Submissions to the DRCF’s 2023/24 Workplan – Call for Input O-Z

Content

17. Ombudsman Services

Thank you for the opportunity to comment on the DRCF Call for Input on the work plan for 2023 to 2024.

In this response we have provided:

1. Background information about Ombudsman Services.
2. Comments on the proposed work plan for 2023 to 2024.

1. Background to Ombudsman Services

Ombudsman Services is a not-for-profit private limited company established in 2002 which runs a range of discrete national Alternative Dispute Resolution (ADR) schemes across different sectors, including the sole ADR scheme in the energy sector, the Ofgem-approved Energy Ombudsman. We are also one of two ADR schemes in the Communications sector approved by Ofcom and we run an appeals service for private parking.

We operate at a critical juncture between suppliers, consumers and the Government to resolve disputes. Each scheme is funded by the members and our service is free to consumers. We share data and insights to support suppliers to deliver better innovation and positive outcomes for consumers. This practice enables us to drive up standards in the industry by encouraging collaborative approaches to making improvements, managing expectations and informing policy.

Tasked with serving some of the UK's most disruptive consumer sectors, we work hard to proactively respond to the continuously evolving requirements of sectors, including our people expanding their technical expertise and our systems expanding their technological functionalities to reflect the changing way consumers are interacting with suppliers, their services and products.

We are a purpose-driven organisation which exists to build, maintain and restore trust and confidence between consumers and businesses and that technology, data and insight are key enablers in the delivery and efficacy of service. We have used data to deliver insights that support suppliers in changing their approach to customer service. In the dispute resolution area, we promote and operate what we call strategic redress. By working with all parties – including businesses and regulators – we can perform an important role to support the improvement of consumer outcomes at a macro level. Integrating redress with processes upstream (such as the way businesses deal with complaints) helps to create the right cultures and practices in businesses and helps to foster trust and confidence in the broader market.

As we have acknowledged the need to evolve, we are also moving to a new group structure under a parent company called "Trust Alliance Group". Our Group purpose strives to build, maintain and restore trust and confidence between consumers and businesses but more specifically to:

- help businesses improve service, change culture and build confidence
- help industries resolve systemic industry-wide issues; and
- harness technology and data analysis to improve services and reduce detriment.

In 2021, we acquired the Internet Commission, a non-profit organisation which promotes ethical business practice to counter online harms and increase platform accountability. Our response to this call for input is underpinned by our knowledge, expertise and interest from this part of our Group.

2. Comments on the DRCF Work Plan 2023 to 2024

We support the work plan set out for 2023 to 2024. We agree with the areas which focus on protecting children online, improving algorithmic transparency and promoting competition and privacy in online advertising. In particular we support the DRCF collaboration and capability activities which support improving knowledge sharing through expert networks. We also agree that collaboration, data and insight sharing will be important for building and underpinning a coherent approach to digital regulation, particularly as digital regulation is both a national and international challenge.

The Video Sharing Platform (VSP) Regulatory Framework to be put in place and the forthcoming Online Safety Bill have put consumer experience of digital services in the spotlight. Facilitating privacy and data sharing, as well as tackling online harms will be important for consumer wellbeing online. Digital skills and access vary across different groups - so we believe that the work plan should be mindful of how children and those who need additional support engage and use these services. With regard to the VSP regulatory framework and closer scrutiny of online services, we also believe that it is important that consumers have access to redress. From experience we know that prevention is better than ure – so we believe there is an opportunity to use data and insight, as well as robust frameworks to improve digital accountability and the consumer experience before issues occur.

We would welcome the opportunity to discuss how we can support the DRCF so please do not hesitate to contact us if you would like further information regarding our response. Our response is not confidential.

18. Onfido

We welcome the opportunity to contribute views about the Digital Regulation Cooperation Forum's (DRCF) 2023/24 work programme.

Onfido is a UK headquartered company that works globally to help businesses verify the identity of their customers and prevent fraud. Our team of 250 employees in the UK is ensuring that our technologies have a real life impact for businesses and society.

We were delighted to see the creation of the DRCF and enthusiastically support your objectives in promoting coherence and collaboration between regulators and regulatory regimes, and in continuing to develop the capabilities required to regulate in the digital age.

As you develop your workplan for next year, we want to propose an opportunity for the DRCF to achieve a relatively 'quick win' that strongly aligns with DRCF priorities and underpins its overarching objective. This proposal would encourage **coherence** and **collaboration** around a vital enabling technology for the digital economy, and highlight where relevant **capabilities** can be best shared and developed.

Our proposal

Our proposal is that the DRCF should investigate the potential to use certification against the Government's Digital Identity and Attributes Trust Framework (DIATF) as a means for digital identity and assurance providers to demonstrate compliance and best practice across the sectors DRCF members oversee, and to consider how the framework's design can support wider objectives such as the promotion of innovation and competition in digital markets.

This speaks to a risk that government and regulators create - unintentionally - a piecemeal approach to the regulation of digital identity solutions in different contexts.

We expand on this proposal in answer to the DRCF's three questions below:

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.**

Digital identity and related technologies are becoming increasingly important in a range of regulated sectors, including those covered by DRCF participating regulators (and beyond):

- **Financial Conduct Authority**: digital ID already has an important role to play in enabling financial services institutions to meet their AML KYC requirements. As the technology continues to evolve, and new use cases emerge (for example in crypto), the FCA will need to continue to develop its approach to digital ID. Further it is likely that certification against this framework will ultimately become a standard requirement for UK-based financial services customers for the ID proofing element of the onboarding process. Indeed there is discussion within government on leveraging the UK trust framework certification to meet AML IDV requirements, see p33-35 of this report.

- **Ofcom**: Digital identity will play an important role in the implementation of the Online Safety Bill - not just for child protection, but for adults too under the user empowerment duties the Bill would place on online platforms.
- **Information Commissioner's Office**: Alongside its existing responsibilities for the Age Appropriate Design Code (and the role of age assurance in supporting it), the biometric technologies that underpin the latest digital identity technologies are an area of active interest for the ICO - with draft guidelines set to be published in the spring.
- **Competition and Markets Authority / Digital Markets Unit**: interoperable digital ID solutions may play a significant role in supporting competition in digital markets e.g. in facilitating data portability (relevant also to the competition objectives and considerations of Ofcom and the ICO); the CMA and DMU may also need to consider the competition implications of Big Tech developing their own digital ID solutions in future.

Despite the wide range of current and potential use cases across different sectors, the underlying digital ID technologies will need to account for much the same considerations regardless of context, including: the accuracy and robustness of the technology, security, safety, inclusivity, accessibility, interoperability and data privacy. These are all covered by the Government's DIATF. Having a common framework against which these different aspects can be assessed offers numerous advantages - to businesses, consumers, digital ID solutions providers and the regulators (we expand on these in answer to Q3 below).

While thresholds may need to be set at different levels depending on the use case, the DIATF allows for providers to be accredited to different levels of assurance. At the highest confidence levels, this includes regular third party audits in a process that will be overseen by a new regulator, the Office for Digital Identity and Attributes (OfDIA) initially housed in DCMS. The system will be underpinned by the Data Protection Bill, providing a statutory basis and fully operational body to cement trust in the system over the long term. **The DRCF's work could explore how these different assurance levels map against requirements in sectors they regulate** (e.g. KYC requirements in the financial services sector may require digital ID providers to meet a different level of certification to use cases for social media).

However, without close cooperation between regulators, there is a danger that the UK develops a patchwork of standards and requirements that will be both burdensome and confusing, and hold back both innovation and adoption.

We see an excellent opportunity for the DRCF to demonstrate the power of **coherence** and **collaboration** by examining how participating regulators can leverage the DIATF to demonstrate compliance or best practice in a range of contexts

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 are conscious that the DRCF conducted research looking at attitudes towards age assurance last year under the "protecting children online" workstream. Our suggested area of work is both distinct and complementary to this research, insofar as it is of wider relevance than protecting children online (though important for this objective too), it is focused on implementation rather than attitudes, and it is of potential interest not just to Ofcom and the ICO, but the FCA and CMA as well.

With specific reference to the DRCF's prioritisation factors:

- **Fit with DRCF goals**: our proposed area of work aligns with and underpins the DRCF's priorities to promote coherence and collaboration, and to develop capability (as outlined above).
- **DRCF added value**: achieving a coherent approach to digital ID by leveraging the DIATF requires collaboration between all four of the DRCF's participating regulators; we believe the DRCF is the only forum through which this could happen, and that the DRCF is exceptionally well-positioned to deliver meaningful progress in a relatively short time-frame by leveraging an existing framework.
- **Alignment with legislative, economic, social and political landscape**: digital ID has an important role to play in a range of the highest priority areas - from online safety, to crypto regulation, and wider attention on the development and use of biometric technologies; digital ID is a key enabling technology for the digital economy.
- **Other regulators and / or institutional partners**: DCMS owns the DIATF currently and should be a key partner, potentially alongside other government departments that are already using the DIATF; others may include Companies House, which will be subject to new anti-fraud requirements through the Economic Crime and Corporate Transparency Bill.
- **An area where the DRCF can have a meaningful impact**: the DRCF is exceptionally well-positioned to take forward this work; the participating regulators cover many of the most significant use cases for digital ID - both today and in the near future - and the work could have enormous impact in establishing an approach that would benefit the wider economy as use cases continue to expand into new domains.

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?

A consistent approach to digital ID will provide benefits across the economy and society, and provide a clear basis for innovation and adoption of technologies that will become increasingly important to the digital economy. For example:

- **Businesses using digital ID solutions** will benefit from having a clear and consistent framework against which to judge the quality and regulatory compliance of the solutions they buy; and it will allow for a more competitive marketplace based on indicators of quality as well as price.
- **Consumers** will benefit from more rapid and wider adoption of digital ID solutions; higher levels of interoperability between systems; and a more consistent experience across use cases which will help to build familiarity with, and trust in, these solutions.
- **Digital ID providers** will have a clear set of standards for developers to innovate against; certification will enable them to demonstrate how their products meet relevant standards to potential customers.

It should be noted that **regulators**, too, will benefit - allowing them to build on the work that's already been done to build the DIATF and certification system rather than "reinventing the wheel"; and providing a common framework and vocabulary for future cooperation and collaboration around a set of technologies that will be a key element of the UK's digital future.

We hope the DRCF shares our excitement about the potential to make a rapid and meaningful impact around this important area of work. We would of course be delighted to answer any further questions the DRCF may have, and to assist in developing these ideas further.

19. Reset

Reset welcomes the opportunity to provide input about the issues that DRCF should take into consideration as it develops its plan of work for 2023 to 2024. This promises to be a pivotal moment for the UK's digital regulatory landscape with lots of opportunities to improve user experience, consumer choice and increase regulatory cooperation —– both between British regulators and with international counterparts.

We believe that in order to harness the opportunities of inter-regulatory cooperation that the forthcoming work plan should focus on a few key areas:

Transparency and Data Access

Clause 146 of the forthcoming Online Safety Bill mandates Ofcom to provide a report on how and whether independent researchers should be afforded access to data relating to social media platforms. Ofcom will be required to do this within the first two years of the Bill coming into effect. We believe that:

- Ofcom should accelerate this work in order to improve researcher access to data within a shorter time frame. The EU's Digital Services Act provides for a similar program of work and will be up and running by mid-2023. In order to ensure that British researchers are not left behind, Ofcom needs to prioritise this important transparency measure and work with European counterparts to ensure a similar standard of data access is in place in the UK. Failure to prioritise this will result in a brain drain of British researchers who will seek to get access to data via European mechanisms. Two years is too long.

- Ofcom should collaborate closely with the Information Commissioner's Office during the course of this work to ensure that the data access regime is fully compliant with UK data protection legislation and follows due process when providing access to data sets.

- Ofcom needs to ensure that data access is provided not only to verified academics and researchers but also to civil society organisations who are embedded within different UK communities and often act as what Frances Haugen, the Facebook whistleblower, described as "the canaries in the coal mine" for potential threats to online services[54]. For far too long Big Tech has benefited from a lack of transparency around its services and the harms they may cause. Over the next two years, the DRCF has a critical and long-awaited opportunity to seek to increase transparency to ensure a safer consumer experience for Britons.

[54] Haugen, Frances. 2022. "Civil Society Must Be Part of the Digital Services Act." Financial Times, March 29, 2022. https://www.ft.com/content/99bb6c10-bb09-40c0-bdd9-5b74224a5086

- Any measures to increase transparency surrounding how tech platforms operate and the societal effects of product changes need to be enhanced and welcomed.

- ‘The Report of the European Digital Media Observatory’s Working Group on Platform-to-Researcher Data access’ provides a helpful guide on the rationale and technical proposals relating to data access. Research, facilitated by improved platform-to-researcher data access can help to “identify trends, to monitor change over time, to build understanding of what is happening and why, and to develop and trial innovations that can improve society.”[55]

Third-party support for regulatory interventions

- The FCA has the power to commission skilled persons reports to inform their activities, which enables them to identify or assess risks and failures of compliance and allow regulators access to broader contextual knowledge. The Online Safety Bill bestows Ofcom with the power to commission skilled persons. To reiterate previous submissions made by Reset, we believe that all DRCF members should have such powers. Any measures that can increase capacity for identifying risks should result in appropriate risk mitigation measures that benefit British consumers.

International cooperation

- In the past half decade there has been much political debate surrounding the UK’s relationship with the world and close neighbours. During the course of Reset’s work with policymakers, civil society and politicians across Europe, Canada, Australia and the United States we have observed a widespread respect for UK regulators. This reputation stems from the independence, mandate, resourcing and efficacy of regulators like the CMA, Ofcom, ICO, and FCA. This is to be celebrated and leveraged for international cooperation.

- An excellent example of this world-leading reputation being leveraged for cooperation was last year’s ‘Data, Technology and Analytics Conference’ hosted by the CMA. By convening leaders from international counterparts and experts from academia and industry, the CMA was able to help foster international learnings and collaboration. Given the scale of the issues that the DRCF and respective regulators are attempting to tackle, often relating to some of the most well resourced and powerful companies in history, these events should become commonplace for all UK regulators.

Data Protection

[55] Tromble, Rebekah. 2022. “Report of the European Digital Media Observatory’s Working Group on Platform-To-Researcher Data Access.” https://edmo.eu/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Groupon-Platform-to-Researcher-Data-Access-2022.pdf.

- The DRCF should ensure data protection remains front and centre of the UK's digital regulatory regime. Attempts to water down the Data Protection Act should be resisted. In Reset's view, the Data Protection and Digital Information Bill is a cynical attempt to water down the data protection regime in the UK as a so-called "Brexit dividend" is wrong-headed and will damage the UK's track record on privacy, fundamental rights and lead to no tangible benefits. Furthermore, the draft Bill would hamstring and severely undermine the ICO, an integral member of the DCRF.

- In June 2022, Reset commissioned Lord Anderson QC and Aarushi Sarathi of Brick Court Chambers to draft a legal opinion in response to the government's consultation, 'Data: A New Direction.' The opinion sought to evaluate whether the proposed legislation would alter the UK's Data Adequacy arrangements with the EU. The authors wrote: "We further conclude that the adoption of these proposals will reduce the chances of obtaining a renewed Adequacy Decision from the [EU] Commission in 2025, and may even jeopardise its continuation in advance of that date."[56] The draft Bill released in late 2022 seemed to take heed of warnings from the consultation, but the Bill should be of great concern to all regulators in the DCRF.

- There is widespread consensus amongst civil society and across parties in Parliament that the adoption of the new Data Bill would have negative ramifications for businesses (small and large) who rely on the easy flow of data between the EU; the rights and privacy of British consumers and the UK economy.

- In response to the draft Bill, the Open Rights Group wrote: "The UK Data Protection and Digital Information Bill would weaken legal standards, hinder the exercise of rights, water down accountability requirements, and introduce loopholes in the law. At the same time, Ministerial powers would be unduly expanded, enabling the Government to co-opt the Information Commissioner and bend primary legislation to their likes."[57] DCRF should be seeking ways to increase data protection rather than weaken it.

Regulatory Independence:

- Recent moves by the government in various legislation have seen a concerning trend of a concerning creep of the executive branch with a consequent erosion of independence for regulators and other independent bodies. As cited above vis a vis the Data Protection and Digital Information Bill, increased ministerial powers at the expense of regulator independence has been a cross-cutting theme, including in the Online Safety Bill. The DCRF should pay close attention to this and know that many in civil society and across the political spectrum harbour concerns about this trend.

[56] Anderson KBE KC, Lord. 2022. "Propose Changes to UK Data Protection Laws: Risks to the EU's Adequacy Decision." June 30, 2022. https://www.awo.agency/files/Opinion-re-Adequacy-Decision.pdf.

[57] Santi, Mariano delli. 2022. "Analysis: The UK Data Protection and Digital Information Bill." Open Rights Group. October 19, 2022. https://www.openrightsgroup.org/publications/analysis-the-uk-data-protection-and-digital-information-bill/.

- As the OECD's guidance on regulatory independence reminds us: "Regulatory independence is not an end in itself but a means toward ensuring effective and efficient public service delivery by market players."[58] In order for all DCRF members to effectively execute their mandates, this independence is to be preserved.

- In his 2014 Currie Lecture to the Cass Business School, David Currie provides a prescient reminder of the importance of independent regulators for effective regulation: "Effective regulation needs to be independent of both the industry and government but at the same time it requires a thorough understanding of the regulated industry."[59]

Support regulatory technical audit, including through pooled technical resources

- We encourage DRCF to support technical audits conducted by regulators. While third-party audit and commissioned expert reports will be important for a robust regulatory ecosystem, they will need to be supported by regulators who can initiate, oversee, assess, and conduct technical audits themselves.

- As described in the DRCF's paper, 'Auditing algorithms: the existing landscape, role of regulators and future outlook'[60] there are three types of algorithm audit: governance, empirical and technical audits.[61] Technical audits allow auditors to look 'under the hood' of a system, including to see if there are problems with the data, source code or methods".[62] New legislation sufficiently empowers regulators to conduct technical audit, although sections of the DRCF consultation document lean towards general and governance audit. For example, the document describes the Online Safety Bill as giving Ofcom powers to "scrutinise the governance of platform's algorithms"[63], while our reading of the Online Safety Bill suggests that Ofcom is empowered to conduct technical audits.[64] Moreover, technical audit will be essential to achieve the Online Safety Bill's objectives.

- However, we encourage a broader view on technical audit. Technical audit begins with data collection, which will require sufficient information powers, to ensure that regulators can gather evidence on algorithmic systems and relevant policies, processes

[58] Baxter, Martha. 2018. "Independence of Regulators and Protection against Undue Influence - OECD." OECD. 2018. https://www.oecd.org/gov/regulatory-policy/independence-of-regulators.htm

[59] Currie, David. 2014. "The Case for the British Model of Independent Regulation 30 Years On." GOV.UK. May 21, 2014. https://www.gov.uk/government/speeches/the-case-for-the-british-model-of-independent-regulation-30-years-o

[60] "Auditing Algorithms: The Existing Landscape, Role of Regulators and Future Outlook." 2022. GOV.UK. September 23, 2022. https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/auditing-algorithms-the-existing-landscape-role-of-regulators-and-future-outlook

[61] DRCF, Auditing algorithms, p. 10.

[62] DRCF, Auditing algorithms, p. 18.

[63] DRCF, Auditing algorithms, p. 10.

[64] 11KBW, The Online Safety Bill and the powers of Ofcom Advice — available on request.

and outputs.[65] Regulators will also need access to the system itself to test inputs and outputs in a controlled environment. We believe that regulators should have the power to access data in real time to create an infrastructure for monitoring and data capture that supports on-going regulatory investigations.

- One information gathering issue that warrants further exposition is extraterritoriality. In R (KBR, Inc) v Director of the Serious Fraud Office[66], the Supreme Court ruled that the Serious Fraud Office could not demand documents held by overseas companies without an explicit power to do so.[67] This overturned a long-held practice and has severe implications for the regulation of large internet platforms, as the majority are foreign-owned. This may present a practical problem if the information required for technical audits are not directly under the control of a UK company responsible for the premises, but their parent company overseas. Regulators should be empowered to compel information, data, documents and interviews from overseas parent companies.

- As described by DRCF, methods to collect this evidence include interviews with developers, APIs and disclosure of internal documentation.[68] Additional audit methods could include:

  - Sock-puppet audits: Auditors deploy computer programs to impersonate users (‘sock-puppets’)” as inputs and record and analyse the output data generated by the platform.[69]
  - Code audits: Auditors gain direct access to the codebase of the underlying system.[70]
  - API audits: Auditors access data remotely through a programmatic interface provided by the platform that allows them to write computer programs to send and receive information to/from a platform.[71] Regulators may need specific powers to compel companies to provide access to APIs or create custom ones.[72]

- DRCF offers an opportunity for regulators to develop and pool technical resources and methods. For example, DRCF regulators may build technical tools to assess regulatory compliance, coined ‘RegTech’ by the Financial Conduct Authority.[73] A competition

[65] “Inspecting Algorithms in Social Media Platforms.” 2020. Www.adalovelaceinstitute.org. November 3, 2020. https://www.google.com/url?q=https://www.adalovelaceinstitute.org/report/inspecting-algorithms-in-social-media-platforms/&sa=D&source=docs&ust=1674834054715135&usg=AOvVaw0Ot2A7ESgnE-szbqZ9cfy5.

[66] R (KBR, Inc) v Director of the Serious Fraud Office [2021] UKSC 2.

[67] Pavlovsky, Lisa. 2021. “The Production of Overseas Evidence in Criminal Investigations - 2 Bedford Row -Barristers Chambers.” 2 Bedford Row. August 4, 2021. https://www.2bedfordrow.co.uk/the-production-of-verseas-evidence-in-criminal-investigations/.

[68] DRCF, Auditing algorithms, p. 18.

[69] “Inspecting Algorithms in Social Media Platforms.” 2020. Ada Lovelace Institute. November 3, 2020. https://www.google.com/url?q=https://www.adalovelaceinstitute.org/report/inspecting-algorithms-in-social-media-platforms/&sa=D&source=docs&ust=1674834054715135&usg=AOvVaw0Ot2A7ESgnE-szbqZ9cfy5.

[70] Ada Lovelace Institute, Technical Methods, p. 13.

[71] Ada Lovelace Institute, Technical Methods, p.13.

[72] Ada Lovelace Institute, Technical Methods, p.13.

[73] Hopwood Road, Francesca, Pavle Avramovic, and Shelley Cross. 2020. “RegTech – a Watershed Moment?” FCA Insight. June 24, 2020. https://www.fca.org.uk/insight/regtech-watershed-moment.

authority could develop a web scraping tool (similar to that developed by Mathur et al.[74]) to investigate results from a search engine. While the specific tool would investigate competition violations, it could be reconfigured to run on other platforms and investigate other types of harm (and Mathur et al. describe the versatility of their web scraper in their academic paper).[75]

- Reset believes that algorithm auditing, by third-party actors and regulators themselves, will be essential to how regulators fulfil their public function in future. DRCF research and collaboration is a crucial effort to ensure the successful regulation of online platforms and implementation of credible, sustainable digital regulation.

Framework for tendering broader engagement and consultation

- Over the past couple of years there has been a packed legislative agenda which has resulted in a heavy burden on civil society groups, academics and the non-profit sector as government and regulators have relied heavily on external expertise to inform thoughtful and effective policy making. We propose that the DRCF and member regulators should establish a formal framework in order to commission research and analysis and solicit tenders from these groups. External engagement is critical to informed policy making but many organisations have scarce resources and capacity and are not able to engage with consultations or projects as consistently as they would otherwise be able to if there was a form of engagement that allowed remuneration.

- By formally commissioning research and responses, regulators would be able to help ensure a sustainable pipeline of external research and expertise. The heavy flow of legislation (and enforcement) shows little sign of abating and this should be something that is considered. Furthermore, a formal tender process might remove the risk of conflicts of interest in the event that third-sector groups are receiving funding from companies that might be under investigation by DRCF.

Whistleblower protections and engagement:

Holding Big Tech to account for its business model and negative externalities over the past decade has proved increasingly difficult given the power imbalance between well-resourced companies and a sector-wide lack of transparency. New laws in the UK and elsewhere will hopefully increase transparency and accountability. However, up until now some of the largest scandals relating to social media platforms have only come to light as a result of brave whistleblowers. Notable examples include Frances Haugen (Facebook), Chris Wylie (Cambridge

[74] For an example of web scraping audit, see Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites', ACM Human-Computer Interaction 3, CSCW, Article 81, November 2019, 32 pages. https://dl.acm.org/doi/10.1145/3359183.

[75] Web-scraping tools will have to be purpose-built for a particular website, to automatically process the code that makes up the website's visual interface. Ada Lovelace, Technical Methods, p. 30.

Analytica) and Peter Zatko (Twitter). Whistleblowers have offered great utility to policymakers and regulators. Consequently, we believe that whistleblowers should be afforded greater protection in the UK and that these protections should be consistent across the regulators involved in the DRCF. London remains a large hub for businesses outside of Silicon Valley and consequently there are many potential opportunities for risk mitigation through whistleblowing. Important work has been done on this issue, such as the Tech Worker Handbook, and the DCRF should articulate a coherent strategy to incentivise and protect such bravery.[76] All member regulators, and consumers, would benefit from such a move.

Key stakeholder groups who should be consulted by DRCF and of particular interest when prioritising the forthcoming work plan are:

- Data protection advocates
- Human and fundamental rights experts
- Advocacy organisations from civil society, including representing marginalised groups
- Dis/misinformation experts
- International regulators and counterparts
- Children's rights groups
- Small businesses and startups

Reset

Reset seeks to improve the way in which digital information markets are governed, regulated and ultimately how they serve the public. We do this through new public policy across a variety of areas – including data privacy, competition, elections, content moderation, security, taxation and education.

To achieve our mission, we make contracts and grants to accelerate activity in countries where specific opportunities for change arise. We hope to develop and support a network of partners that will inform the public and advocate for policy change. Reset (https://www.reset.tech/) was launched in March 2020 by Luminate in partnership with the Sandler Foundation.

[76] https://techworkerhandbook.org/

20. Royal Mail

About Royal Mail

As the UK's sole designated Universal Service Provider (USP), Royal Mail is proud to deliver a 'one price goes anywhere' service on a range of letters and parcels to every address across the UK.

The Postal Services Act 2011 identifies Ofcom as the postal sector regulator. Ofcom set out the regulatory framework for the next five years in July 2022 and Royal Mail looks to work with Ofcom to ensure the regulation of Royal Mail continues to meet consumer needs and protects the USO's longer term financial sustainability. We also engage regularly with the ICO on data protection and the CMA on competition and consumer law issues, as required.

DRCF Workplan for 2023-24

Given our work with Ofcom, the ICO and the CMA, we welcome the opportunity to respond to the DRCF's invitation to stakeholders to provide views on issues that the forum should consider as it develops its workplan for 2023-24. This includes looking at how the regulatory landscape could evolve to join up existing regimes and ensure any future legislative changes facilitate a coherent approach to digital regulation.

Given Royal Mail operates across the areas and sectors for which three of the DRCF regulators are responsible, we are keen to support the forum in playing a strong role as a co-ordinating body, ensuring the different regulators work together on some of the challenges facing the postal sector today and tomorrow.

Royal Mail's overarching priority is providing a sustainable, affordable, one-price-goes-anywhere universal letter and parcel service that meets the needs of consumers, including the more vulnerable. The long-term decline in letter volumes and increases in parcel volumes mean we must change as an organisation to respond to the current challenges we face. We are keen to work with our regulators and the DCRF to secure this future and deliver the necessary change.

There are numerous regulations, like the Data Protection and Digital Information Bill and Digital Markets, Competition and Consumer Bill, due for implementation in the short to medium term. These will bring significant change that will require a greater understanding of the areas in which we operate. Regulatory frameworks need to be sufficiently adaptable and responsive to rapid changes in technology, including online marketplaces, to further accelerate innovation while ensuring responsible regulation. Therefore, we would urge early, extensive and continued engagement between the regulators and key stakeholders, including Royal Mail, to ensure that the implementation of new regulations promotes growth and maintains a fair, competitive market environment.

While we recognise the importance of information sharing between the regulators, such as to ensure coherence between regimes, we ask that to the extent possible any confidential or commercially sensitive information provided to one regulator is not shared with any other body without our explicit permission.

Should you have any questions or would like to discuss these comments further please do not hesitate to contact Jayanthi Ezekiel - Head of Regulatory Strategy and Policy - on [redacted]

21.techUK

Introduction:

techUK and our members have welcomed the creation of the DRCF and want to see the organisation develop to become a successful and long-lasting part of the UK's regulatory architecture.

We are supportive of the DRCF model, seeing this as a more effective way of achieving regulatory coordination and coherence than the idea of a single regulator for digital services. Our members see the DRCF as a key development for improving regulation and regulatory behaviours at a time when the Government is pursuing significant new legislation and regulation, creating competing and concurrent duties between regulators across a range of areas.

Against this backdrop, the DRCF has already started playing a role in clarifying regulators responsibilities and thinking. For example, through statements on the intersection of different proposed regulator regimes, through the publication of joint research such as on attitudes towards age assurance and publishing summaries of roundtables on technologies which can create tensions between regulatory objectives, such End-to-End Encryption.

Getting this right and ensuring a well-functioning DRCF is vital to the aims of the Government's Plan for Digital Regulation and it's three principles (i) Actively promote innovation, (ii) Achieve forward-looking and coherent outcomes and (iii) Exploit opportunities and address challenges in the international arena.

techUK welcomed the DRCF 2022/23 workplan as providing greater transparency over the DRCF's aims for the year as well as setting out specific work programmes and structures that industry could engage with. The call for inputs on the 2023/24 workplan is a further welcome step to improve transparency to support industry and stakeholder engagement.

In our response to the DRCF's call for input into its 2023/24 workplan we provide our reflections on the operation of the DRCF in 2022 and early 2023 under its three themes (Coherence, Collaboration and Capability) and provide suggestions for how the organisation could build on these in it's third year of operation.

This response is informed by techUK's own engagement with the DRCF as well as feedback from members over the last year.

Coherence:

The DRCF has delivered welcome extra clarity: techUK and our members have welcomed the increased clarity provided by the DRCF under this theme, in particular roundtable discussions and the publication of summaries to show how the DRCF is engaging with the industry on technologies which pose challenges for cross cutting regulatory objectives. For example, through the roundtable on End-to-end encryption.

However, this could go further: we would encourage the further use of these roundtables as methods to explore regulatory questions raised by particular technologies. We see these as vital for informing and educating regulator(s) on the technologies themselves and their design, providing transparency on areas of focus for the DRCF as well as informing public debate and providing an avenue for businesses to input in a secure and anonymous way.

Statements on regulatory overlap are welcome but high level: techUK has also welcomed statements published regulators view on regulatory regimes which can have some inherent tensions, for example between competition, privacy and online safety objectives. These statements however remain high level and we would welcome in the 2023/24 workplan further details and plans for engagement on how the DRCF aims to explore these issues further and identify potential points of tension in emerging regimes so these can be addressed once legislation has been passed and implementation by regulators begins. Examples of this might include on age assurance and verification, further work on end-to-end encryption and access to data/ data portability proposals that emerge through the UK's pro-competition regime for digital markets.

There is a lack of knowledge on how the DRCF works in practice and this can distort expectations: through its coherence objective the DRCF has been able to improve its awareness across the tech industry. However through techUK's own conversations with members and stakeholders there remains a limited understanding of the operating model of the DRCF. This can lead stakeholders to inadvertently view the DRCF as being responsible for setting regulatory guidance separate to the four regulators it works across.

This not aligned with the spoke and wheel model through which the DRCF operates and its function of improving the processes within and between the four regulators. We believe extra clarity could be provided by the DRCF by publishing details of how it operates in the 2023/24 work plan including for example the level of resourcing received from the four regulators, details on how the expert groups operate in practice and examples of where stakeholders should seek to refer issues to the DRCF and the likely actions that may be taken by the DRCF in response.

This we believe would help improve the awareness of the role of the DRCF and prevent it from being inadvertently viewed as a single regulator for digital services.

Collaboration:

techUK has welcomed the work of the DRCF on algorithmic transparency and its recognition that regulatory approaches to algorithmic processing should depend on levels of risk. In our response to the DRCF Algorithmic Processing Workstream Papers, we did however highlight that greater clarity could have been provided on what regulation already exists when it comes to addressing some of the harms associated with AI. techUK members, in particular SMEs, would appreciate the support to help navigate the breadth of existing guidance in this area.

The objective to support innovation is welcome but could be developed further: techUK's members particularly welcome the commitment of the DRCF to better enable innovation in regulated industries. This has an important role in supporting the objectives of the Plan for Digital Regulation. We look forward to seeing further details of the funded project on assessing whether and how to introduce a multi-agency advice service for innovators via a joined-up regulatory advice.

However further to this we would encourage the DRCF to expand its work on seeking to better enable innovation by exploring the possibilities of joint sandboxes between regulators and running workshops or an 'explorer' series to understand as, new regimes emerge, potential best practices and schemes that the regulators could undertake to provide clarity to businesses seeking to innovate in a period of change.

Two examples of this could include:

- A project focused on ensuring a coherent approach to the use of Digital Identities, that would examine how plans for a Digital Identity and Attributes Trust Framework (DIATF) can support digital ID to be used effectively and support regulatory objectives across all four DRCF regulators and new regimes in development, for example the data protection, online safety and pro-competition regimes.

- The DRCF might also wish to explore the impact of Automated Learning (AI) and Machine Learnings' (ML) on the FCA/PRA's regulation of operational resilience. As AI and ML looks set to change vital business processes within the financial services sector greater cross-sector collaboration, and regulatory coordination (domestic and international) could ensure more effective compliance within both FMI's and Critical Third Parties. At the same involving firms in discussions around changing regulatory policy could help better ensure the effective, safe and secure uptake of new technologies.

Any outreach or projects in this space should take a special focus on smaller firms. This would hopefully provide useful feedback to the DRCF on how smaller and challenger companies are confronting new and cross regulatory requirements.

Capability:

Transparency over knowledge networks is welcome and should be continued: The DRCF’s work to build knowledge networks has been welcomed and helped support engagement with techUK and our members. In the 2023/24 workplan greater clarity on the progress of the five knowledge networks mentioned on the 2022/23 workplan (regulatory and supervisory technologies, cloud services, advertising technologies, choice architecture and privacy-enhancing technologies) would be appreciated as well as detail on plans to establish any further knowledge networks.

techUK would encourage the DRCF to be more specific about the issues being considered by these networks as the expert group headings are very broad and provide limited detail on the work being undertaken. This extra level of detail would be appreciated by stakeholders and helps the industry understand key focus’ across the four regulators.

The DRCF’s symposiums have been a welcome initiative: techUK has welcomed the symposiums on the metaverse and Web 3.0. These provide good opportunities to engage with regulators and broader stakeholders around emerging technologies. The DRCF should continue to host these events, continued to run these as exploratory sessions and ensure that it is involving a range of market participants and innovators in order to gather the greatest breadth of experiences and perspectives.

The DRCF must be mindful to engage with smaller and challenger firms: techUK has received feedback from members that engagement with the DRCF remains difficult. This has come principally from smaller and challenger firms. techUK would encourage the DRCF to work with partners to improve outreach to these communities. techUK has worked with the DRCF to support this kind of outreach in the past and would be happy to do so again in the future.

Recruitment and retention of specialist talent is vital: we strong welcome this focus of the DRCF. Ensuring regulators have expert and specialist staff that have good knowledge and experience of the sectors they are regulating is vital to good regulatory outcomes both for consumers and for businesses. The DRCF should continue to prioritise this objective.

22. Tony Blair Institute

About the Institute

The Tony Blair Institute for Global Change (TBI) aims to equip leaders to build open, inclusive and prosperous societies in an interconnected world. We seek to achieve change through politics and institutions, and we do this by developing policy and advising governments. We are a not-for-profit organisation with a staff of 500 and a presence in over 20 countries.

We have a dedicated Technology and Public Policy team to equip the world's leaders to master the revolution in technology. We aim to influence policy by curating the key debates and generating politically actionable policy and strategy, while convening a structured, productive dialogue between leaders in tech and politics. Our team engages high-level tech sector businesses and policymakers to bridge the gap and publish papers on pressing relevant issues. We have four pillars of work in the team looking at (1) internet policy and digital platforms (2) digital government, (3) science and innovation and (4) tech for development.

You can find links to all our recent work at institute.global.

Response

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.

1. Extend the audit model across different types of digital regulation, and not just algorithms
    - The DRCF has already started to coordinate algorithmic audit across digital regulators, including the CMA, ICO and Ofcom. While the Online Safety Bill does extend Ofcom's information gathering powers, it may also be worth exploring how the audit model could be applied across different information asymmetries in tech regulation, and not just to algorithms.
    - The major benefit of audit is thought to be in rebalancing information asymmetry between the regulated and regulator, but it is also useful for providing a 'stamp of approval' and thus building trust with digital platforms. It enables regulators to scrutinise decision making processes, as well as outcomes, which is especially difficult for regulation of notoriously subjective decisions like online harms.
    - It is true that transparency reports are a smaller regulatory burden, but corporate audits of **all parts** of a business is commonplace in other industries. They are generally effective (with some notable exceptions) and provide continuous reassurance for the regulator and the public.

- The alternative - telecoms-style information-gathering powers - provides broad powers linked to specific investigations, and creates clear incentives, accountability and enforcement powers. However, speculative requests can be resource intensive for companies. Ongoing scrutiny and social media regulation for example is a very different task to broadcast or telecoms regulation.
- It is worth differentiating between audit type and audit purpose. You can have different types of audits:
    - Technical/algorithmic process audits that look in depth at algorithmic workings
    - Results-based audits that more look at inputs/outputs of a system
    - Business model/corporate-type audits that look more at business processes/other aspects
- Other digital regulation areas where audit models could be deployed:
    - Online safety
    - Processing of personal data and privacy
    - Ad based fraud

2. Develop a framework to regulate crypto assets in the UK from financial, national security, data protection, consumer protection and competition standpoints.
    - The global crypto assets market in 2022 underwent severe turbulence in a sustained indication of the volatility that roils these assets and, by extension, investors and governments.
        - Cryptocurrencies plummeted worldwide in a resurgence of 2018's 'crypto winter' phenomenon. Bitcoin, the first and most popular cryptocurrency, lost close to 60 percent of its value.
        - In November 2022, the second-largest cryptocurrency exchange FTX, collapsed, triggering the largest crypto-related bankruptcy ever. Other market participants like BlockFi and Genesis Global Capital are feeling the reverberations and have paused withdrawals.
        - Users lost hundreds of millions of dollars to crypto hackers in 2022, including through three of the largest cryptocurrency hacks to-date.
    - Despite this, crypto assets in the UK (with the exception of security tokens) are not regulated.
        - The FCA oversees anti-money laundering and terrorist financing procedures in crypto asset firms but does not regulate non-security tokens.
        - The UK government, through the Advertising Standards Agency, has also been keen to investigate the promotion of such assets to consumers through online media like social networking platforms.
    - Regulating non-security crypto assets as well is in the UK's best interests and in line with the DRCF's mission and its 2022 goals.
        - Europe became the world's largest crypto market in 2022, with the UK the largest national market in the region. Europe constitutes over a

        quarter of global crypto activity and the UK is poised to lead its regulation in this region, if not globally.

        - In 2022, the DRCF focused on protecting vulnerable consumers like children online as well as promoting competition and privacy in the online ads market.
        - By expanding their purview to crypto assets, the DRCF will continue improving consumer rights online and regulating the online ads market while enabling digital financial innovation, building on synergies among its constituent agencies and leveraging its horizon scanning activities.
        - This will draw on expertise from all four agencies, especially the FCA, the CMA and the ICO.

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?**

    - Explore further areas of alignment with international regulators on issues like competition, data governance and cybersecurity, including encouraging the formation of DCRF equivalents in emerging digital economies to help streamline alignment and coordination.
        - With the explosion of the consumer internet over the last thirty years, businesses have ventured into cross-border trade with ease, from retailers to financial service providers.
        - These global tech firms have vast repositories of data, money and labour to lobby decision-makers and stave off regulatory action. Regulators, meanwhile, continue to be limited by resources and geography.
        - Through Brexit, the UK recognised a unique opportunity to establish its footprint as a global regulatory force. To realise this, it needs to communicate and collaborate with international regulators to leverage their collective strength, especially on digital issues.
        - Further, this is in line with what the DRCF and related UK government agencies' strategy over the last few years. In 2020 the Department for Business, Energy and Industrial Strategy (BEIS) recognised the need for international regulatory cooperation and coherence to promote trade and a 'Global Britain.' In 2022, the DRCF itself has been focused on mapping regulatory interactions among agencies and building expert networks.
        - Encouraging the export of the DCRF model to emerging digital economies will aid alignment and create parallel points of contact to reduce friction between regulators globally.

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?**

- DCRF priority areas of focus for 2023 should also include digital labour platform workers.
  - As multi-sided platforms continue to proliferate in the UK, as many as one-fifth of British workers can be classified as non-traditional, in roles like freelancers, sub-contractors and gig workers.
  - Despite and even prior to this, the UK has one of the least-regulated labour markets and there is speculation that the government favours further deregulation. Currently, the UK follows a three-tiered system of employee, self-employed and workers.
  - This stakeholder group intersects with the DRCF's mission of developing a coherent joined-up approach to digital regulation. For example, without adequate supply of labour opportunities (i.e. competition among digital labour platforms), workers may be forced to accept those with subpar income and/or benefits.
  - Further, this ties into and builds upon the DRCF's collaboration with the Department for Business, Energy and Industrial Strategy (BEIS) in 2022, on innovators in the digital economy.
  - Finally, this focus will be timely given BEIS' recent guidance on gig workers that clarifies rights for workers and providers advice for businesses.

Acknowledgements

If you would like to discuss any points included here in further detail, please reach out to the below individuals:
Rhea Subramanya – [redacted]
Rosie Beacon – [redacted]
Melanie Garson – [redacted]

23. Vodafone

Vodafone welcomes the opportunity to input into the DCRF workplan 22/23. Given the complexity and constantly evolving nature of digital markets, the work of the DCRF is increasingly vital if the United Kingdom is to establish robust and coherent digital regulation. The communications sector has a long-established regulatory approach that largely predates the existence of digital markets. The rising prominence of digital markets and increasing consumer dependency upon them means that regulation needs to evolve, both in terms of regulating digital markets where it is proportionate to do so and updating or removing regulation from traditional regulated sectors to ensure there is a consistent and level playfield for all.

We firmly believe that competition remains the best remedy to deliver for consumers, allowing them to take advantage of both supplier choice and reap the benefits of innovation. This can't happen if digital markets aren't contestable or inappropriate burdens remain in traditional sectors that don't apply to broadly equivalent digital services. Given the different jurisdictions and competencies of the various regulators who span these markets, a coherent and joined up approach is needed. Issues should never be allowed to fall between the cracks and there should be an active desire to explore topics from a number of different perspectives to ensure that all angles and viewpoints are properly considered. This means regulators working together collaboratively for the good of consumers and the wider UK economy.

We need to remain cautious around the potential outcomes resulting from very large digital gatekeeps entering existing markets. The traditional competition assessment framework may not be appropriate in these cases as leverage from existing digital markets can quickly be exploited, even from an initial position of zero market share destabilising previously competitive markets to the long-term detriment of consumers.

In the past decade we've seen the digital landscape change massively and there is little sign that the pace of change is slowing. This necessitates a more dynamic approach to regulation that is more flexible, with an emphasis on fairness. Many digital markets are now firmly established and need to make an active contribution towards public good outcomes. This means sharing burdens more evenly, seeking to open more markets to competition and wider distribution of obligations where they remain appropriate.

We have considered the questions posted in the draft workplan with our responses set out below:

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.**

Regulators' work such as the CMA's mobile ecosystem market study, the investigation into mobile browsers and cloud gaming, Ofcom's review of the mobile market and the Government's wireless strategy review have fixed and limited scope leaving out important aspects of market analysis. We have highlighted in submissions the interlock of connectivity markets and the mobile ecosystem and therefore the need to cast analysis more widely. For example, the CMA has found evidence of market dominance in the mobile ecosystem. Ofcom's mobile market review expects investment in new 5G networks, yet an unresolved concern for investors of those networks is the ability to generate investment returns for the networks. There are actions that operating systems owners can take which can be either positive or negative but are outside of the control of the 5G network investor, yet this important analysis is beyond the scope of Ofcom's and the CMA's work.

Ofcom's forthcoming review on Online personal communications services is another important area of work. Ofcom have expressed an interest to better understand these services and how they are used and valued by consumers (such as WhatsApp or Zoom). There is clearly a significant difference in the regulatory approach to these services and more traditional services in the calling and messaging markets. There are number of areas to consider around competition, consumer protection, access to essential services and securing end to end connectivity and it is likely that they will need considered by a number of different regulatory bodies to ensure a meaningful outcome.

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?**

With its cross-department expertise on technology and innovation the DCRF would be well placed to identify the practical barriers- technological and commercial that can stand in the way of achieving desired competition and regulatory outcomes. For example, enabling consumers to port data to promote device competition does not consider the role of the distribution chain in brand promotion.

3. **We have the following comments on the workplan.**

We will follow your work package on protecting children online with interest, sharing relevant findings from our news centre and digital parenting readers resource pages which can be found at https://www.vodafone.co.uk/newscentre/smart-living/digital-parenting/

Your work on mapping interactions between relevant regulatory regimes is very important as is understanding which organisation is the lead on topics to enable efficient escalation of important issues.

We discuss in response to question 1 the challenges that exist with incentivising investment in 5G networks. The 5G ecosystem via the development of innovative 5G applications and devices are also core to the deployment of extensive and high quality 5G networks. We have worked extensively on case study applications and support any additional focus on the enablement of innovation. Case studies (vodafone.com)

Horizon scanning is an important aspect of a regulators work. We were pleased to contribute to the Web.30 symposia and show case to Ofcom our progress with the Openran technology and look forward to sharing and learning in the year ahead.

24. Which?

Which? welcomes the opportunity to respond to the Digital Regulation Cooperation Forum (DRCF)’s call for input on their 2023/24 workplan. We support the DRCF’s activities and acknowledge their important role in coordinating functions across the FCA, ICO, CMA and Ofcom.

The DRCF has a vital role in ensuring greater cohesion, collaboration and helping developing the necessary capabilities between regulators of digital services. Given that role, we urge the DCRF to include the following four priorities in their workplan:

- Facilitate opening and sharing fraud data between regulators and industry to improve online fraud prevention and reporting
- Ensure coherent regulation of artificial intelligence (AI)
- Facilitate the implementation of smart data schemes
- Ensure a coherent cybersecurity regulatory framework

Facilitate opening and sharing fraud data between regulators and with industry

We welcomed the inclusion in the DRCF’s 2022/23 workplan to ***“optimise information sharing and platform engagement”*** in relation to the Online Safety Bill (OSB) *and* ***“map interactions between relevant regulatory regimes”***.[77] We believe that collaboration 1 between regulators to share data presents an opportunity to better tackle online fraud.

The scale of fraud in the UK is immense. In 2021, UK scam victims lost £2.6 billion in total, demonstrating a significant financial harm to UK consumers.[78] Recent data from the Home 2 Office has also shown that fraud accounts for 41% of crime, a staggering figure considering fraud prevention only takes up 1% of law enforcement resources.[79]

Which? has been a vocal champion for the Online Safety Bill and we have worked for a number of years to ensure platforms are accountable for preventing fraud in relation to paid for advertising. Now that the Bill is progressing, the DRCF has an opportunity to support Ofcom as it develops new codes of practice which will set out the requirements of platforms to prevent fraud. Which? proposes that platforms should be using data held by the other regulators as part of their fraud prevention processes. We also urge the DRCF to work with Ofcom to ensure that the fraud data submitted by platforms will be useful to all the regulators and industries they work with.

[77] “Digital Regulation Cooperation Forum workplan 2022 to 2023”, DRCF, April 2022 https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-2022-to-2023

[78] “TOWARD A FUTURE WITHOUT FRAUD: How platforms can do more to tackle misleading and fraudulent adverts online”, Which?; Demos Consulting, December 2022, https://www.which.co.uk/policy-and-insight/article/toward-a-future-without-fraud-asOA54p6cVLo

[79] “Fighting Fraud: Breaking the Chain”, House of Lords Digital Fraud Committee, November 2022, https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf

The DRCF should take on the role of facilitator on behalf of the regulators to reach a consensus definition of what data collected from platforms and regulators can be used to take positive action to protect consumers by preventing fraud across relevant industries.

A current example in practice is some online platforms having used FCA data from the Financial Services Register in order to prevent scams since 2020.[80] Platforms like Google and TikTok perform checks against the FCA's register to prevent bad actors publishing advertising and therefore reaching consumers. Google told a House of Lords Committee that this had "***almost all but eliminated scams on Google search***."[81] Which? believe thatplatforms should be required to make similar checks by Ofcom under the OSB.

The data that the ICO holds on data breaches should be reviewed to assess its value to a wider ecosystem of fraud prevention. We note that the recently published joint statement from Ofcom and the ICO on online safety and data protection includes a commitment to "***sharing information and intelligence as appropriate and coordinating approaches to compliance and enforcement***".[82] As part of this, we would like the DRCF to push this area of collaboration further to see how the data that the ICO holds on data breaches can be of value in the fraud prevention ecosystem.

We therefore recommend that the DRCF focuses on:

- collaboration on the Ofcom codes of practice to maximise the use of data used by the platforms and from the platforms to increase consumer protection against fraud across regulators and sectors;
- collaboration between the regulators to identify what data on suspected fraud/suspicious activity is currently collected by the regulators to determine whether there is data that could be directly actionable for service providers across sectors to tackle fraud and agree the minimal amount of data that can be shared to have this effect.

Ensure coherent regulation of AI across sectors

We welcome the inclusion of algorithmic transparency in the DRCF's 2022/23 workplan and the work that has been done so far in this area. We are supportive of AI and the benefits that it can bring consumers, including greater choice for products, services and personalisation.

[80] Fraud Act 2006 and Digital Fraud, https://committees.parliament.uk/oralevidence/10281/html/

[81] https://committees.parliament.uk/oralevidence/10268/html/

[82] "Online safety and data protection: a joint statement by Ofcom and the Information Commissioner's Office", CMA, November 2022, https://www.gov.uk/government/publications/online-safety-and-data-protection-a-joint-statement-by-ofcom-and-the-information-commissioners-office

However, the current regulatory landscape for AI is complicated, with guidance coming from different regulators, including the ICO[83] and FCA,[84] as well as the inclusion of automated decision making in several pieces of legislation including the Data Protection Act 2018, UK GDPR, Equality Law and Consumer Protections from Unfair Trading Regulations 2008.

Which?'s engagement with businesses of various sizes has shown that businesses struggle to find clarity or take positive action where there are multiple sources of guidance. This ultimately impacts consumers who will face different experiences with how the technology is applied and then their ability to seek redress, ultimately impacting on consumer's confidence and trust in that technology. We note that lack of clarity is particularly acute for smaller businesses.

We therefore urge the DRCF to focus attention on developing coherence across the regulator's guidance on AI. The approach should examine cross industry compliance with principles including, transparency, safety, accountability, fairness and access to redress, which are set out in the DCMS policy paper '*Establishing a Pro-Innovation Approach to AI regulation*'[85] published in July 2022. This is key to building clarity for business to procure and implement AI with best practice in mind and developing clear routes to redress on behalf of consumers.

There is a lack of AI expertise available in the UK as highlighted in a speech by Prime Minister Rishi Sunak in November 2022.[86] This impacts industry, the regulators and the consumer's experience. Expertise is essential to achieving best practice and effective monitoring of take up of the principles. To combat this, Which? have urged DCMS to consider establishing a group of AI experts to provide advice to regulators and businesses on AI regulation.

Which? welcomes the DRCF recognition that its members' current understanding of the risks associated with algorithmic processing is limited.[87] We recommend that the DRCF works with the different regulators to set up a group of AI experts and achieve a basis to share AI resource capability and expertise to achieve the coherence we are calling for in the guidance and monitoring.

With the imminent publication of a DCMS white paper on AI regulation, we recommend the DRCF work with the relevant regulators in the:

[83] "Guidance on AI and data protection", ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/

[84] "The AI Public-Private Forum", FCA; Bank of England, October 2020, https://www.fca.org.uk/publications/discussion-papers/dp22-4-artificial-intelligence

[85] "Establishing a pro-innovation approach to regulating AI", DCMS, July 2022, https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishinga-pro-innovation-approach-to-regulating-ai-policy-statement

[86] Further, in 2021 49% of firms were affected by a lack of candidates with technical skills and 55% of firms reported gaps in employee's understanding of AI concepts of algorithms. Statistics from "9 key findings from Understanding the UK AI labour market: 2020 Report", DCMS, May 2021, https://www.gov.uk/government/publications/understanding-the-uk-ai-labour-market-2020/9-key-findings-from-understanding-the-uk-ai-labour-market-2020-report

[87] "The benefits and harms of algorithms: a shared perspective from the four digital regulators", DRCF, June 2022, https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/the-benefits-and-harms-of-algorithms-a-shared-perspective-from-the-four-digital-regulators#executive-summary

- harmonisation of AI best practice guidance for business across the regulators with a view to have a coherent approach across sectors;
- establishing an oversight group of AI experts to the DRCF members to share capability and knowledge.

We would also like to draw the DRCF's attention to small businesses as a key stakeholder when looking at AI regulations and monitoring. The majority of UK businesses will procure AI as a product, rather than develop it in-house. It is imperative that consumers have consistent safe and transparent experiences when AI is applied, regardless of the size of the organisation they are transacting with. We encourage the DRCF to bring regulators together to support SMEs as they utilise the new technology.

Implementation of smart data schemes

Part 3 of the Data Protection and Digital Information (DPDI) Bill, introduced in July 2022 and currently awaiting its 2nd reading in parliament, seeks to implement a framework for the introduction (via secondary regulations) of smart data schemes in different sectors of the economy. The FCA already oversees Open Banking, which enables consumers to consent to sharing their financial data with third parties for improved services, leading to them saving money. Analysis shows that consumers could stand to gain £18bn from Open Banking.[88] Ofcom has previously consulted on Open Communications, a proposed smart data scheme in the telecoms sectors and the FCA and CMA recently issued a joint statement[89] which gave an update on the future of open banking and the introduction of Open Finance.

We are supportive of the introduction of smart data schemes when they are designed in ways that bring benefits such as savings and greater choice to consumers. This includes greater control over their data, more competition and innovation across sectors where data can be used to provide better personalisation of services and products. To mitigate against unintended consequences, such as data being onward shared with unregulated third parties without consent, consumer protection principles must be built in from the start.

These protections must be based around principles that include:

- consumer consent
- consumer control

[88] Consumer Priorities for Open Banking", Faith Reynolds; Mark Chidley, June 2019 https://www.openbanking.org.uk/wp-content/uploads/2021/04/Consumer-Priorities-for-Open-Banking-report-June-2019.pdf

[89] "Joint statement by HM Treasury, the CMA, the FCA and the PSR to update on the future of Open Banking", CMA, FCA, PSR, HM Treasury, December 2022, https://www.gov.uk/government/publications/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-to-update-on-the-future-of-open-banking/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-to-update-on-the-future-of-open-banking

- consumer education
- transparency

The DRCF has the opportunity to facilitate the design of cross sectoral smart data schemes, to ensure any emerging harms which come from the roll out of the technology are identified and mitigated between sectors, implementing a safety by design approach. This is much like the DRCF's ICO & Ofcom joint statement on the online safety and data protection[90] which called for:

1. Users of online services to have confidence that their safety and privacy will be upheld and that we will take prompt and effective action when providers fail in their obligations.
2. Providers of online services of all sizes to comply with their obligations and to continue to innovate and grow, supported by regulatory clarity and free from undue burden.

The DRCF should prioritise smart data for 2023/24, with a specific aim to achieve a shared approach for ensuring consumer protections are embedded at the design stage and realised during the implementation and use stages.

Coherent cybersecurity regulatory framework

Cybersecurity is an area Which? is particularly concerned about. DCMS published research which showed that smaller organisations take little proactive action on cybersecurity due to lack of knowledge and competing priorities with budgets.[91] Just 4% of smaller businesses say they have accessed the NCSC's small business offerings, with similarly small numbers accessing advice from the police on cybercrime prevention.[92] This is startling when compared to the prevalence of cybersecurity breaches for SMEs - with the majority of cyber-enabled business crime reports to Action Fraud in 2021/22 being made by SMEs.[93]

Which? urges the DRCF to be particularly mindful of SMEs as an important stakeholder group when developing their plan of work for 2023/24, to ensure that consumers are not left with unequal protections which are dependent on the size of the organisation they transact with.

As with AI, there is guidance on cyber security issued by multiple regulators, as well as many different law enforcement agencies working on cybercrime making it difficult for small

[90] 4 “Online safety and data protection: a joint statement by Ofcom and the Information Commissioner's Office”, CMA, November 2022, https://www.gov.uk/government/publications/online-safety-and-data-protection-a-joint-statement-by-ofcom-and-the-information-commissioners-office

[91] “Cyber Security Breaches Survey 2022”, DCMS, July 2022, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[92] “Calling Time on Business Crime”, FSB, https://www.fsb.org.uk/resource-report/calling-time-on-business-crime.html

[93] “Fraud and Cybercrime National Statistics”, Action Fraud, https://www.actionfraud.police.uk/data5

businesses to understand who they should be working with.[94] Which? engagement with relevant stakeholders suggest that businesses find the fragmented regulatory approach confusing. This adds to the difficulties small businesses have with engaging with cybersecurity where it can be difficult to know who to talk to and to deal with the technical jargon.[95]

There are also concerns about the level of expert resource available to the regulators to monitor the scale of attack and breaches. Which? recommends that resource expertise in cyber security be upscaled and used efficiently across the regulators to reach a coherence on best practice guidance for any size business.

As the Home Office prioritises its Cyber Security Duty to Protect[96] work programme this year, and DCMS builds on its January 2022 cybersecurity incentives and regulation review[97] the DRCF must:

- seek to harmonise cybersecurity best practice guidance approaches across the regulators;
- ensure there is sufficient cyber security expertise resources shared across the regulators to avoid duplication of effort or conflicting approach;
- build consensus across the regulatory landscape that cybersecurity risks in both SMEs as well as big businesses can cause consumer harm.

Without a clear, complimentary, collaborative approach on cybersecurity for businesses the risk continues that consumers will have unequal protections based on the size of the business they are transacting with.

About Which?

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good, here to make life simpler, fairer and safer for everyone. We're the independent consumer voice that provides impartial advice, investigates, holds businesses to account and works with policymakers to make change happen. We fund our work mainly through member

[94] Best practice guidance is issued by the ICO and Ofcom under the Network and Information Systems (NIS) regulations https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018; "Security Guidance", ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/#:~:text=your%20cybersecurity%20measures%20need%20to,appropriate%20to%20your%20business%2 0practices; "Network and Security Guidance", Ofcom, https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience

[95] "Calling Time on Business Crime", FSB, https://www.fsb.org.uk/resource-report/calling-time-on-business-crime

[96] Home Office call for evidence https://www.gov.uk/government/consultations/unauthorised-access-to-online-accounts-and-personal-data/call-for-information-unauthorised-access-to-online-accounts-and-personal-data

[97] DCMS Policy Paper 2022 cyber security incentives and regulation review https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-se curity-incentives-and-regulation-review#foundations-advice-guidance-and-campaigns

subscriptions. We're not influenced by third parties – we never take advertising and we buy all the products that we test.

For more information contact Bethany Marson, Policy Adviser at [redacted], November 2022

25. Yoti

Organisation name: Yoti
Respondent full name: Julie Dawson, Chief Policy & Regulatory Officer Florian Chevoppe-Verdier, Public Policy Associate
Email address: [redacted], [redacted]
Contact phone number: [redacted]

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

New technologies

Yoti would draw the DRCF's attention to recent evolutions in digital identity as well as AI Age estimation technologies, which have a great potential in helping it and its members reach many of the objectives it has set in terms of improving public trust in technology and protecting vulnerable people online. AI age estimation could for instance enable organisations to ensure that content is age appropriate and that adult advertising is not misdirected to minors.

In 2021, the United Kingdom Digital Identity & Attributes Trust Framework (UDKIATF) was a major step forward as it saw the accreditation of digital identity service providers by the UK Government, of which Yoti and the Post Office was the first in May of that year.

Participation in various intergovernmental and inter-regulators working groups

Structures exist already that allow like minded governments to collaborate on sectoral initiatives such as the Agile Nations. Therefore, we would encourage the DRCF to consider participating in these fora where cross-border work structures exist already and where it can collaborate with other nations' regulators on developing supervisory technologies and enforcement mechanisms for large, international digital industry which will be in scope of the upcoming online safety regimes across the globe.

Membership of the DCRF

In order to capture the largest possible breadth of expertise, we would suggest that the DRCF be widened to welcome additional member regulators and bodies. These could include the Advertising Standards Authority, Center for Data Ethics & Innovation, the Digital Markets Unit, and the Gambling Commission.

Other bodies such as Government departments could also be included into the DRCF as observers, such as the Home Office and its alcohol age verification sandbox[98] trials team, the DVLA, the Government Digital Service, the DCMS, and the UK's delegation to the Agile Nations group. Observer status could be considered so as not to compromise the DRCF's independence.

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 work plan?**

We believe the DRCF should prioritise work dependent on how likely it is that collaboration between member regulators would result in the deterrence of specific harms and the protection of vulnerable people online.

We would also encourage the DRCF to consider building and implementing a joint plan for consumer education and experiential research in conjunction with industry representatives.

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?**

Yoti would encourage the DRCF and its member regulators to work in a spirit of transparency and accountability. This could be achieved by ensuring that work is carried out in a transparent and clear manner, with regular and thorough engagement with the largest possible number of civil society groups and business representatives. The work of the DRCF could also be made more transparent, including through the publication of regular reports and meeting minutes, as well as an organigram.

This would ensure that the public is more confident about the DRCF's critical work, and that it can scrutinise and participate in it. Engagement with business would ensure that regulator staff can keep abreast of the ever-changing landscape of technological and private sector evolutions.

We would also welcome discussions between member regulators on how research is coordinated and planned where it can benefit all participants. Research could also lead to the development of joined up consumer education campaigns similar to Ofcom's Making Sense of Media (MSOM) duties.

[98] Age verification technology in alcohol sales, From the Home Office and Office for Product Safety and Standards, published on 18 March 2021 and last updated on 30 December 2022. https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox