their specific risk factors. Such mapping is necessary to develop coherent and coordinated regulatory approaches to assess and mitigate such risks. Vulnerability can depend on situations and characteristics that can be very different from one group to another. As a result, effective interventions should be targeted to the specific needs of each group.

  A good starting point would be the **elderly population**, which – also because of the Covid-19 pandemic – is a rapidly growing proportion of online users exposed to multiple risk factors. Such risks particularly concern financial crime and fraud which often involve financial services and products and the exploitation of personal information. Recent research conducted by our Centre[42] identified such risk factors and grouped them into three main themes: cybersecurity skills and behaviours (e.g., limited cybersecurity skills and awareness, receiving poor advice, vulnerability to certain types of scams); social and health-related issues (e.g., declining health and mobility, memory and cognitive deficits, social isolation, bereavement, wealth); social context (e.g., stereotypes and increased perceptions of vulnerability). The research also identified possible interventions.[43]

Summary of recommendations

1. The DRCF's workplan for 2023/24 should include a **prioritisation exercise** to identify the technologies which require urgent regulatory attention. The **prediction and prevention of crime** should be amongst the criteria for prioritisation and a specific focus should fall on **crime-enabling technologies**. Priority areas of technology include: the **metaverse** and related technologies, the '**Internet of Things' (IoT)** and **cryptocurrency**.
2. The 2023/24 workplan should focus on developing its joined-up approach on future technologies into a more sophisticated and collaborative framework of methodologies and techniques for DRCF's member regulators to develop **rigorous and systematic**

[41] FCA (2021) *Must Know: Online Harms*: https://www.local.gov.uk/publications/lga-online-harms

[42] Burton, A., Cooper, C., Dar, A., Mathews, L. and Tripathi, K. (2021). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. Experimental Gerontology 159 (2022) 111678: https://www.sciencedirect.com/science/article/abs/pii/S0531556521004605?dgcid=coauthor

[43] Tripathi, K., Cooper, C., and Burton, A. (2021). Policy Briefing: Older adults as victims of online financial crime: https://www.ucl.ac.uk/future-crime/sites/future_crime/files/ucl_policy_briefing_-_older_people_and_financial_crime_december21.pdf

evidence-based foresight of possible and desirable futures and explore **shared policymaking and regulatory techniques** to future-proof regulation in the areas within the member regulators' remit**.**

3. The 2023/24 workplan should include specific initiatives for the understanding, detection, assessment, and mitigation of the **risk of crime or any other unintended consequence of present and future regulation of digital technologies.**
4. The 2023/24 workplan should include amongst its area of focus the issue of **online anonymity** with a view to advancing the dialogue between regulators and relevant stakeholders, promoting a better understanding of the competing interests at stake, and building the knowledge base and the consensus required to develop adequate regulatory solutions.
5. The 2023/24 workplan should focus on the protection of **other groups of vulnerable users** of digital technologies, also through a **mapping exercise** of vulnerable groups and their specific risk factors. A starting point could be the **elderly population.**

8. Electronic Money Association

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments, open banking payments, and cryptoasset services. A list of current EMA members is provided at the end of this document. The EMA has been operating for over 20 years and has a wealth of experience regarding the regulatory framework for electronic money and payments.

We welcome the opportunity to comment on the DRCF workplan 2023 – 2024.

The EMA would welcome if the DRCF could consider including work to support the implementation of the UK's Smart Data regime under its 2023-24 workplan. We believe that once the underlying legislative framework[44] for the Smart Data regime progresses through Parliament there will be critical need for the DRCF to coordinate and align policy work and implementation projects as Smart Data schemes emerge in different sectors. For instance, DRCF's goals of promoting coherence and greater collaboration amongst regulators could help accelerate developments in Open Finance which the Smart Data regime may allow.

We recognise that the Joint Regulatory Oversight Committee (JROC)[45] is responsible for overseeing the development of the vision and strategic roadmap for Open Banking in the UK. However, Open Finance will reach beyond the current boundaries of open banking, and will likely require cooperation amongst a broader group of regulators to achieve successfully implementation. For these reasons, we believe that DRCF should consider including a workstream to support the Smart Data regime in 2023-24.

Thank you for taking our comments into consideration.

Yours faithfully

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

[44] Data Protection and Digital Information Bill - Parliamentary Bills - UK Parliament
[45] The future of open banking and the Joint Regulatory Oversight Committee | FCA

9. Eversheds Sutherland

INTRODUCTION

Thank you for issuing a call for input and views upon the recent DCRF policy paper (deadline 6 th January 2023). We have set out our combined responses from our respective financial services, competition, consumer and data privacy teams below for your consideration. We'd be happy to discuss any of the issues raised and our responses, if required.

RESPONSES

1. **Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.**

Putting in place an effective and compliant data sharing agreement between the members of the DRCF (as well as any appropriate data sharing terms with organisations sharing data and information with each member of the DRCF) will be essential to clarify and restrict the purpose and type of data that is shared (and in what form and if any de-sensitisation is necessary before sharing). In addition, a shared platform for holding information and any aggregated insights seems appropriate to avoid multiple copies of data being held by more than one regulator member. This platform will also enable the measurement and tracking of API-use and data ploaded and downloaded (and, in turn, can be used to measure the engagement of each DRCF member, when compared to its peers).

The data sharing arrangements and terms of engagement will be essential to mitigate risk and also ensure that the right form of data is shared so as to build insights which are realistic and measurable (and in line with key focus areas and the DRCF's core policy and factors to be taken into account). The central data platform will also reduce cybersecurity risk and assist in data nalysis and aggregation.

Also, the DRCF refers to mapping interactions between the regulators - for our clients and our experience, ensuring that the DRCF effectively communicates and provides transparency regarding that data sharing and/or collaboration in relation to enforcement action would be the most impactful, as well as ensuring that guidance links across agencies where relevant (and is consistent). This would echo John Edwards' (the Information Commissioner's) stated commitment to providing certainty to controllers as to what the law requires.

As part of this, the DRCF should also follow best practice in the development and use of any algorithm it uses to analyse data shared and develop and approve an appropriate data privacy impact or algorithm assessment for this purposes (as well as develop associated fair use and data analysis terms and policy to ensure its data sharing between DRCF members and its analysis is transparent).

We also note that the table sets out “Supporting improvements in algorithmic transparency” as a collaboration area - we’d be interested to see the DRCF look at issues of algorithmic ethics not just transparency.

From a technology perspective, the use of neural networks (e.g. potential lack of transparency and whether its use is appropriate and proportionate) and biometrics (e.g. use in fraud prevention as well as digital marketing and entertainment) should be given specific and due care and consideration.

2. In line with the ‘factors we consider when prioritising work’ (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan?

Suggested other areas of focus or factors to consider when prioritising work –

- Can we afford not to collaborate – in other words, is the digital economy so advanced now that a failure to collaborate would result in outdates or misinformed regulation?
- In addition, even though a DRCF member may not necessarily have the resources to collaborate, it may be able to help other regulators, even by sharing its results or insights with the other DRCF members via a designated data sharing platform.
- Can the DRCF ensure that organisations which fall within each other’s regulatory sphere are not required to duplicate or re-share information with one DRCF member which it has already shared with another?
- Can any regulatory onus or resourcing be passed onto the organisations which are regulated – can any efficiencies be achieved by organisations self-reporting or sharing data into the DRCF’s data sharing platform or cloud

3. Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?

Consumers generally, as well as vulnerable consumers (with clarity on what is meant by “vulnerable” – e.g. whether the intention is to identify specific minority groups, or to identify and apply certain risk factors to identify consumers who may be particularly susceptible to detriment, whether on a permanent, temporary or sporadic basis), and SMEs and mid-sized businesses. In relation to vulnerable consumers, the approach taken by the FCA under the Consumer Duty is a good model and it would be desirable for any additional rules relating to vulnerable consumers in relation to digital content (which much financial services advertising and interaction is and will increasingly be) to be at least congruent with the FCA approach (if not the same) to avoid financial services firms having to consider two different vulnerable consumer regimes when providing digital financial services.

As well as the overarching Consumer Duty, there are specific FCA regulations dealing with financial promotions which should be taken into account when considering the regulation of digital advertising. We note the good work of the Advertising Standards Agency (ASA) in relation to the promotion of financial services online and digitally, and urge the DCRF to work with the ASA in this regard. In relation to the regulation of data privacy and competition in respect of financial services firms, the FCA already has regulatory oversight, either jointly in respect of data (for which the FCA regulates the fair treatment of customers in relation to their data) or solely in respect of competition (where the CMA's functions were transferred to the FCA some years back). We wonder whether the FCA should be the appropriate primary regulator for the digital activities of FCA regulated firms too.

The 'building on engagement between Ofcom and FCA on online fraud and scams' – under Coherence – should also inherently include the ICO.

We also think there should (as far as is possible and in due course) be increased collaboration between related international regulators (e.g. in the context of UK and EU GDPR with supervisory authorities in the EU and the EDPB).

It would be good to see thought given to the digitally excluded/deprived as well. Just as HMT has legislated to ensure continued access to cash, consideration should be given to regulatory or legislative guarantees that certain services (e.g. payment for parking, applications for benefits, claiming and receipt of pension funds) will not become accessible only by digital means.

Should you wish to discuss any of the above responses or issues raised further, please contact:

Philip James,
Partner, Global Privacy and Cybersecurity Group
T: [redacted]
M: [redacted]
E: [redacted]

10.Gambling Commission

We are pleased to respond to the DRCF's call for input to its workplan for 2023 to 2024. In developing this input, we have considered the three questions set out in your open consultation:

1. **Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.**

We broadly agree with the direction of travel set out in DRCF's existing workplan for 2022 to 2023 and support DRCF continuing to build on these areas of focus. There are some areas we would support being prioritised where we feel the greatest value can be added for member organisations and for the wider public interest.

DRCF is already exploring ways to **promote competition and privacy in online advertising.** We would encourage a focus in 2023 to 2024 on accelerating progress to provide consumers greater control over the online marketing and advertising content they receive. This is relevant to the remits of Ofcom and the ICO – and would deliver opportunities for consumer protection and fairer operation of markets across several regulated sectors, including gambling. There is also an important opportunity for search engines and internet service providers to play in **blocking access to illegal content and activity**. Opportunities to build partnerships to ensure this opportunity is taken would deliver benefits to all members of DRCF. This is an area of work we would be particularly interested in collaborating on.

We support the synchronisation of effort to **better protect children online** and would welcome a focus on improved online age assurance. Findings from our Young People & Gambling Survey 2022 show that 44% of 11–16-year-olds had seen gambling ads on social media and 36% had seen them on live streaming or video sharing platforms. 13% said they followed or watched gambling companies on social media. These findings likely correlate with Ofcom research showing that a third of children aged between 8 and 17 with a social media profile have an adult user age after signing up with a false date of birth. Linked to this, we are also interested in developing understanding of how better age protections can be delivered through **facial recognition technology**.

The Gambling Commission also supports the continuation and expansion of DRCF's existing work to **map interactions between different regulatory regimes**. This provides opportunities to identify risks to consumers and highlight where innovations in technology have created products and services which do not fit easily within established regulatory frameworks. For instance, there are examples – relevant to the FCA and Ofcom – of digital assets that do not fit wholly or neatly as gambling products under the Gambling Act 2005 and sit in largely unregulated spaces. These are generally sports-based products and include synthetic shares, non-fungible tokens (NFTs) and/or cryptocurrency, some of which have been reportedly advertising pitch-side at sports arenas.

DRCF's strategic priority around **capability** is an area which presents great opportunities to add value to all members, as well as other regulators, such as us, who are exploring how best to utilise data to deliver effective and proportionate regulation. Better use of data is an essential for modern regulators – we would support expansion of activity to establish and share best practice. As well as forums to share learning and collaborate on projects to build capacity in relation to data and application of RegTech. There is potential to draw on the collective expertise of relatively new and established regulatory groups such as the Institute of Regulation (IOR) and UK Regulatory Network (UKRN), which have special interest groups focused on cross-cutting issues (e.g. data sharing, enforcement, risk management).

We also support the continuation of work around best practice in the **transparency of algorithms**. These are relevant to the work of all member regulators, we well as providing benefits for learning and information sharing across a range of related regulated markets.

Developing understanding of **how consumers interact with businesses' digital platforms** and whether those platforms are – by design – resulting in consumer decision making that could be against their interests, is an area that would span more than one regulator. There may be scope to coordinate efforts to build understanding of business practices and associated risks. In gambling, we see this in features such as anchoring/ranges for limiting financial deposits, countdown clocks for next game/next race starting and adding friction to accessing gambling management tools. Other businesses operate in similar ways using approaches such as scarcity messaging to drive consumer decisions to purchase. We are interested in the balance regulation needs to achieve to provide a proportionate response to this risk.

2. **In line with the 'factors we consider when prioritising work' (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan?**

We have not identified any entirely new topics of work.

3. **Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?**

Given asymmetry of information for consumers when engaging in many digital and online markets and activities, there are many situations where consumers may be vulnerable. Focusing on vulnerable consumers and children are therefore essential. This needs to be balanced against wider consideration of the needs of all consumers. We encourage an approach which balances the needs of all of these groups.

11. Gener8

Gener8 proposes that, as part of its 2023-24 workplan, the DRCF conducts a feasibility study into potential interventions to provide people with frictionless access to their own online data.

About Gener8 The open secret within the online advertising industry is that it is built on exploiting people's data. Gener8 changes that. We build tools that empower people to control and be rewarded from their data by giving them a simple choice: Rewards Mode or Privacy Mode.

With rewards mode activated, users of our desktop browser and our newly launched (in beta) mobile app give us their explicit consent to process and monetise their data in anonymised form on their behalf. In return, our users earn points, which can be redeemed for rewards such as free products, discounts, and gift cards.

While our offer is simple, our impact could be profound. Gener8's business model can simultaneously topple two of the most significant barriers to effective competition in digital markets:

- **Unequal data access**: large online platforms protect their market power through an unassailable and self-reinforcing data advantage. Though they will never voluntarily share this data with their competitors, they are rightly required to hand it over to their users to whom it relates. By accessing, anonymising, aggregating, and monetising this data on our users' behalf, Gener8 can help to level the playing field with respect to data access.

- **Zero price floor**: new entrants in digital markets are prevented from competing on price, because the dominant online platform services are typically provided for 'free'. By acting as an agent on behalf of consumers, Gener8 empowers people to be rewarded from their data, essentially introducing a negative price for browsing the web or shopping online.

Gener8's mission is pro-privacy and pro-competition in equal measure - our growth is evidence that there are strong synergies between these important overlapping policy objectives. Similarly, our success will be a strong indicator of regulatory coherence in the digital space, and so we greatly value the platform for collaboration between UK regulators provided by the DRCF.

Giving people frictionless access to their data

Academic research often refers to the so-called privacy paradox - the fact that people often express strong feelings about online privacy and data protection issues, but then typically don't follow up these sentiments with action.

The rights to personal data portability and data erasure are prime examples. Data protection law gives everyone the right to request access to the data that companies hold on them and request that it be deleted, but in practice few people take up these options.

But there is no paradox here. The processes for submitting requests are generally clunky, slow, and lead to fatigue, to which disengagement is a rational response.

The only way that people will engage effectively and consistently is if the 'friction by design' is reduced to an absolute minimum. The initial effort level to take control must be kept to a minimum number of steps, and people should not be forced to needlessly keep repeating the same actions over and again. While Gener8 is able to build tools to overcome the technical challenges of data control, such as the need to transfer, store, and interrogate large volumes of data, we need regulators to remove the friction put in place by design by the digital gatekeepers.

Take Amazon for example. After making and then verifying a download request, Amazon states that it could take up to one month to provide all of your information. There is no option to automate this process for future downloads.

People with a Google account are able to request to download their data via Google Takeout, after completing an online form. This can be a one off request, or set to happen automatically every two months, but a more up-to-date picture of Google's tracking would require the user to keep returning to the page and completing the form. While Google's process is more streamlined than many, it can take hours or even days, rather than seconds.

While likely to be compliant with existing law, existing approaches to data portability rights are degrading users' experiences and holding back disruptive and transformative innovation. For companies of the scale and technological capability of Amazon and Google, we should have the right to know what they are collecting about us as it is happening. If this level of transparency is too costly, then they ought to stop collecting the data.

A pro-privacy, pro-competition intervention is needed to loosen the digital gatekeepers' grip on their users' personal data, with options available including requirements for open APIs based on common standards. The question at hand is not whether the ICO and the CMA are aligned on this issue, but with which regulatory tool should the change be implemented.

Proposal

Gener8 believes that the DRCF is uniquely positioned to explore these much needed interventions in more depth.

We propose that as part of its 2023-24 workplan, the DRCF undertake a feasibility study into providing people with more frictionless access to their online data, which could seek to answer the following questions:

- What are the key barriers to people accessing and controlling their own data?
- What are the potential benefits from enabling people - and companies operating on their behalf - to take full control of their own data?
- What actions - regulatory or otherwise - would be needed to reduce friction and put people in control?
- Which regulatory tool (existing or incoming) would be most appropriate to deliver these changes, given the cross-regulator nature of the issues, and to which companies should they apply?

This proposed feasibility study is consistent with the DRCF's prioritisation factors:

- **It fits with the goals of the DRCF** to promote collaboration and coherence, taking a proactive and joined-up approach to potential future policy making.
- **The DRCF can add substantial value in this space** - we are not aware that this is already being explored independently by regulators in the UK, or otherwise within other international jurisdictions. This is an opportunity for the DRCF - and the UK - to lead the way globally.
- Now is **the right time to consider this issue, given the broader legislative and economic landscape**:
    - The incoming DMU regime could be one option for implementing the necessary changes, while there could also be interactions with the incoming Data Protection and Digital Information Bill.
    - Given the financial challenges facing so many UK households, enabling people to get a fair deal online and share in the value of their data can no longer be viewed as a niche technical policy challenge for the future.
- It would appear that **members of the DRCF are ideally placed to consider these issues collectively**. Given the potential interactions with incoming legislation, it may be necessary to engage with DCMS when considering the specifics of incoming regulatory tools.
- This is **an area where the DRCF could have substantial meaningful impact**. It is an opportunity for regulatory action to be driven proactively by the DRCF from the ground up, with potential to create a monumental shift of power from digital gatekeepers to people.

The DRCF is uniquely equipped and positioned to answer the above questions and establish the way forward for unlocking frictionless data control, which is the key to leveling the digital playing field and creating a thriving online ecosystem that works for everyone.

We look forward to engaging with you on this important topic.

12. Institute for Future Work

Institute for the Future of Work response to DRCF Call for Input 2023

1. Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.

Workplace technologies ought to be taken into consideration. We elaborate further on the need for this in the response to the next questions below. To some extent, the workplace falls within the remit of the ICO and the CMA, although other regulators should be included in the DRCF to ensure adequate consideration of workplace-specific harms.

The Health and Safety Executive, new Single Enforcement Body for Employment and Equality and Human Rights Commission should be included in the DRCF, or alternatively consulted and work as closely as possible with the DRCF, to ensure impacts on work and people are properly understood and taken into account, as well as meaningful accountability and redress for any harms. Work currently being undertaken by the ICO on publishing guidance surrounding the use of AI at work provides a solid base upon which the DRCF can further develop the regulatory conversation.

2. In line with the 'factors we consider when prioritising work' (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan?

AND 3. Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?

There is not enough discussion of and protection for workers in the remit of the algorithmic processing workstream of the DRCF, or indeed, of the regulatory debate surrounding AI in the UK more broadly, which largely focuses on harms to consumers. Workers represent a stakeholder group which is both vulnerable, due to information asymmetries and inherent power imbalances between employer and employee in the workplace, and particularly deserving of protection, due to the significant impacts algorithmic processing has on workers' lives, livelihoods and wellbeing.

Existing regulations for the protection of workers from algorithmic harms are largely rooted in a patchwork of disjointed legislation, primarily data protection rights, human rights as enforced against public bodies and equality law. Methods or templates to structure consideration or forecasting of harms in advance of system deployment, before impacts arise, are few and far in between and are not mandated in legislation.

With this in mind, work as a cross cutting area of concern and environment of AI impacts ought to be prioritised by the DRCF. In terms of the factors the DRCF considers while prioritising areas of focus, we believe that the goal of regulatory *coherence* in particular would be addressed by including work. The regulatory lacuna highlighted above also serves as justification to explore this area based on the current legislative landscape, which is certainly in a nascent state.

Finally, this is certainly an area where the DRCF can have meaningful impact in convening regulators, encouraging standardisation and closing regulatory gaps by considering work as a *cross cutting* concern: a socioeconomic space, and not a sector, onto which individual futures are projected and determined. There is great potential for the DRCF to provide clear and singular guidance for employers and other accountable agents in the AI lifecycle, signed off by all the regulators rather than different pieces of guidance from different regulators.

To take assurance and information disclosure as an example, the DRCF should, where possible, provide single pieces of guidance on the procedural requirements for audits; for example, how they should be conducted across the supply chain, how stakeholders should be consulted and notified, the processes for triggering external or internal audits, how audits should be reported on to the regulator, workers, the public or otherwise, and so on.

In terms of disclosure employers should disclose key information about the functioning of AI systems, such as the nature, purpose and scope of the system, the outputs produced by the systems (eg. recommendations, employee scores), and how to access further information, contest automated decisions or provide feedback.

A more comprehensive model of disclosure, such as for more advanced systems with a significant impact on work and working lives, would include more granular disclosures, for instance the inputs, criteria, variables, correlations and parameters used by the systems in producing those outputs, the logic used by the systems to produce their outputs, including but not limited to weightings of different inputs and parameters, if and how the system is operated by third parties (eg. algorithmic hiring providers separate from the employer), and relationships of accountability in the organisation and beyond for AI harms.

We are planning to pilot methods of assurance and information disclosure in the workplace with corporate and academic partners. We would welcome the chance to share our insights in the future.

13. ITN

ITN welcomes the opportunity to take part in this consultation and contribute to this important piece of work. ITN approaches this call for evidence from the perspective that the news services we produce (ITV News, C4 News and C5 News) provide key social and democratic benefits.

1. **Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.**

ITN would urge the DRCF to consider the policy interactions that will affect online competition in the news industry and discovery of news content online in its workplan for the coming year.

ITN believes that effectively promoting competition in journalism online and ensuring news prominence online are areas that both the CMA and Ofcom should be concerned with.

Journalism and news deserve special consideration because of the important role they play in healthy democracies and therefore any regulation affecting its distribution and creation in the online sphere will set an important precedent for the future.

Legislators and regulators have a unique opportunity to ensure that news content is protected and promoted by ensuring that legislation takes a holistic approach to journalistic content online.

Therefore, ITN is urging regulators to proactively consider how news will be affected by any new regulation governing the dissemination of information online.

As already noted by the DRCF[46], algorithms have the potential to have wide-ranging benefits and harms on society.

ITN's commercial news activity, grounded in a public service ethos, means that ITN is procompetition and any regulation relating to algorithms and opening up competition, but also tackling mis/disinformation are highly pertinent to the organisation.

As the Digital Markets, Competition and Consumer Bill is concerned with opening up key markets, ITN is keen to stress the vital role of broadcast journalism's role within the UK's media eco-system.

ITN has invested heavily in producing bespoke, high-quality, trusted journalism for digital platforms. This investment is despite commercial digital revenues remaining small, at present.

[46] The benefits and harms of algorithms: a shared perspective from the four digital regulators 2022 (DRCF) - GOV.UK (www.gov.uk)

Furthermore, ITN's online journalism is produced and complied to the same editorial standards as its TV bulletins, despite there being no regulatory requirement to do so. This rigorous compliance process ensures that ITN's journalism can be relied upon by all audiences – whether watching TV or going online - to be trusted and impartial. It includes scrutinising information through both editorial and legal lenses, using multiple sources, reporting with transparency, and offering alternative views.

It is for that reason, that ITN believes, that any regulatory regime affecting the news industry, whether that is through the Digital Markets Unit or the Media Bill, should prioritise: promoting competition and giving consumers easy access to information that is trustworthy.

This can be achieved in two ways:

1. The creation of a bargaining code to ensure that high-quality content can continue to be invested in sustainably. By creating a bargaining code to rebalance the relationship between publishers and tech platforms this would allow more parties interested in creating regulated journalistic content to come to market.

2. A kite-marking system that allows consumers to better understand when content is produced by a reputable outlet to a higher standard than other content creators.

These two areas together are key to protecting and enhancing the UK's journalistic eco-system in the years to come as well as preventing the wider societal harms of dis and misinformation.

2. **In line with the 'factors we consider when prioritising work' (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan? See above.**

See above.

3. **Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?**

Ofcom's latest news consumption report (July 2022) found that social media is overtaking tradition channels for teenagers as the main source news.

With large amounts of misinformation available online it is crucial that these measures are enacted and work harmoniously with each other to promote trustworthy content to this key group.

About ITN

Independent Television News (ITN) holds a unique place in the UK media landscape providing news services to up to 9m people daily by producing ITV News, Channel 4 News and 5 News as well as hundreds of hours of long-form factual programming for broadcasters and platforms. It has 66 years' experience in public service broadcasting and is renowned for being able to deliver journalism of the highest standard across all output.

ITN's relationship with the UK's broadcasters not only exists through the news contracts for ITV News, Channel 4 News and 5 News, but through the production arm of ITN which frequently delivers successful long-form programming to broadcasters. ITN Productions established a Leeds operation in 2020, and the team makes topical and current affairs programmes for the BBC, ITV, Channel 4 and Channel 5, as well as other UK broadcasters, with most productions involving filming around the UK. ITN Productions hold the live programming contracts for The Andrew Neil Show on Channel 4 and the weekday current affairs discussion programmes on Channel 5 Jeremy Vine and Jeremy Vine Extra. ITN also produces ITV's London news programmes, broadcasting seven days a week with around 30 staff covering news in London and the east of England.

ITN is home to a unique and delicate ecosystem which provides economies of scale for all three PSB news services (Channel 4 News, ITV News and 5 News). Each of ITN's newsrooms are staffed by trained, expert journalists, producers, reporters, and behind-the-scenes technical staff making daily broadcast bulletins, social media content, podcasts and digital video content right across the commercial PSBs. Each newsroom benefits from cost-effective sharing of resources to ensure efficient value for money and maximum investment in journalism – wholly founded on decades of prowess built from the ethos of public-service broadcasting, compliance with Ofcom regulation and high internal editorial standards.

Over its history, ITN has played an important role in the news production ecology of the UK – not only as a counter to the BBC and other commercial media outlets, but as a driver of innovation in the industry, training up talent, investing across the UK, and as the biggest independent producer of high-quality, impartial news and current affairs.

In May, ITN launched ITN Business, a new division that combines its work in business-to-business (B2B) communications, from corporate films to hybrid events and its broadcast standard news-style programming, Industry News. Recent projects have included hybrid events for Tesco, the CBI and Google, microsites, and content series for International Women's Day and COP26 and programming such as How Vaccines Are Changing the World in partnership with the New Scientist, fronted by Louise Minchin.

In recognition of ITN's contribution to broadcast journalism in the UK, at the Royal Television Society (RTS) Television Journalism Awards this year, our teams took home seven awards: six for ITV News alone, which won Daily News Programme of the Year for ITV News at Ten, Journalist of the Year for Robert Moore, Specialist Journalist of the Year for Daniel Hewitt; and Robert Moore's report 'Storming of the Capitol' won – best International News Coverage, Scoop of the Year and Breaking News, as well a prestigious International Emmy Award and a BAFTA for best news programme. While Channel 4 News' Krishnan Guru-Murthy won Presenter of the Year at RTS.

Contacts
Lisa Campbell, Director of corporate communications [redacted]
Balihar Khalsa, Head of press and public affairs [redacted]
Independent Television News Limited 200 Gray's Inn Road | London | WC1X 8XZ Registered in England & Wales Registered Number: 548648 +44 (0)20 7833 3000 | www.itn.co.uk

14. Match Group

1. **Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.**

Match Group operates a portfolio of online dating brands which provide online dating services across the globe. We are grateful for the opportunity to respond to this consultation, outlining our experience in working with the individual bodies of the Digital Cooperation Regulation Forum (DRCF) and our views on your existing workplan and future priorities.

We understand the serious responsibility that comes with operating online dating services, and Match Group believes that safety of our users and the broader online community must be a priority. We believe any misconduct on our platforms is one incident too many. The policies that Match Group currently have in place provide a solid foundation on which to tackle online harms within Match Group and across its digital ecosystems. However, we also recognize that addressing safety concerns is a dynamic process and we adopt industry leading protocols and services to help protect consumers from online fraud and scams.

Match Group brands invest meaningful resources, both in terms of capital and human resources, with the aim of providing a safe user experience. The focus on safety begins at registration and continues throughout our members' user journey on our platforms. We have spent more than $100 million on product, technology and moderation efforts related to trust and safety to prevent, monitor and remove inappropriate, illegal, or harmful content.

Match Group is pleased to have worked closely with many member organisations of the DRCF to combat the most pressing cyber security and online safety challenges facing the online dating sector and we are pleased that the creation of the DRCF will help to maintain a commitment to upholding the high regulatory standards that have been established thus far.

We have been supportive of the DRCF's workplan for 2022-23, in particular the collaborative and coherent approach which the DRCF's existence promotes. We are extremely supportive of efforts to protect children online, as well as long needed governmental action to promote greater competition throughout the digital economy, and we hope that these objectives will be carried over to the next year's workplan with urgency and enthusiasm. We hope that the DRCF continue to investigate the role of gatekeeper entities in the digital economy, in particular app stores, and the role these gatekeepers play in both online safety and digital competition policy. We will provide further detail on these points below.

Promoting responsible online safety legislation and regulatory action is a priority for Match Group, and we are pleased that both legislative and regulatory bodies are also treating it as such. Match Group has worked closely with Ofcom and have met with the authority five times in the past year alone to discuss how government and the private sector can and must work together to protect the public from harmful and offensive online material. Match Group applauds the prioritization of passing the Online Safety Bill. This important bill if passed, will direct Ofcom to draft codes of practice for tech companies and govern how they tackle online harm. Match Group hopes passage of this bill will encourage greater collaboration between the government and companies offering online services. Match is hopeful that the new safety regime envisioned in the Online Safety Bill will result in new safety innovations designed in partnership with UK regulators. One example of our existing work on online safety is the automated content classification (ACC) system, which Match Group uses to remove harmful content from its platforms, and which Ofcom conducted a report upon last year to examine its potential in closer detail.

Match Group is pleased to see that the Digital Markets Unit (DMU) legislation will be moving in Parliament, and we urge the Parliament to pass this needed pro-competition measure that will benefit both UK citizens and developers of online applications "apps". The CMA has a storied history of advocating on behalf of British consumers and businesses and the Digital Markets, Competition and Consumer Bill will empower the CMA's Digital Markets Unit with the tools needed to investigate and meaningfully address competition concerns in the digital marketplace. Match Group will continue to support the important work of the CMA and the DMU as they conduct vital work to ensure that digital markets work for the benefit of consumers.

In your previous workplan for 2022-23, DRCF noted the desire to clearly articulate "the relationship between competition and online safety policy". We believe this is the right approach for the DRCF to take and applaud the work of the Competition and Markets Authority (CMA) and Ofcom in addressing each of these issues individually. We welcome the establishment of the DRCF as a means of identifying and addressing in a holistic manner the links between both. We discuss in further detail below how the key players at the distribution layer of the digital ecosystem, Apple and Google, are impeding progress for both of these objectives and we therefore welcome the CMA's important report calling out the significant existing harms in this sector and demonstrating a clear case for regulating the monopoly control that Apple exercises on the iOS platform and Google does on the Android platform. In our view, there should be no need for further in-depth analysis to decide if Google and Apple justify a Strategic Market Status ("SMS") designation in the activities covered by that report. We look forward to the CMA concluding their necessary and timely investigations into these topics.

Match Group understands the importance of balancing online safety measures with data privacy concerns and is committed to working with the DRCF and the Information Commissioner's Office (ICO) within it to uphold users' data privacy rights. This is why we are committed to finding solutions to crucial online safety concerns including but not limited to important issues such preventing underage individuals from accessing our platforms – also referred to as 'age-gating' -- without making unnecessary intrusions into users' privacy. Later in our submission, we explain the need for a holistic app ecosystem approach to more effectively use existing available tools to keep underage users off of Match Group brands platforms as well as other online services where the UK government believes there are concerns. Match Group welcomes the opportunity to engage with the ICO and DRCF and discuss such initiatives in greater detail.

Lastly, Match Group appreciates the work of the Financial Conduct Authority (FCA) in dealing with online fraud, which is a major issue in the United Kingdom and affects many users. To tackle online fraud specifically, in the UK context, Match Group has established a partnership with the City of London Police and the National Fraud Intelligence Bureau (NFIB). This relationship comprises a voluntary agreement through which Match Group and UK law enforcement collaborate on reducing online crime and sharing high level data around scammer behaviour. To further augment Match Group's commitment to safety, Match Group launched in 20xx the first-ever law enforcement portal for the dating industry to support law enforcement investigating crimes involving our users on a global basis. Match Group will continue to work with the FCA, the City of London Police and other relevant authorities on the issue of online fraud where it can and we have been proud to partner with the City of London Police, Australia, the Netherlands, U.S. federal law enforcement and others around the globe to combat online fraud and protect users

2. **In line with the 'factors we consider when prioritising work' (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan?**

At Match Group, we appreciate the unique responsibility we have as a leading provider of consumer online dating services and we are very proud of our work to improve online safety not just for users of our services, but for online community at large. We believe it is important that all companies within the digital ecosystem adopt a similar approach and take their responsibility seriously. While we support the previous workplan's focus on promoting competition in online advertising, we believe the enhancement of digital competition can and should go further. The DRCF has a responsibility to investigate multiple spheres of market dominance and ensure that these markets are free, fair and operating for the benefit of their users.

This is certainly true for entities such as app stores who can and must do more to help age gate when underage users try to download apps intended for older audiences. The overwhelming majority of phone users access content through applications which are downloaded through two app stores – the Apple App Store or the Google Play Store – yet there are currently no enforcement measures to ensure that these gateways are regulated. This presents a glaring flaw in the implementation of the online safety regime, the data privacy regime and other related goals. So long as app stores, a vital element of the entire digital economy, are left unaddressed by these regulatory frameworks, such frameworks will be missing a foundational piece.

Match Group wholeheartedly supports the UK's Online Safety Bill and welcomes the opportunity to engage further with Ofcom and the DRCF in ensuring that the Bill is as cohesive, holistic and effective as possible. To achieve this, we believe that more should be done, both within the Bill and by DRCF, to examine the role which app stores play in promoting and enforcing online safety practices at the 'distribution layer' of the digital economy.

The only way to improve online safety for the whole of the online community is to address the issue holistically, importantly making sure that both app developers and the companies that distribute apps (app stores) do more to ensure that children are appropriately kept away from adult applications and content. Similarly, the only way to ensure a dynamic, free and fair digital market is to assess the overarching structure of the digital economy, such as where content is overwhelmingly distributed and who owns these gateways or makes the rules.

As Match Group have outlined in previous consultation responses to both regulators and government, we believe that to prevent minors from accessing adult-only apps (and thereby reducing the risk of many online harms experienced by children through adult content), the most efficient measure would be to check users' ages during the distribution step, which means directly in the app store, and block underage users from 18+ services.

The Apple App Store advertises our adult-only apps as 17+, while Google's Play Store advertises it as PEGI 18. Match Group has repeatedly made clear that our apps are by design only to be used by adults and we have asked that both Apple and Google do not allow minors to be able to download our apps.

Developing a reliable age-verification regime applied at the "distribution layer" of the internet supply chain would significantly advance the United Kingdom's objective of creating a safer online experience and would set a precedent that other governments of the world could readily follow.

Approximately 99% of all users of Match Group brands access our services via an app, and they access the app by downloading it from either the Apple (iOS) App Store or the Google (Android) Play Store. The role of app stores as 'gatekeepers', with a strong understanding of who the customer is (developers are introduced to users 'blind' whereas app stores have a large amount of data on their account holders), means that both app stores (the distribution layer) and the app developer share responsibility to make the online experience safer. Currently, the emphasis is placed heavily onto the app developer, despite app stores holding greater information on a customer, information they choose not to share. We are a developer which takes our responsibilities for our users seriously, yet we have received no assistance from app stores despite years of insistence for greater cooperation and transparency.

The online safety of users, as well as their choice of what services or digital architectures to use, are heavily impacted by gatekeepers such as Apple and Google. This makes the link between digital competition and online safety concerns very clear. DCMS is already examining the relationship between app stores and application providers, as indicated in their recent announcement on a voluntary code of practice for app store providers and app developers. This is a welcome development which Match Group fully supports. We believe that DRCF can and should conduct a similar investigation.

The CMA recently announced that they will be examining the role of Apple and Google relating to mobile browsers as part of their ongoing investigation into mobile ecosystems. We appreciate this approach as it will help to address longstanding imbalances within the digital economy which not only affect UK users but also smaller digital businesses who are reliant on such digital infrastructure. We believe this investigation should be expanded to not just apply to browsers, but also to app stores since they serve as an important means of distributing and disseminating online services. As we have detailed above, app stores are a crucial component in the digital supply chain and as such we strongly urge the appropriate regulatory agencies to act and establish an appropriate regulatory framework that addresses both online safety issues and to creates a more competitive marketplace benefitting both app developers and consumers.

Although the issues of app stores and the consequences of their market dominance for online safety and digital competition have not yet been explicitly addressed by the DRCF, we hope that the DRCF will use its advantages as a collaborative organisation to articulate and investigate the links between online safety and digital competition. Doing so will benefit consumers, businesses and the most vulnerable in society in enhancing online safety, increasing data privacy and ensuring a free and fair digital marketplace which works for the benefit of users.

3. **Are there any particular stakeholder groups (e.g., end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?**

Match Group supports the efforts of Ofcom and the Government to add additional safeguards to the online marketplace to protect children and other at-risk populations. Match shares the government's view that this is of the utmost importance. We continue to believe that the safety of underage users of digital services must not be sacrificed in the support for the cause of privacy. While efforts to establish a balance between safety and privacy, we must prioritize the safety of children first and Match supports the efforts of the DRCF and other agencies to improve online safety measures for the most online vulnerable populations.

We therefore believe that the DRCF should continue to focus on children as the most vulnerable users who are susceptible to online harms.

15. Nash Squared

About Nash Squared:

Nash Squared is the leading global provider of technology and talent solutions, with over 3,000 employees in 41 locations across the UK, USA, Europe and the Asia-Pacific. We help organisations across the world to recruit and retain highly skilled technology talent, including Meta and Alphabet, as well as build and transform their IT capability through our nearshore and offshore centres. Our mission for Nash Squared is to tackle the technology skills deficit within the United Kingdom by empowering employees to long-lasting careers. We support a huge range of service capabilities, from software development and technology solutions, to talent and workforce management.

Question 1: Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.

In 2022, Nash Squared published its 24th Digital Leadership report, the world's largest and longest-running survey of senior technology decision-makers. The data, gathered from almost 2,000 people from 87 countries worldwide in this year's report, found the following policy interactions to be crucial to strengthening the future of the UK's Digital Regulation sector.

a) The UK needs cybersecurity skills now more than ever but neither the people or the pipeline is equipped to meet the needs of the industry. Almost half of the largest organisations (total IT budget >$250m) in the UK are reporting that the cloud is creating security risks, with 52% of large organisations reporting major cyber attacks in the last two years. Furthermore, half of digital leaders in the UK fear an attack from foreign powers, a stark increase from 12% in 2018.
b) UK's cyber security recruitment pool has a shortfall of 10,000 people per year, as reported by a 2021 by DCMS. As a consequence, only a third of digital leaders in the UK feel confident that they have reasonable risks covered to tackle a cyber threat. Furthermore, 68% of digital leaders in the UK state that a skills shortage prevents them from keeping up with the pace of change.
c) Current UK Government policy isn't meeting the tech skills demand, a sentiment felt by 78% of digital leaders in the UK. This is a stark comparison to the 41% of digital leaders in Asia. We further found that the top 3 skills being sought after include, data analysts, cybersecurity specialists and technical architects. It seems clear that although Government recognises that access to technology talent is key to its competitiveness, the industry feels that there is a discord between the creation of that vision and realising it on the ground.
d) Diversity remains a core issue in the tech sector. With an increase in hybrid working, and an average of 2-3 days working in the office, we are starting to see a positive impact on the number of women in the technology sector, and female leaders in the UK tech

sector have increased from 12% in 2021 to 15% in 2022. Furthermore, 27% of new hires in the last two years have been women, and 25% of digital leaders said that remote working has enabled them to start recruiting more from overseas. However there remains a long way to go. Ensuring recruitment and retention techniques are as inclusive and un-bias as possible are therefore advised in ensuring that this trend continues to positively increase. Furthermore, each regulator should actively promote and allow for flexible working arrangements, such as hybrid or remote working, or flexi-time or job-share option. Such policies will help those with caring responsibilities feel confident in entering or progressing in the sector.

Recommendations:

Area 1: Collaboration

- **Nash Squared recommends that to enable innovation in the industries that DRCF operate in**, it should continue to consider and invest in emerging technology industries, such as Quantum Computing and The Cloud. DRCF could also consider creating a dedicated crossorganisation innovation team to specifically drive innovation at the heart of the DRCF. It could facilitate innovative driven collaborative initiatives such as Hackathons.
- **Nash Squared recommends continued investment in emerging tech, such as artificial intelligence (AI), automation and big data**. Our report found that two-thirds of digital leaders think that big data and analytics will be in the top 2 technologies to deliver competitive advantage in the next year, and that only a fifth feel that they are effective at using data insights to generate more revenue.
- **Nash Squared recommends that the DRCF** engage with Government appointed industry experts – such as recently announced by the Treasury:
  - **Matt Clifford**: Chair of the new **Advanced Research and Invention Agency (ARIA)**, to advise on new digital technology
  - **Priya Lakhani OBE**: Member of the **AI Council**, to advise on new digital technology
  - **Sir John Bell**: Member of **Genomics England's** board of directors, to advise on the life sciences sector
  - **Camilla Fleetcroft**: Eclevar UK's Vice-President of **Clinical and Regulatory Affairs**, to advise on the life sciences sector
  - **Jane Toogood**: Chief Executive of Catalyst Technologies at **Johnson Matthey**, to advise on green industries including hydrogen and battery development.

Area 2: Capability

- **Nash Squared recommends that to improve knowledge sharing through expert networks**, the DRCF should continue to engage with industry groups, such as The UK

Cyber Security Council, or CIONET, the largest private network of CIOs internationally, with over 10,000 technology executives.

- **Nash Squared recommends that to build on synergies and bridge gaps in horizon scanning**, the regulators should consider investment in bilateral horizon scanning projects which look at the impact of lack of diversity at the core of recruitment, and how this impacts the innovation in the sector. This includes the lack of diverse teams including ethnic minorities, of which 19% of teams in the technology industry have no representation. The average proportion of ethnic minorities in a team globally further only sits at 21%.
- **Nash Squared recommends that in order to recruit and retain specialist talent across all 4 regulators**, that the DRCF utilise the expertise of recruitment specialists, such as ourselves, who have equity, diversity and inclusion at the centre of its expertise. In order to see the change that the industry needs, it is important the DCRF set a best practice and work primarily with organisations that reflect the values we, as an industry, wish to see. This also starts with good representation within organisations, as poor representation in the workplace can lead to increased feelings of isolation and lack of confidence.
- **Nash Squared recommends that in order to achieve an equitable and diverse workforce**, the DRCF highlights job flexibility at the centre of its roles, offering roles that are highly flexible in terms of location and time commitments (full-time, part-time or on job share), in order to take away barriers to employment such as location or caring responsibilities.

Question 3: Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?

Whilst the technology sector has come a long way in increasing its equity, diversity and inclusion, there is still much progress to be made in ensuring that the sector best reflects the communities in which it operates. Much of this work can be undertaken in the strategic planning stage, and through engagement with previously under-represented stakeholder groups. Doing so can provide a significant opportunity for the DRCF to help shape the sector for a more inclusive, equitable and diverse future.

The first group which should be considered are ethnic minorities. In the digital sector, 19% of teams in the industry have no representation of ethnic minorities, and the average proportion of ethnic minorities in a team globally sits at only 21%. There are many facets to consider in the inclusion of all under-represented groups, across both new hires at graduate and apprentice level to experienced hires later in their careers. Mentoring and networks can play a significant part in supporting those already in the industry, providing a space of structured support for individuals going through similar experiences. Furthermore, allyship, and representation of allyship throughout the structures of DRCF, further supports the messaging that each of the four regulators knows that it takes every individual in the industry to support inclusion.

A second group often left out of consideration in the sector, is the inclusion of refugees. Part of Nash Squared's work is to collaborate with organizations such as Techfugees, who focus on supporting refugees into technology sector careers. This is valuable work that provides refugees with quality employment, personal development opportunities and networks that will help them to settle into the UK faster. To aide this, Nash Squared has further created several roles within Harvey Nash Group's IT solutions division, NashTech, specifically for recent migrants and refugees who may need extra support and job flexibility.

Recommendations:

- Nash Squared recommends the consideration of ethnic minorities and refugees as key stakeholder groups when the DRCF considers its priority areas of focus for the group's next work programme.
- Nash Squared recommends that each member regulator part of the DRCF pave the way for inclusion by creating positions specifically allocated for refugees fleeing war torn countries, who have settled in the UK.

16. News Media Association (NMA)

1. The News Media Association (the "**NMA**") is the voice of UK national, regional and local news media in all their print and digital forms - a £4 billion sector read by more than 47.4 million adults every month. Our members publish around 900 news media titles - from The Times, The Guardian, The Daily Telegraph and the Daily Mirror to the Manchester Evening News, Kent Messenger, and the Monmouthshire Beacon.

2. The NMA welcomes the opportunity to comment on the Digital Regulation Cooperation Forum's ("DRCF") workplan for 2023 to 2024 (the "Consultation"). The long-term financial sustainability of journalism, and its potential impact on media plurality, has increasingly been called into question over the last decade. This is not because consumers no longer wish to read news – the reality is that the demand for news has never been greater. Audiences turned to news publishers in record breaking numbers seeking high-quality, factchecked journalism during the Covid-19 pandemic, and have continued their patronage since. The total market reach of news brands now stands at 47.4 million people in Great Britain.[47] News publishers' considerable audience is indicative of commercial news continuing to be a valuable commodity in the modern age with a vibrant future.

3. Therefore, it is regrettable to report that, during a period of great demand, publishers' revenues are suffering in large part due to the shift of audiences from print to online, and the subsequent reliance on digital revenue streams where profit margins are considerably smaller.[48] The average digital reader is worth approximately eight times less to a publisher than a print reader.[49] The sector nonetheless has risen to the challenge by increasing the rate of digitalisation, innovation and, in some cases, moving to digital subscription (reader revenue) models. However, to sustain a diverse news media offering there must be regulatory change. The imbalance of bargaining power between publishers and digital platforms requires enforceable news media bargaining codes overseen by ex-ante regulation, for example.

4. As the DRCF will agree, it is therefore imperative that the Digital Markets, Competition and Consumer Bill, which will provide the Digital Markets Unit ("DMU") with statutory powers, is brought forward as a matter of urgency – a point that enjoys cross-party support and which the NMA continues to raise the awareness of with Government, Parliament, and officials.

5. We believe digital markets is an area where the DRCF has shown its aptitude to collaborate. By way of example, we were pleased that Ofcom and the CMA cooperated to demonstrate

[47] Data available from PAMCo.
[48] JICREG figures show that, in 2017, news media's online reach was 22% of all adults (aged +15) living in Great Britain, which has since increased to 70% in 2021. Conversely, a downward trend is visible in print form, which had a reach of 41% in 2017 to 30% in 2021.
[49] Specifically, Deloitte estimated that the industry's average annual revenue per print media user was £124 in 2016, compared to £15 per digital media user. See: Deloitte, "UK News Media: an engine of original news content and democracy", December 2016; Mediatique, DCMS, "Overview of Recent Dynamics in the UK Press Market", April 2018.

that competition in digital markets and online safety are two sides of the same coin.[50] Indeed, poor competition conditions have led to a handful of social media platforms securing entrenched market power, meaning consumers have little scope to 'vote with their feet' when online safety does not meet their expectations. In this regard, the issue is cause and effect – the Government cannot adequately succeed in its ambition to make the UK "the safest place in the world to be online" without meaningful digital markets competition reform.[51] The NMA encourages the DRCF to continue this important and impactful workstream in 2023 to 2024.

6. The Chancellor committed to bring forward the Digital Markets, Competition and Consumer Bill this session, but we recognise that the road to a fully functioning DMU remains long. Indeed, after the DMU is underpinned by statute, the DMU will have to designate companies with Strategic Market Status and implement enforceable codes of conduct. We have seen Ofcom and the CMA work effectively to co-author advice to the Department for Digital, Culture, Media and Sport on "Platforms and Content Providers, Including News Publishers".[52] There may be scope for further cross regulatory support to ensure that the DMU is prepared to function as intended as soon as it receives statutory underpinning.

7. The DRCF should also utilise its considerable breadth of knowledge, data, and experience to further evidence the harm caused to consumers and small businesses by the continued anti-competitive practices of monopolistic tech-platforms; including the financial impact on households during this time of elevated inflation. Furthermore, to demonstrate the economic benefit to UK PLC of correcting such market failures and unlocking economic potential and investment across the UK.

8. Regarding Question 3 of the Consultation,[53] we believe that the DRCF should be particularly mindful of the news media industry when prioritising its areas of focus. This will support publisher sustainability and media plurality – which are currently under threat – but crucially, the 2023 and 2024 period will see legislation for online safety and digital markets move through Parliament; policy areas that will have a seismic impact on news publishers, necessitating particular attention to our industry more than most.

We are happy to arrange a meeting to discuss any of the above and to include representatives from NMA member publications who could talk in detail about the day-to-day challenges they face if helpful.

6 January 2023

Harvey Shaw
Legal, Policy and Regulatory Affairs Advisor
News Media Association

[50] The CMA and Ofcom, "Online safety and Competition in Digital Markets: A Joint Statement Between the CMA and Ofcom" July 2022.
[51] Pg. 20 Conservative Manifesto, 2019; House of Commons Library, "Analysis of the Online Safety Bill" April 2022.
[52] The CMA and Ofcom, "Platforms and Content Providers, Including News Publishers", November 2021.
[53] Section 5, DRCF "Call for Input - Digital Regulation Cooperation Forum workplan 2023 to 2024", December 2022.