2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? response to the Digital Regulation: Driving growth and unlocking innovation policy paper

27th September 2021

Introduction

Which? welcomes the Digital Regulation - Driving growth and unlocking innovation policy paper. We welcome the intention to "ensure a coherent, innovation-friendly and streamlined regulatory landscape", the intention to "provide businesses with certainty" and to "give people the confidence they need to engage with digital technologies safely". We welcome the move to create the Digital Markets Unit, the pro-competition regime and the voluntary creation of the Digital Regulation Co-operation Forum.

Which? believes that consumers' digital lives should be enriched with choice across a wide range of products, services and markets. Consumers should be able to purchase and engage with exciting innovations that are designed, built and maintained with privacy by design, security by design and fairness by design at the very core and that the rights consumers have should include data rights and data protection.

We welcome the government's push to ensure that the complex, multifaceted digital landscape of today is regulated and that consideration is being given to what the future challenges in the digital and innovation space will be. But Which? is concerned by reference to deregulation in the policy paper and wider suggestion that regulation inhibits growth and innovation. If done well, regulation can ensure that there are clear rules of the road for businesses of all sizes and clear rights and protections for consumers - whose data and consent are after all integral to digital innovation. While it is vital that the current harms consumers are exposed to online are addressed swiftly, government should not be blind to the harms coming down the road. Government should ensure that rather than deregulating protections around data, the regulations and legislation are clear on preventing new harms from becoming entrenched, for example in relation to automated decisions made by the use of machine learning algorithms and AI.

If the future of digital innovation and growth is to thrive and flourish it is absolutely vital that these aspirations are married with good, clear, agile and ethical regulation and rights which protect consumers as well as enabling business.

Questions

1. Do you agree we have identified the three most impactful strategic objectives and relevant outcomes to deliver our vision? Are there any other outcomes we should consider?

Objective 1. Drive growth, promote competition and innovate across the digital sector
Which? welcomes the intention of government to promote competition and develop innovation across the digital sector.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

With regard to competition, we welcome the creation of the Digital Markets Unit (DMU) and believe that reform of the competition regime is needed to tackle the substantial and entrenched market power of a small number of the largest firms. This will help to build a fairer and more competitive tech sector that will work better for consumers by giving them more control and more choice. Consumers should have choice, in the products and services they can access and consume, and with regards to how data about them will be collected, shared, accessed, used and retained.

The intention to put the DMU on a legislative footing is also welcome. The DMU must be given the necessary tools, including robust oversight and tough enforcement powers to punish companies that act anti-competitively. It will be critical that staff have the right expertise and technical skills and that access to the right evidence, intelligence and data will be made available to the Unit to enable them to do their job properly. We are aware that recently agreed trade deals limit the mandatory disclosure of source code, software and algorithms expressed in that software, and this is a point of concern for us. Measures designed to protect IP and drive competition can pose problems in terms of transparency and accountability of technical systems increasingly being used in decision-making systems that affect the lives of consumers. It is essential that regulators are able to access source code or algorithms in order to scrutinise businesses practices and protect consumers.

Objective 2. Ensure growth and innovation does not harm citizens or businesses, we will keep the UK safe and secure online

Which? supports these intentions. While growth and innovation are critical, neither have to be at the expense of an individual or a group's safety or security, including of their data.

The following elements of digital regulation are areas Which? has been actively involved in to ensure the protection of UK consumers.

Security of devices

We welcome the acknowledgment in the policy paper that "security needs to be embedded into innovation and planning" so that consumer products and services are safe, reliable, cyber secure and have the highest protections for consumers data.

Innovation in consumer products in the digital space - such as connected products, internet of things, mobile phone applications, and products and services which collect data in order to make decisions, develop algorithms, serve the consumer with choices or recommendations, or enable the consumer to connect, communicate and live online - are based on the consumer contributing data, often in order for the product/service to function. Protection of data, through good security of devices and good solid data protection is therefore essential, not just a nice to have.

Internet-connected products have the potential to bring huge benefits to consumers' lives. However, our testing continuously exposes popular connected devices with serious security flaws, many of which are currently on the market, that put consumers at risk from cybercrime. We know that consumers want secure devices, but all too often they are making purchases without fully understanding what exactly they are buying. This is particularly true of smart devices bought from

some online marketplaces. Insecure devices connected to a home environment can bring a wide range of security and privacy risks, both to the individual consumer and to our wider networked society. For innovation like smart devices to flourish, it is vital to ensure security is at the core of

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

design and that mandatory requirements are introduced and enforced to keep people safe from harms caused by the weak security of these products. This would also help increase trust and engagement, particularly with older consumers.

Which? therefore shares the government's ambition to make the UK one of the safest places in the world for consumers to be online and to use smart technologies. To do that however requires government ensuring that regulation enables enforcement and effective redress when consumers purchase devices that fail security standards which leave them open to data breaches and scams. It is also critical to ensure regulation is able to adapt and be kept up-to-date as the technology and consumers' use of technology evolves.

We therefore look forward to the soon to be published Product Security and Telecommunications Infrastructure (PSTI) Bill and hope that the Bill will include; taking action on products sold via online marketplaces, ensuring effective consumer redress mechanisms are in place, and clear guidance on transparency of software update information given at the point of sale to improve product longevity. Overall we hope that this is the start of ensuring that the design and build of connected products have security by design as integral and fundamental requirements.

Online product safety

The safety of products sold online continues to be a high priority for Which? We have recently submitted a response to UK Product Safety Review: Call for Evidence led by the Office for Product Safety and Security (OPSS)[1] that noted that Which? tests and investigations as well as tests and investigations carried out by European consumer groups and authorities[2] have found large numbers of unsafe products available for sale through online marketplaces, including products that are subject to warnings or recall notices. These products have included children's toys and car seats, smoke alarms, USB chargers and power banks. In addition, when platforms are notified about an unsafe product it can take an unacceptable length of time for the product to be removed from the site and the same products often reappear with slightly different descriptions or sold by a different third party seller.

Our recommendations are set out in detail in our policy paper "Online marketplaces and product safety"[3], but the key actions that we think are needed are:

- The general safety requirement that applies to economic operators, including producers, importers and distributors (including retailers), in the General Product Safety Regulations 2005 (GPSR) and sector-specific product safety legislation should also apply to online marketplaces along with a defence if they exercised all due diligence. As part of this, online marketplaces should enhance their checks before including sellers on their sites, so that evidence of compliance with safety requirements is a condition of their listing as well as ensuring that products and their manufacturer are clearly identifiable. Responsibilities should also be applied to fulfillment service providers.
- The actions that are required by online marketplaces when unsafe products are identified should be clarified. Online marketplaces should be required to respond within 24 hours and remove unsafe products once they are identified. They should also be required to inform consumers of safety issues and any action needed, to ensure that their suppliers carry out recalls effectively and to prevent recalled products from being listed again.

[1] OPSS Product Safety Review: Call for evidence. Which? Response, Which?, 2021
[2] Online product safety – trends and challenges, OECD digital economy papers no. 261, OECD, 2016
[3] Online marketplaces and product safety. Which? 2019

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

- UK law should place a requirement on online marketplaces to make it clear to consumers whether they are buying from a trader, a consumer, or directly from the company that owns the marketplace and clearly and accessibly explain the rights that apply.

Encryption Whilst complex and challenging, encryption is also a critical element of any digital economy, building security and trust for consumers, business and national security.

Which? has raised caution in our submission to the Computer Misuse Act against the weakening or undermining of encryption. Which? believes that encryption of consumer data should always remain protected. Every effort to break or weaken encryption undermines consumer protections of data, and so poses a risk to the integrity of their engagement with vital digital products and services. The notion that encryption is an inhibitor rather than a protector must not be encouraged to seep into the thinking of companies and organisations in their own security setup. The potential for harm through insecure systems, the ability for unsuspected, unwanted or unintended prying eyes to gain access to systems, or the simple reduction in control an organisation has to ensure their systems are 'safe and sound'; or held to account if they are not, will be a greater risk to consumers and indeed wider national security long term. That data protection law encourages security as well as 'privacy by design' would be detrimentally undermined if businesses and the wider public learn to see encryption as an inhibitor.

We have also emphasised in our response[4] to the Data Saves Lives strategy from NHSX that secure, reliable and consistent technology will be critical in relation to healthcare and the use of technology - including consumer products such as wearables, apps, connected IoT devices and products using AI and machine learning algorithms. Encryption of data in movement and at rest will be vital to engender consumer trust.

Consumers are protected from fraud and scams online. Fake and fraudulent digital content that facilitates fraud and scams is prolific online. Whilst we welcomed confirmation from the Government that the draft Online Safety Bill will include measures to tackle fraud, it is not currently clear on the face of the draft Bill exactly how fraud will be tackled. Given the scale and severity of the harm, Which? wants to see fraud designated as priority illegal content. Failure to do this will mean fewer requirements on platforms to put in place the measures required to protect against the risk of consumers being exposed, and falling victim to, a criminal posing as a legitimate business.

We are also seriously concerned by the exclusion of paid-for advertising from the draft Bill. Paid-for advertising on online platforms is a primary method used by criminals to target consumers and engage them in a scam[5], as it gives them instant access to large numbers of target audiences. Prominent types of scams enabled by paid for adverts include investment scams, pension scams and purchase scams.

We are engaging with the DCMS Online Advertising Programme team on their work in this space, but we fear that the exclusion of paid-for adverts in the draft Bill is a huge missed opportunity and will continue to leave consumers exposed to these serious and life changing criminal offences for far longer than is necessary. It is for that reason that we are actively calling for paid-for advertising to be in scope of the legislation.

[4] Which? submission to Data Saves Lives consultation July 2021
[5] Investment scammers run riot on search engines, while victims pay the price' - Which?

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? wants to see the creation and implementation of measures that stop illegal content from appearing on online platforms in the first place, and enable content to be blocked from being reuploaded. The emphasis here must be on a proactive approach of identifying, blocking and preventing the misuse of online platforms by the networks of criminal and 'bad actors', rather than a solely reactive approach of identifying and removing illegal content which has already been posted and therefore already exposed consumers to potential harm.

Whilst the temptation may be to try and determine ways of analysing the content for signs of fraudulent behaviour linguistic forensics are still in their infancy in this space and are unreliable. Technical measures exist which can detect illegal content online such as behavioural analytics, Open-Source Intelligence (OSINT) and hash sharing databases. Such an approach can be used to identify network criminal behaviour. Furthermore platforms need to take a stronger approach to verification of businesses advertisers before paid-for content is posted is needed, permitting content to 'go live' before checks have been undertaken and verification is confirmed, simply leaves consumers at risk of being exposed to content that could harm them. By undertaking advertiser verification, online platforms can ensure anyone paying for adverts is legitimate and seeks to engage with consumers in a good faith, this would act as a protection mechanism and would reduce the fake and fraudulent content appearing on platforms.

At present, based on the current drafting of the Bill, Which? is not confident that consumers will be adequately protected online. Which? is actively engaged in the progress of the draft Bill and has submitted a response to the Joint Scrutiny Committee's call for evidence detailing these concerns.[6]

Consumers are protected from fake reviews

Consumers use reviews to inform their buying decisions for both goods and services, on and offline. Customer reviews have never been more important following the growth in online shopping triggered by the pandemic. A recent Which? survey found that 89% of respondents said they use online customer reviews to inform product purchases or choice of services. However we know that fake and misleading reviews on some of the biggest online platforms are undermining consumers' trust and exposing them to harm. The same survey exposed low levels of trust from consumers that platforms such as Amazon and Facebook are taking effective steps to protect them.

We welcome the proposals in the government's consultation on Reforming Competition and Consumer Policy[7] to address the issue of fake reviews. Over recent years, Which? investigations and research have identified fake review practices across many of the largest online platforms, and across multiple sectors. The manipulation of reviews misleads consumers and undermines legitimate businesses that are unable to signal the true value of their products or services. We therefore support

the proposal that commissioning and incentivising any person to write and/or submit a fake consumer review of goods or services should be added to the list of automatically unfair practices in Schedule 1 of the Consumer Protection Regulations and businesses should take steps to ensure the reviews that are hosted or referenced on their sites are genuine.

Ensuring fake reviews are tackled is urgent if consumer trust in digital life is to not be diminished further. We will continue to call on the relevant government departments to work collaboratively to increase the legal responsibilities on platforms in tackling this issue.

---

[6] Which? submission to the Joint Scrutiny on the draft Online Safety Bill September 2021
[7] Reforming Competition and Consumer Policy, BEIS

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Objective 3. To protect our fundamental rights and freedoms, we will shape a digital economy that promotes a flourishing, democratic society.

The ability for consumers to live rich and meaningful digital lives enhanced by innovation, relevant and strong competition law, product security and meaningful data protection laws and rights is absolutely vital to a flourishing and democratic society. We note reference here to "fundamental rights" this must include the qualified right of Article 8 of the Human Rights Act - the right to respect of private and family life.

Which? believes that our existing data protection laws should be built upon and adapted rather than dismantled. We need to ensure the law and people's data rights are fit for purpose and provide the necessary protection over how data about us is collected, stored, shared, used, analysed (including by automated decision making).

Good innovation comes from being responsible, ethical and considering the impact on the user - both good and bad - and ensuring that meaningful and transparent rights and protections are built into law. It is critical that innovators consider the consumer throughout the R&D phase. Consumers are contributors of much of the data that enables innovation. It is vitally important therefore that absolute consideration is given to how consumers' data will be used, for what purpose and why and what clear data protections and rights will be embedded.

We note the emphasis across government about the importance of putting people in control of their data and we welcome the inspiration and aspiration of this. Putting people in control also means giving them the right to say no, to delete data, to challenge decisions made about them including by automated means and having transparency and clear understanding of what the data will be used for when, why and by whom. We believe that there is still some way for the government to go to achieve these aims even in existing data related programmes, projects and schemes.

The failure by NHSX and the Department for Health and Social Care to undertake widespread, easy to access, easy to understand, clear and honest communications about the detail of the GPDPR scheme and to provide a clear and easy way for people to opt out if they chose is a critical example. The approach taken led to mistrust, a proliferation and subsequent reliance on misinformation online and over 3 million people opting out. Our own survey[8] revealed that 20 million people hadn't heard of the scheme.

Our concerns of the lack of easily accessible and transparent communication about this scheme appear to have been shared, and we note that there is review of the scheme and tests the scheme needs to fulfill before going live.

We believe that access to data can provide great benefits to society as a whole, but people need to be brought along and feel buy-in to the scheme. That comes from engagement and explanation and discussion about the risks as well as the benefits. We note the emphasis from government to talk up the benefits of data - this is clear in the National Data Strategy. We don't disagree, data can bring huge benefits to individuals, families, groups, society as a whole, but pretending that harms do not exist or should not be discussed or tackled is disingenuous. We are concerned that when consumers

[8] 'NHS health data sharing: what you need to know about your medical data and GPDPR' - Which?

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

do raise concerns or worries or questions about projects, programmes, products, schemes or plans for the collection, use, sharing, retention of personal, special category or behavioural data they are seen to be overcautious, obstructive or simply ignorant to how technology works or how data is used. This is not universally the case, consumers regularly demonstrate understanding of the use of data. Just as people manage their physical lives based on choices that are nuanced and contextual, they manage their digital lives similarly. Our willingness to share data for one purpose doesn't necessarily translate to another purpose. If people choose to not share data for one purpose it is not necessarily going to be the case across the board, nor should it inhibit innovation, rather it is an opportunity to encourage innovation to understand that people make decisions that change over time - sometimes a matter of minutes - but that choice and control is not negative.

Regulation, engagement, control and honest transparent conversation are not inhibitive to innovation, rather they help to build an ethical and engaged approach which is more likely to bring people along as it enables people to be part of the journey and therefore be part of a flourishing and democratic society.

2. Do you have views on the three guiding principles for better digital regulation to deliver our vision and objectives?

Principle 1 and 2: Actively promote innovation and achieve forward looking and coherent outcomes

We note the positive intentions towards innovation, and we welcome the acknowledgment in the UK Innovation Strategy that "to be a global hub for innovation means having companies of all sizes creating breakthrough new products"[9] and the intention of the Strategy to want to "create the conditions for all businesses to innovate". This approach combined with a pro-competition approach we hope will help to stimulate and create a vibrant market of choice for the consumer that enables smaller companies to provide alternatives from the services offered to the consumer from the Big Tech companies.

Furthermore we hope this will enable services and products to be developed that do not solely rely on consumers being asked to contribute vast quantities of personal and personal behavioural data in order for a product or service to work, nor rely on giving the consumer the choice to either pay financially for a service or pay with "their data".

The development of innovation that puts the consumer in active control, enables only necessary data collection or contribution, with clear opt in choices and transparency, and clarity over what data will be used for, by whom, for how long and with what meaningful benefits for the consumer, would be a welcome extension of products and services in the consumer market.

With that in mind, Which? is concerned that the approach to ethical innovation and growth is being overlooked and that the government's current emphasis is that growth and innovation can only come from more relaxed regulation which will benefit business but undermine the consumer.

The reference in the policy paper to "deregulation", the removal of "unnecessary regulations and burdens where possible" and "trade-offs between different objectives...reducing confusion and red tape for businesses" appears to be a driving factor. We raise concern that moves to deregulate and

[9] UK Innovation Strategy

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

to deviate away from the precautionary principle approach to regulation runs the risk of embedding further the approach taken by big tech to date - namely voluntary approaches to mend the gaps created by the "move fast and break things approach" - that have led us to the current situation we find ourselves in. The concern that requiring innovators to "demonstrate no possible harm from an innovation" is too cautious and could impinge or prevent the benefits from being explored or developed is one that does not need to be dismantled entirely, indeed the concept of being proportionate is not inconsistent with the concept of being precautionary.
While we don't disagree that being precautionary can prevent people and organisations from taking a leap, and that the use of voluntary standards can be useful, we do not agree that regulation stifles innovation. Good regulation that creates clear rules of the road, on points such as trust, ethics, evidence and problem solving can be enormously beneficial, particularly in the digital and technology space and can lead to exciting innovation developed around appropriate "guardrails".

To date, the lack of regulation of digital markets has led to a wide range of harms to consumers and to society; lack of competition in some markets the breakdown of societal norms in relation to misinformation and disinformation, a thriving epidemic of online fraud and scams, the sale of unsafe and insecure products, fake reviews, bullying, abuse, data misuse, discrimination and challenges to people's autonomy. These harms are well acknowledged by government particularly in the draft Online Safety Bill and by the regulators, for example in the workplan[10] published by the Digital Regulation Co-operation Forum (DRCF). Developing more light touch regulation would therefore appear to directly contradict the urgent and longstanding moves by government to regulate the platforms in order to protect us from online harms and ensure that the UK is the safest place in the world to be online.

Creating clear and comprehensive digital regulation in the UK would enable and establish all innovation players, big or small, an opportunity to play on a level playing field and work within the appropriate, necessary and proportionate "guardrails" or rules of the road. Furthermore rather than being reactive to problems, the UK would proactively be preventing problems from becoming unmanageable, unsolvable and in some cases endemic.

Furthermore, whilst some of the big techs have brought us vast opportunities, the approach taken by them is not the only way to innovate. Innovation can be looked at in two ways. One: the development of products that align with existing trends and therefore existing harms and weaknesses. Or two: the opportunity for investment, support and enthusiasm for innovations that challenge the big players, challenge the status quo, or seek to improve our digital lives. Innovation that approaches the existing problems and existing markets from another angle, for example by adhering to and working to embed principles of fairness by design, privacy by design and security of design has the potential to be completely world leading.

Such an approach would enable better choice for consumers, would create a dynamic marketplace and thriving digital economy. Data would not be walled off as it currently is by the world's largest tech companies, there would be greater equity of data across all size businesses, opportunities for smart data projects could thrive, and the principles of open data could be developed to enable data to be better used for improvements to society and societal decision making.

Being "pro-innovation by default" as indicated in the policy paper must be developed with users in mind. If innovation continues to depend on treating users not as the consumers of a product or service, but as contributors who can be harvested or mined for their data in order that business can

[10] Digital Regulation Cooperation Forum: Plan of work 2021 to 2022

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

make money, then many of the harms we are having to deal with now will not only continue but will become more entrenched.

By taking this golden opportunity to lead the way in developing innovation that can work for all within an ethical trust framework, the UK could really be world leading.

Principle 3: exploit opportunity and address challenges in the international arena

In light of the government's stated principle to 'exploit opportunities and address challenges in the international arena' it is necessary to consider the potential impact of the international arena on consumer protections.

We are pleased that the UK obtained an adequacy decision from the EU and that the UK GDPR remains an integral part of the UK's data protection framework, however we are of course aware of the publication of the 'Data: A new direction' consultation on the 10th September 2021 and the government's proposals for wide ranging changes to the UK's data protection regime. We will be reading the proposals closely and will respond with a submission in due course. Under the current data protection regime UK consumers have become accustomed to an internationally recognised high standard of protection and a certain relationship with their data - how they access it, how organisations interact with it, limits placed on the use of it, and pathways to redress.

The success of the UK's digital trade policy is heavily dependent on the impact it has on consumers, alongside businesses, which is discussed in further detail in our digital trade report[11]. Which?'s research has shown that consumers find the protection of their interests in trade negotiations of high importance[12], however, many consumers have limited understanding of the intricacies of the risks and opportunities, and therefore look to the government to safeguard their interests, particularly when it comes to digital trade. As digital trade is underpinned by data flows, data protection is a critical issue for consumers when it comes to international trade.

In our written and oral evidence to Parliament we stressed that strong data protection must be maintained both domestically and internationally when UK consumers' data flows abroad[13]. Which? is concerned that negotiations with potential trade partners have the potential to undermine the UK's ability to regulate consumers' privacy and data protection in the future[14]. Provisions that create the potential for trade partners to legally challenge domestic regulation of privacy or data protection as barriers to trade should be avoided. The government should uphold the current high standards of data protection in force in the UK and ensure that negotiations with potential trade partners who have lower protections do not undermine the UK's ability to regulate or upgrade consumers' privacy and data protections in the future.

Which? wants to be assured that trade rules on cross border data transfers facilitate free flows of data whilst ensuring the highest level of data protection and privacy for consumers by retaining full autonomy and the exclusive right to regulate in the field of personal data protection. The UK-Japan CEPA has already signalled a departure from this approach, with provisions that set a new precedent of general binding commitments not to prohibit or restrict cross-border transfers of data, with privacy as a mere public policy exception that can be legally challenged. It also encourages mechanisms that promote compatibility between different data protection frameworks and the recognition of voluntary

[11] Digital Trade: Opportunities and Risks in Future Trade Deals, Which? 2020
[12] National Trade Conversation, Which? 2021
[13] International Trade Committee Report on Digital Trade and Data
[14] Digital Trade: Opportunities and Risks in Future Trade Deals, Which? 2020

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

undertakings, a form of self regulation - this is of particular concern. As Japan also has an adequacy decision from the EU, that was carried forward by the UK, this does not pose an immediate threat to the handling of UK consumers' data. However, creating precedent for self-regulation in trade partner countries to be recognised on equal footing to the comprehensive data protection regime that currently exists in the UK could be detrimental for consumers if this precedent is followed in future agreements with trade partners with less stringent data protection frameworks.
Which? believes that references to data protection without specific detail made in trade agreements could be detrimental to UK consumers if the language introduces flexibility into the well regulated UK system by promoting interoperability or compatibility between the Data Protection Act 2018 (DPA 2018) and weaker international rules for data transfers. Which? believes that trade deals should not limit the UK's ability to regulate to protect consumers from online harms, such as unsafe products, scams and fake reviews. In particular, the UK Government must stand firm against external negotiating objectives of limiting the UK's ability to extend legal liability of online platforms, including online marketplaces.

3. What other practical steps can we take to improve coherence and coordination across the digital regulatory landscape? What else could meet these aims other than the recommendations of the Digital Regulation Cooperation Forum?

We welcome the creation of the Digital Regulation Cooperation Forum. We believe that collaboration of this kind enables regulators to share knowledge and expertise, permits staff with specialist skills to be seconded in order to train other staff and learn from them and helps to foster improvements to the sharing of data, intelligence and information.

As noted, we also welcome the creation of the DMU, the intention of government to put the DMU on a legislative footing and the development of ways for the DMU to collaborate with other regulators when undertaking investigations.

With online platforms and big tech companies offering products and services that are so multifaceted it is logical and indeed necessary for the regulators to collaborate and bring their specialist skills and knowledge together rather than working in isolation. This is particularly vital when it comes to undertaking investigations regarding anti-competitive behaviour, data collection, use and breach and the cross cutting nature of online harms/safety.

However, with any form of collaboration between different bodies, it is vital that clear parameters are defined in order that each regulatory body understands their role in an investigation or in a collaboratory/cooperative environment.

We are of course conscious that there are a number of other regulators that may also need to contribute or be asked to engage as innovation in the digital space develops, for example:

- the Office for Product Safety and Standards may be have views on security, product safety, standards etc
- the Medicines and Health Products Regulation Authority (MHRA) may be required to contribute in terms of development of connected products and services in the health and medicine space - particularly if the use of machine learning, algorithms and AI become as integral as is anticipated and indeed hoped for
- engagement and collaboration with the Advertising Standards Authority (ASA) with regards to online harms and the future of advertising online.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Getting the balance right will be critical, as there is always the risk of too many cooks, but we are encouraged by the voluntary approach the regulators are currently taking and will follow the workplan of the DRCF with interest.

Of course, the success of the regulatory bodies also rests on them having the correct, and necessary support. We welcome the statement in the policy paper that government "will continue to make sure our regulators can adapt and have the right capabilities and expertise to take action effectively and proportionately."

With this in mind Which? hopes this will include:

- staff with the right technical, ethical, data, digital, security and legal skills
- regulators having the necessary tools, such as the ability to deliver robust oversight, auditing where relevant and needed, and tough enforcement powers to ensure the regulations are adhered to and when not that organisations and companies are appropriately sanctioned
- the ability for regulators to be able to access all the necessary evidence, intelligence and data including from companies that sit outside of the UK but are used by UK consumers. Ensuring there are no restrictions on access to such data and evidence will be a critical element of UK trade deals
- the ability for UK regulators to work and collaborate with their international counterparts to ensure cross border issues are tackled appropriately.

4. What challenges have you experienced in the current approach to digital regulation?

While we welcome the vast array of work government has recently undertaken in relation to digital regulation, we are concerned that the speed with which we are moving has enabled the wide range of problems and harms to become so embedded in society and in consumers' lives that we are in a cycle of catch-up and reaction to the actions of the largest tech companies.

We hope therefore that the current wave of draft regulation, consultations and strategies move quickly enough that legislation can be approved and the UK can begin to establish the meaningful "guardrails" so desperately needed.

We stress this for example in relation to the draft Online Safety Bill and the intention as already noted to leave paid for advertising out of scope of the legislation, whilst deferring it to the DCMS Online Advertising Programme which has only just begun its investigation. We are concerned that by kicking the can of regulation down the road, government is failing to adequately protect consumers. The Government has sought to give online platforms an inordinate amount of time to embed voluntary measures - which to date have failed to be sufficient in tackling the harms - before imposing regulation onto them. Whilst this may keep relations with business happy, the impact on consumers continues to be profound with huge financial loss and physical and emotional stress caused by falling victim to scams generated by fake and fraudulent content online. s.

Speed therefore is one element, but so is comprehension of the problems. Investment in training existing staff and hiring the right staff with the correct skills, knowledge and training in these complex digital, data, technology areas is critical. A generalist approach can be useful, but approaching these problems with a diverse mix of people on a team, combining humanities as well as STEM skills can bring meaningful context and nuance to identifying the wide range of technical problems and societal harms. This approach would ensure that all aspects of legal, ethical, technical, philosophical and creative considerations are given to proposed solutions.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

As noted earlier, we also would encourage the government to invest in engagement with people, to hear what they know and don't know, how they engage as consumers with technology, what their concerns are, what they see as benefit or risk or harm around data and their digital lives is worrying. And then to actually tackle the risks or harms they identify rather than dismiss them as negative or based on misunderstanding.

The policy paper makes reference to citizens being empowered - citizens can be empowered to use digital services but it is not in their gift as consumers to protect themselves from the multifaceted harms they face online, be it fraud, data loss, weak security, data use for reasons that they don't consent to, challenges to their autonomy from companies making decisions for them, bias in built in algorithms, data misuse and an overwhelming lack of control. By only singing the benefits, the government is persistently failing to acknowledge consumers' concerns and real world experiences of harms be they financial, psychological or physical.

No longer are people blind or ignorant to the role data plays in their lives, if anything the pandemic has increased people's awareness of data. By being honest, engaged and transparent with people and listening to their concerns a two way conversation can be established which will enable better engagement - and potentially greater buy-in in the long run.

5. How can government better utilise expertise from industry and civil society to design and implement pro-innovation regulation for digital technologies?

We believe that the government should engage with a wider range of stakeholders than just the big tech firms to ensure a broad range of voices are heard when it comes to innovation and regulation. While big tech firms have absolutely been innovators to get to where they are in terms of their global success, the very nature of innovation dictates that new ideas are less likely to come from the incumbents, and much more likely to come from outside the existing ecosystem. Well established theory of innovation[15] dictates that disruptive innovation comes from outside; from smaller players. As such, it is essential that government works with startups and scaleups to understand the sorts of approaches that are being tried and tested, the sorts of products that consumers are going to be using in the near future.

In order for disruptive innovation to occur, there must be a pro-growth regime that enables smaller businesses to flourish, an environment that allows smaller players to enter digital markets in the first place.

We hear the argument that regulation stifles innovation coming from big tech, yet without regulation to properly ensure fair competition in digital markets, big tech is simply able to stifle innovation itself by ensuring there can be no new entrants to a market. In this conversation, big tech firms paint the picture of themselves as the innovators. We would question whether they are still innovators or whether they simply use an argument about innovation to stop others from challenging their position.

We are keen to see true innovation in digital markets, but urge the government to be clear about what it means by innovation - and we urge the government to challenge big tech's role as an innovator, if it accepts that innovation usually comes from new players in a market.

As we have stated, engagement with consumers is vital in order to understand the challenges that consumers genuinely face. Understanding consumer challenges, real world consumer problems, and

[15] What Is Disruptive Innovation? Harvard Business Review

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

often challenges with how they interact online, can be solved by innovation. But problems are more likely to be solved by fresh new approaches, and less likely to be solved by the incumbents that have created many of the challenges in the first place.

Engagement with civil society organisations such as Which? can help bridge the gap between consumers and innovators and is therefore invaluable to the design and development of both products and services and also regulation. Qualitative research can be used to explore how consumers think and feel about innovation; it is always thought provoking. We believe that engagement with consumers is critical as consumers are key data contributors - without them many products and services simply wouldn't exist. The key will be to ensure that even if consumer responses are challenging, they are taken on board.

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

For further information, please contact Renate Samson, Principal Policy Adviser, Which? via email at renate.samson@which.co.uk