Digital Services Act package: open public Consultation

Google's submission

Keeping users safe online, deepening the Internal Market, and clarifying responsibilities for digital services

Table of contents

SECTION I: Overview 2

Part I. How to Effectively Keep Users Safe Online 2

Part II. Reviewing the Liability Regime of Digital Services Acting as Intermediaries 4

Part III. What Issues Derive from the Gatekeeper Power of Digital Platforms? 9

Part IV. Other Emerging Issues and Opportunities, Including Online Advertising 38

SECTION II: Questionnaire 53

Part I. How to Effectively Keep Users Safe Online 53

Part II. Reviewing the Liability Regime of Digital Services Acting as Intermediaries 89

Part III. What Issues Derive from the Gatekeeper Power of Digital Platforms? 93

Part IV. Other Emerging Issues and Opportunities, Including Online Advertising 117

Part VI. What Governance for Reinforcing the Single Market for Digital Services? 124

SECTION I: Overview

Google welcomes the opportunity to submit feedback to the European Commission's open public consultation on the Digital Services Act (DSA) package. Digital services connect individuals and communities around the world. They can inspire the best of society by democratising access to knowledge, powering business, and providing new opportunities for art and creativity. In Europe, digital services will play a central role in driving a faster, fairer, and greener recovery from the COVID-19 pandemic.

Our mission at Google is to organise the world's information and make it universally accessible and useful. Information quality and content moderation are integral to this mission. These issues are uniquely challenging, but we recognise this is a critical part of our responsibility to our users and partners. We want to contribute to a more responsible, more innovative, and more helpful internet.

The products we have built have been a force for creativity, learning, and access to information. Our products have expanded economic opportunity, allowing small businesses to market and sell their goods across borders. Products like Google Search have helped educate billions of people around the world, by opening up their access to information from across the web. YouTube serves as both an entertainment destination and a video library for the world. Google Play allows users to enjoy millions of the latest Android apps, games, music, movies, TV, books, magazines, and more. Google Cloud helps businesses modernise their workloads on world-class infrastructure, with multi-layered security and intelligent analytics. And Google Ads makes it easy for businesses to show the world what makes them unique, allowing them to reach customers searching for what they offer.

Our products support jobs, growth, and responsible innovation in Europe. According to research by Public First, Google's products supported €177 billion in economic activity for businesses, developers, creators, and publishers across Europe last year; and Google's core services of Search, Maps, and YouTube create €420 billion in value for European consumers. The revenue generated from Google Search and Ads, by connecting customers with businesses and driving revenue to content creators, supports the equivalent of 2.3 million jobs across the continent. In addition, Google's products help EU users navigate the immense amount of new information on the internet. Businesses in Europe estimated that online search was the most important way of customers finding them, ahead of word of mouth. Every month 71% of European YouTube consumers use the product to learn something, from new skills to new perspectives. As a result of the training we provided through Grow with Google, over 594,000 European businesses (mostly SMEs) have taken on more staff or seen revenue growth, and over 978,000 have grown careers or found jobs.

Part I. How to Effectively Keep Users Safe Online

We take our responsibility to our users extremely seriously. We continue to invest in tools, processes, and teams that help us elevate trustworthy information and moderate content across our services. In our submission, we detail the policies, systems, technology, and resources we bring to bear to tackle challenges related to illegal content and content that violates our Terms of

Service. We include information our many transparency reports and provide additional data on content removal requests and our removal actions, including:

- Our transparency report on requests to remove content. We receive content removal requests through a variety of avenues and from all levels of government— court orders, written requests from national and local government agencies, and requests from law enforcement professionals.
- A report on actions related to European privacy law. In a May 2014 ruling, the Court of Justice of the European Union found that individuals have the right to ask search engines like Google to delist certain results about them. This report provides data on the volume of requests, the URLs delisted, the individuals submitting requests, and the content of websites and URLs identified in requests. Google has delisted over 1.5 million URLs, and the report breaks down the percentage of URLs evaluated for delisting by the category of site identified in the request (e.g., news, social media).
- Information on counterfeits. We shut down approximately 12,000 Google Ads accounts containing 10 million ads for attempting to advertise counterfeit goods in 2019. Google takes strong action against any promotion of counterfeiting on our ads platforms, and we devote significant engineering and machine learning-based tools to prevent abuse that violates our policies, including counterfeiting. Over 99% of the Google Ads accounts we terminated under our counterfeit policies were done proactively using these tools.
- Content delistings due to copyright. Google regularly receives requests to delist content from Search results that may infringe on copyright. This report provides data on the close to 4.7 billion URLs requested to be delisted from Search from over 2.9 million unique top-level domains, by 213,483 unique copyright owners and 207,281 unique reporting organisations.
- Our annual Bad Ads Report. We blocked more than 35 million phishing ads and 19 million "trick-to-click" ads in 2019. Overall that year, we blocked and removed 2.7 billion bad ads— more than 5,000 bad ads per minute.
- Removals under our Terms of Service. In 2019, more than 30 million videos were removed from YouTube for violating our Community Guidelines. Google Play stopped over 790,000 policy-violating apps before they were ever published to the Play store. Google Maps detected and removed more than 75 million policy-violating reviews and 4 million fake business profiles, and took down more than 580,000 reviews and 258,000 business listings that were directly reported to us for violating our policies.

Jump to the questionnaire responses for this section

Part II. Reviewing the Liability Regime of Digital Services Acting as Intermediaries

The current legal framework has supported innovation from companies throughout Europe, and allowed users throughout the EU to benefit from those services. We acknowledge that regulatory changes may be needed in light of the digital transformation of the last two decades. But in doing so, we must be careful to not unravel the benefits that the current framework has delivered.

We have shared principles that have informed our practices and that we believe would make for an effective regulatory framework, and we submitted to the Commission's Inception Impact Assessment on the Digital Services Act: Deepening the Internal Market and clarifying responsibilities for digital services. This submission contains additional considerations for the Commission's evidence gathering exercise. As the Commission reviews the liability regime of digital services acting as intermediaries, we want to highlight the following points.

Cornerstone principles of the Single Market: The DSA should retain core principles such as the country-of-origin principle, the guarantee of the freedom of establishment and of the freedom to provide digital services cross-border in the Union, and respect for fundamental rights. These core principles have enabled the growth of the digital economy in Europe, expanded access to information, broken down social barriers, and created new opportunities for European citizens to learn, grow, and prosper for the past twenty years. The country-of-origin principle is a cornerstone of other important regulations for the sector, including the Audiovisual Media Services (AVMS) Directive and the General Data Protection Regulation (GDPR). It ensures the Single Market continues to support a variety of online services and business models, and enables businesses to provide services across borders without confronting internal barriers.

Updating the liability regime: The DSA should clarify the legal framework for digital services to reflect the nature of today's services. In doing so, the liability regime should continue to acknowledge the relevant differences between services, using a harmonised, graduated, and conditional exemption scheme. Such an approach can provide businesses with legal clarity while ensuring an effective response to illegal content. The DSA should further clarify that services are not liable without actual knowledge, which is critical to ensuring that businesses have the legal certainty needed to scale up and grow across the European Union. We believe that, to be truly effective, the regulatory regime must protect against illegal content migrating across platforms by ensuring a consistent set of rules for all market players.

In our submission, we propose one way to update the harmonised, graduated, and conditional exemption scheme. We propose the current three-level system of mere conduit, caching, and hosting services be clarified and expanded to explicitly include other services.

- **Digital infrastructure services:** It should be clarified that Article 12's "mere conduit" category encompasses services such as domain name services, in addition to services consisting of the transmission in a network of information provided by a user of the service, or the provision of access to a network. Such services would still be required to

meet equivalent conditions to the existing Article 12 to benefit from the liability exemptions.

- **Search engines:** As correctly noted by Advocate General Maduro (in C-236/08 to C-238/08), the nature of a search engine service is such that it most logically falls under the e-Commerce Directive's Article 13 for caching services. Similar to search engines, which are indexes of the web at large, caching services are defined as those consisting of the automatic and intermediate storage of information hosted by a third party, where the information stored is updated to reflect updates to the information hosted by the third party. The services are performed to make the onward transmission of that information to users of the service more efficient upon request. The Digital Services Act should codify this understanding, and make clear that caching services, including search engine services, should fall under a liability regime equivalent to the existing Article 13, without prejudice to recent EU legislative developments such as the General Data Protection Regulation.
- **Cloud providers:** We believe cloud providers, including software as a service ("SaaS") providers, should fall into a separate category of service. Cloud providers are limited in what they can do to address illegal content stored at the direction of their customers or their customers' users, given the technical architecture of their services, privacy protections, and the contractual obligations they hold towards their customers' data. Factually and contractually, such providers do not have the requisite authority and control over content such that they should have responsibility for removing specific content from a third party's service. Therefore, where a third party digital service provider uses a cloud provider, that third party should remain responsible for compliance with the law. Equally, where a third party business uses a SaaS provider and has authority and control over content, that third party should remain responsible for compliance with the law regarding that content.
- **Platform services:** We recommend moving away from the distinction in some case law between "active" and "passive" hosts, which has created significant uncertainty and liability risk for common features of current services. It should be clear that hosting services can continue to benefit from a limitation of liability by retaining the requirement in Article 14 of the e-Commerce Directive for services to act expeditiously, upon obtaining actual knowledge or awareness of illegal activities, to remove or to disable access to the information concerned. To the extent some hosts are expected to go beyond notice and takedown of specifically identified illegal material, we believe any requirement be limited to best efforts for identical copies of content that was previously notified in an adequately substantiated manner. We would remain concerned about the risks to fundamental rights where companies are forced to prioritise speed of removal over careful decision-making and where staydown obligations are proposed.

A liability regime for illegal content: The liability regime should continue to be based around clearly-defined illegal content, and should be careful not to blur the important distinction between illegal and lawful-but-harmful content. As the Center for Democracy & Technology has noted, "it is inconsistent with [human rights and rule-of-law] principles for governments to leverage private companies to limit speech that authorities cannot directly restrict." Where Member States believe a category of content is sufficiently harmful, their governments may make that content illegal directly, through democratic processes, in a clear and proportionate manner, rather than through back-door regulation of amorphously-defined harms. The European Court of Human Rights has confirmed that freedom of expression includes

the right to “offend, shock or disturb.” Finally, the changing nature of and norms around harmful content make it unsuitable for the liability regime. That said, the focus on illegal content and activity in the new framework need not preclude further evaluation and action on “lawful but harmful” content through self- and co-regulatory initiatives, such as the EU Code of Practice on Disinformation.

Strengthening notice formalities: Notice formalities would help review teams process information more efficiently and responsibly, as well as protect against abuse by fraudulent or bad-faith actors. This is especially important given that the boundaries of illegal content can vary significantly across EU Member States, and content permitted in one Member State may not be permissible in another. Formal notice should include, at minimum, requirements to: clearly identify the content at issue by URL, video timestamp, or other unique identifier in a tangible and usable format; state the law and basis of the legal claim; clearly identify the sender of notice where the nature of the rights asserted requires identification of the rightsholder; and attest to the good faith and validity of the claim. Policymakers should consider penalties to deter bad actors from submitting fraudulent or false claims, a known problem that could significantly slow review of notice.

Maintaining prohibitions on mandating general monitoring and use of automated tools: The DSA should also ensure that fundamental rights are respected by maintaining the prohibition on general monitoring obligations. As noted by the Court of Justice of the European Union (CJEU) and human rights organizations, general monitoring would undermine free expression, the freedoms to receive and impart information, and the freedom to conduct a business. While breakthroughs in machine learning and other technology are impressive, the technology is far from perfect, and less accurate on more nuanced or context-dependent content. Their mandated use would be inappropriate, and could lead to restrictions on lawful content and on citizens’ fundamental rights. Finally, it is critical to maintain a prohibition on general monitoring obligations in order to not create inconsistency and compliance issues with other key EU legislation such as the Art. 17 of the Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market.

Safeguards for careful review: The DSA can help prevent risks to fundamental rights by ensuring that companies are not forced to prioritise speed of removal over careful decision-making. We encounter many grey-area cases that require appropriate time to evaluate the law and context, and we remain concerned about recent laws that enable imposition of large penalties if short, fixed turn-around times are not met. As the Commission has previously noted, such requirements could lead to “excessive content deletions.” The French Constitutional Council recently ruled that this combination, as included in France's Act to Combat Hateful Content on the Internet, "undermines freedom of expression and communication in a way that is not necessary, adapted, and proportionate." Any new standard should safeguard fundamental rights by ensuring an appropriate balance between speed and accuracy of removal.

Incentivising services to take more action on illegal content: Policymakers can encourage intermediaries to engage in the responsible use of voluntary actions for content moderation, *above and beyond what is required by the liability regime*. Currently, an intermediary that engages in voluntary moderation risks being labelled as an “active” service provider, or otherwise being deemed to have knowledge of all of the content on its platform.

This current risk of liability creates a perverse incentive for intermediaries to either refrain from engaging in reasonable proactive moderation, or to over-remove content in the course of moderating. An intermediary should be able to manually review content voluntarily in respect of one type of unlawfulness (e.g., illegal terrorist content) without being deemed to have knowledge of all of the other potential ways in which that same content might be unlawful (e.g., defamation). In our submission, we propose language to that effect.

Transparency measures: We stress the need for transparency reporting obligations to be reasonable, proportionate, and based on clear metrics. We recognise the Commission's concerns and the importance of improving accountability and user trust, and have a long track record of providing information to users on our services, including our content moderation policies. It will be important to take into account the risks that information can be used by bad actors to game systems, that commercially sensitive information is exposed, or that user privacy is affected. We also highlight our recent announcement of a new **advertiser identity verification initiative**, which will require advertisers to complete a verification program in order to buy ads on our network and give users more information about the ads they see online.

Maintaining safeguards for disclosure of user data to law enforcement: We would remain concerned with proposals that would circumvent existing legal protections or require internet service providers to disclose user data to the government without any prior oversight by an independent authority and without proper safeguards. We appreciate that law enforcement agencies have legitimate interests in obtaining digital evidence to protect public safety. That's why we support initiatives that make this process simpler but which maintain procedural safeguards. The European Commission's proposal for an Electronic Evidence ("e-Evidence") Regulation, if passed, would enable government authorities to obtain digital evidence from service providers, streamlining and harmonising the process without sacrificing privacy safeguards.

Oversight: Governance should support the digital Single Market and the country-of-origin principle. We note that the trend towards Member States imposing varying obligations around notifying, detecting, and removing content has caused fragmentation in the Single Market. A framework that would allow firms to comply with one set of processes for undertaking and reporting on these activities would reduce regulatory complexity, strengthening the Single Market for digital services and helping users understand the rules, roles and responsibilities in the regulatory scheme. The DSA should simplify the regime around the country-of-origin principle and increase cooperation between national regulators.

- **Cooperation between regulators.** We identify how cooperation that promotes consistency supports growth and innovation by providing legal certainty to platforms and users. We also suggest that cooperation should be structured around clear purposes, and those purposes should reflect the specific needs of the regulatory frameworks for the intermediation of third party content, services, and goods.
- **Objectives of regulatory oversight.** We outline our view that the functions of regulatory bodies should be centered around: systemic efforts to protect users from illegal content; growth, providing legal certainty across the ecosystem; and innovation, supporting user choice and accommodating new technologies. We suggest that these objectives should be provided for in the regulatory framework, and that the regulatory toolkit should have a systemic focus, with transparency at the center.

- **Towards generally accepted standards.** We also suggest that the Commission may wish to explore mechanisms to support the development of generally accepted international standards for compliance frameworks related to illegal content. Today, online platforms successfully leverage an array of compliance frameworks for security, privacy, and finance, amongst others. Many of these compliance frameworks are rooted in international standards, established best practice, and sector-specific guidelines. On this basis, we propose that the DSA could include mechanisms that support the development within the EU of international standards for compliance frameworks related to addressing illegal content.

Jump to the questionnaire responses for this section

Part III. What Issues Derive from the Gatekeeper Power of Digital Platforms?

This section of our accompanying document provides further details on our responses to Section III of the Commission's questionnaire on the Digital Service Act package. Our responses in the questionnaire cross-refer to sections of this document.

1. Introduction

An updated regulatory framework can provide greater clarity on the rights and responsibilities of digital platforms and to do this in ways that benefit European consumers and businesses. This has the potential to give consumers greater confidence that their interests are being protected as they shop, search, and socialize online and to encourage business customers to make more use of intermediary platforms to the benefit of the European platform economy. We are an advocate of acting openly and promoting consumer choice — this is a long-standing Google commitment. Free, open choice goes hand-in-hand with flexible, choice-enhancing regulation as reflected in the observations we make in our responses to the consultation questions and this supplemental submission.

Any framework should ensure that consumers, suppliers and businesses all continue to benefit from useful products that allow them to save time and get things done when they are online. A blanket approach to ex ante competition regulation could have unintended consequences on user experience as well as multiplying costs for European businesses. That's why we recommend first - fully and on the facts - assessing the effectiveness of regulation that is already in place to ensure that markets are working properly. Where the evidence shows meaningful gaps, the next step ought to be to consider how one can modernise those existing rules and procedures to address the underlying concerns before turning to consideration of new and distinct regulatory frameworks. In any event, we believe regulatory reform of any kind should aim to be flexible and future-proof to adapt to technological change and accommodate the diverse European tech ecosystem.

In particular:

The process of designating firms as "gatekeepers" should be based on clear definitions and supported by evidence; it should not discriminate against particular business models or technologies.

- **Determining which platforms qualify as "gatekeeper" is a complex exercise that requires further analysis.** It will need to ensure that *ex ante* regulation applies only to markets where large online platforms have the requisite degree of market power. Digital platforms often operate using different business and monetization strategies, across

multiple markets, geographies, and sectors, with varying degrees of competitive strength in each.[1] Regulators should not favor or discriminate against any business, business model, or technology from the outset. In certain sectors, the platform may have market power; in others, it may be a new entrant or marginal player. The digital ecosystem is extremely diverse and evolving rapidly and it would be misguided for gatekeeper designations to be evaluated by reference to the position of an entire company or corporate group.

- When assessing the factors to determine whether an online platform should be designated as a gatekeeper, **it is important that the Commission provides clear and future-proof definitions of the criteria and how they should be applied**. An overly simplistic assessment (eg, number of users) would not necessarily reflect whether a specific platform has power over consumers and other firms at a particular moment in time.

The design of any *ex ante* regulatory framework should focus on promoting innovation and ensuring regulation that remains fit for purpose as technologies and markets evolve

- *Ex ante* regulation ought to promote competition and innovation from all digital platforms and should promote platforms' entry or expansion into new markets. **Any new rules ought to enhance competition and consumer welfare and will require regular reviews and updates to ensure that regulation keeps pace with market developments.** To that end, any new regulation should be based on a set of high-level principles that could be applied across different types of platforms (*e.g.*, a measure to address actual or perceived conflicts of interest where a platform owner competes on the platform), complemented by platform-specific guidance that depends on the technologies at issue (*e.g.*, what this means in the context of ad tech services as compared to what this means in the context of an app store or marketplace).

- **Possible *ex ante* rules should preserve incentives to innovate and invest.** The Platform economy contributes substantially to investments and innovation that supports consumer welfare and competition. Any orders or interventions should be considered pragmatically and informed by evidence of actual harm. Further-reaching orders (*e.g.*, powers to suspend or reverse product changes) would be invasive and require safeguards, including rights of defence and appeal. A pragmatic approach to

[1] There are also platforms that focus exclusively (or almost exclusively) on a particular sector, but which nonetheless occupy powerful market positions in their area of focus — such as TV and movie streaming (Netflix) and music streaming services (Spotify) — or in a particular geography (*e.g.*, Zalando's position in fashion in Germany).

implementing *ex ante* regulation could involve a sequencing of new measures to test how markets respond.[2]

- ***Ex ante* rules should allow concerns to be resolved quickly and consensually.** In particular, to ensure effective administration of these rules, the Commission could deploy a combination of reputational sanctions and referrals of unresolved matters for resolution under the established antitrust regime, including any new competition tools (see further our responses to questions on the NCT).

The *ex ante* regulatory framework should take proper account of existing measures, initiatives and competition tools; any gaps should be evidenced before moving to consideration of potential solutions.

- For harms that can arise regardless of an online platform's size or market position, **some rules may need to apply on a sector-wide basis** (*e.g.*, greater transparency over fees, ensuring consistent privacy standards, enabling data portability, approaches to default settings, and unfair sales methods). Many such rules have been introduced for example through the Platform-to-Business Regulation and have yet to take full effect. We have a long-standing commitment to providing an open, transparent relationship with those who use our services, and to leading data portability initiatives like the Data Transfer Project.

- It will be important that any proposed *ex ante* rules for platforms should be considered alongside other initiatives that the Commission has proposed, including the creation of a new competition tool (**NCT**) and revisions to the Market Definition Notice.

This submission builds on our response to the Initial Impact Assessment. Section 2 considers questions on how 'gatekeepers' should be defined; Section 3 engages with the 'emerging issues' section of the Questionnaire (in particular the questions open to 'all respondents'); and Section 4 includes our reactions to the Questionnaire's final section concerning 'regulation of large online platform companies acting as gatekeepers'.

We would welcome the opportunity to discuss these matters with the Commission and other relevant stakeholders further.

2. Questions 1–4: Main features of gatekeeper online platform companies and main relevant criteria for assessing their economic power

Questions 1–4 seek to determine how gatekeepers should be identified. The Questionnaire presents a list of market and platform characteristics — such as geographic coverage, network effects, and barriers to entry — and asks whether they are relevant, separately or in

[2] The purpose of *ex ante* regulation is arguably to create conditions in which markets can be effectively competitive without the need for such regulation. Any framework for the *ex ante* regulation of online platforms should, we think, incorporate regular reviews of whether *ex ante* regulation remains necessary in a given market or whether effective competition has already been restored.

combination, to identifying gatekeepers. The Questionnaire also asks whether the integration of certain activities — such as online search, advertising intermediation, and cloud services — within a single company could strengthen its gatekeeper role.

I. Gatekeeper designations should be business model agnostic

We believe that if gatekeeper designations applied, they should do so in a way that minimizes the potential harms from asymmetric regulation (*i.e.*, the risk of distorting competition and exposing consumers to harm from players falling in and out of scope of new rules based on arbitrary and/or outdated designations). In particular, the criteria for identifying 'gatekeeper power' should be independent of the particular business model that a platform uses, making no distinction as between platforms that operate business models based on advertising, subscriptions, sales commissions, or sales of hardware.[3]

Gatekeeper designations appear to focus on consideration of three factors: market power, gateway functionality, and dependency.[4]

- **Market power.** Recent competition enforcement demonstrates the range of platforms that have been found to have market power (*e.g.*, Microsoft, Google, Facebook, Amazon, and Apple) and other platforms may be found to have market power in the future (borne out, for example, by the UK CMA's investigation into online auction platform services). The gatekeeper assessment should therefore recognize that a range of platforms — operating a range of different business models (*e.g.*, ad-funded, subscription-based, commission-based, hardware sales) — may hold 'market power' in different circumstances and *vis-à-vis* different platform participants.

- **Gateway functionality.** Platforms operating a range of different business models might be said to act as gateways for businesses to reach consumers.[5] Developers and consumers connect through app stores. Large smartphone manufacturers determine how users engage with particular apps or services. Software developers and desktop or laptop manufacturers operate through desktop OSs. And merchants find buyers through e-commerce sites. In each of these sectors there may be firms that hold a strategic or

[3] Imposing a heavier regulatory burden on some businesses (*e.g.*, ads funded services) than others (*e.g.*, fee-based licensing or selling high-priced smartphones) could distort competition among platforms that pursue different business models, reduce choice, increase costs, and ultimately harm consumer welfare.

[4] *See e.g.*, CMA, Final Report, Online platforms and digital advertising, 1 July 2020 (the **CMA FInal Report**), para. 7.55 (noting that SMS "*is described as a position of enduring market power or control over a strategic gateway market with the consequence that the platform enjoys a powerful negotiating position resulting in a position of business dependency*").

[5] Inception Impact Assessment, p.2 ("*Large online platforms are able to control increasingly important platform ecosystems in the digital economy. Typically, they feature an ability to connect many businesses with many consumers through their services*").

gateway position at a particular moment in time (*e.g.*, during the COVID-19 pandemic). Other sectors may also be characterized by gateway platforms. For example, vertical search services — not only general search services — can act as important gateways (online travel agencies are likely to be significant sources of business for airline and hotel bookings).

- **Economic dependence.** The Commission's Inception Impact Assessment describes a situation where "*traditional businesses are increasingly dependent on a limited number of large online platforms*."[6] The gatekeeper assessment should take into account that all platforms through which a materially significant proportion of business (e.g. in the form of highly valuable traffic) is channeled ought to be treated as satisfying this criterion.

If gatekeeper designations are based on such factors, the Commission would need to ensure that there is clear guidance for firms, and consistent application of these factors across varying contexts and business models.

II. Gatekeeper assessments should be reviewed periodically

Gatekeeper assessments should be reviewed periodically. Digital markets are fast-moving, and companies with seemingly formidable competitive advantages can lose competitive strength quickly. Similarly, small companies can rapidly achieve a prominent position displacing incumbents (e.g., despite only being released globally in 2018, TikTok is now one of the most downloaded apps of the last decade and ranked in sixth place in the global mobile app rankings by monthly active users for 2019). To remain relevant and effective, regulation has to keep pace with the market changes, otherwise inefficiencies can arise. For example, the hard-copy Yellow Pages publication used to be considered a powerful market player and was subject to fee caps and restrictions on publishing new products. But these interventions were only revoked in 2013, long after the print version of Yellow Pages had lost its former competitive significance and had been largely displaced by online directories.

To ensure that the application of *ex ante* rules continues to reflect competitive realities, any *ex ante* regulatory framework should specify time periods after which the relevant body should review gatekeeper designations and add or remove such designations as appropriate. This is consistent with the Commission's practice of including clauses in commitments decisions that allow for a review of obligations where there has been a material change in circumstances.[7]

III. Gatekeeper designations should apply to identified activities in specific markets

Gatekeeper designations should apply to identified business activities in specific markets within a corporate group. Large digital platforms tend to operate across multiple markets and sectors, with varying degrees of competitive strength in each. In certain sectors, the platform may have

---

6 Inception Impact Assessment, p.2.

7 *See e.g.*, Case COMP/AT.40153 *E-Book MFNs and related matters*, Commission decision of 4 May 2017, Clause 5 of the Final Commitments.

market power; in others, it may be a new entrant or marginal player (and may even struggle to compete and subsequently leave the market). Conversely, companies with a smaller market capitalization may nonetheless hold market power in particular markets where they operate. Accordingly, gatekeeper designations ought to be evaluated by reference to specific business activities in specific markets; not by reference to the position of the entire company or corporate group.

The provisions of any new *ex ante* regulation ought, therefore, only to apply to firms in markets where they are found to have 'gatekeeper' power.[8] Applying *ex ante* rules outside these markets would create a risk of deterring pro-competitive market entry through excessive regulation, thereby depriving SMEs and consumers of attractive new products.

IV. Some rules ought to apply on a sector-wide basis

Perceived concerns about digital services — such as those relating to privacy, transparency, and ranking decisions — may apply regardless of the size of the service provider or its business model. For example, the Guardian Media Group brought a high-profile claim against the Rubicon Project in respect of alleged hidden fees. And several of the possible *ex ante* rules appear to us designed to address consumer harms independent of the gatekeeper/non-gatekeeper status of a platform. If that is the case, the benefits to platform users would be maximized by ensuring a consistent application across all players in the sector.[9]

We think *ex ante* rules addressing the following kinds of issues are potential candidates for a more expansive application given the types of issues they seek to address and the potential benefits.

- **Data portability.** Data portability regimes most effectively facilitate user switching, multi-homing, and innovation when the maximum number of platforms take part. Rules on data portability or mobility should therefore apply on an industry-wide basis. For example, participation in data mobility systems, such as the Data Transfer Project,[10] could be mandated for some use cases that have been demonstrated to materially encourage entry and expansion.

- **Fee transparency.** Customers have an interest in fee transparency, regardless of the size or market position of the particular platform. There is no compelling reason why

---

8 *See e.g.*, G. Federico, F. Scott Morton, and C. Shapiro, Antitrust and Innovation: Welcoming and Protecting Disruption in Innovation Policy and the Economy (Eds. J. Lerner and S. Shern, University of Chicago Press), December 2019, p.127 ("*the same firm can be a market leader in one area and a disruptive upstart in another*").

9 As a general matter, regulations governing the digital sector are consistently applied on a sector-wide basis (*e.g.*, the General Data Protection Regulation (**GDPR**) and the Platform To Business Regulation).

10 The Data Transfer Project is an open-source collaboration supported by organizations (Apple, Deezer, Facebook, Google, Mastodon, Microsoft, Solid, and Twitter) committed to building a common framework with open-source code that can connect any two online service providers, enabling a seamless, direct, user initiated portability of data between the two platforms.

some platforms should be afforded discretion to maintain opaque fee structures whereas others should be subject to transparency requirements. As the Rubicon Project example above shows, this risks leading to uneven protection for consumers and businesses, creating uncertainty and eroding trust in digital services.

- **Data privacy.** The GDPR is not limited to 'gatekeeper' firms; it is an industry-wide regulation and any enhancements or supplements to the GDPR that are included in *ex ante* rules ought to apply equally to non-gatekeeper firms.

- **Choice of services.** Users of any platform — large or small — may have an interest in being presented with a choice of frequently used services, particularly if there is otherwise a risk of their being defaulted to sub-optimal services. These issues can arise on a range of different platforms — mobile, desktop, web-based services, and more. And it may distort competition if some platforms are permitted to 'nudge' consumers towards a particular service, but others are not.

In determining which rules should be applied to which platforms, the Commission should take account of the risk that applying regulations to only certain firms in a given sector could: (i) raise the costs — and limit the activities — of those companies relative to their rivals, thereby distorting competition; (ii) expose customers of out-of-scope companies to harm; (iii) create a regulatory framework that is complex to administer; and (iv) reduce companies' incentives to grow beyond a certain size. Certain studies have identified instances where inconsistent regulation has left gaps in consumer protection and less competition.[11]

3. Emerging Issues[12]

- **Questions 9 and 11: Specific issues and unfair practices**

---

[11] For example, the CMA published a policy paper in 2015 on creating 'An effective regulatory framework for higher education.' This paper identified significant concerns arising from applying regulations to certain higher education institutions but not others. In particular, it found that gaps and discrepancies in the scope of regulatory oversight could (i) distort competition between higher education providers and (ii) lead to worse outcomes for students (*i.e.*, consumers). The CMA's paper stated that: "*[The] regulatory gap creates a risk that poor quality provision by providers that are not subject to direct QAA scrutiny will not be noticed and addressed promptly, thereby causing detriment to students and the reputation of the sector. Such uneven application of the quality assurance regime also risks distorting providers' incentives to provide quality.*" (pp. 22–23 and 27). *See also* a 2006 note by the European Commission's former Chief Economist. It relates to the approaches that regulators have taken to regulating mobile termination rates, noting that "*Despite all the flaws of asymmetric regulation, some countries are still regulating mobile termination charges on an asymmetric rather than symmetric basis*" (p. 11). The Note pointed out that requiring larger operators to reduce their charges, while allowing others to set higher charges, "*may be expected to harm the competitive process and reduce the incentives to efficiency*." In addition, this approach could create "*situations where the small firm will indeed prefer to stay small for a long time to keep the benefits arising from this inappropriate form of protection. In other words, the very same policy that arguably tried to make the small firm more aggressive, ends up achieving the opposite effect*" (p. 12).

[12] Google's response is limited to the questions in this section open to all respondents (*i.e.*, Question 9 onwards).

Questions 9 and 11 ask respondents to identify any "*specific issues and unfair practices*" they perceive with respect to online platforms, and what impact these issues or practices have on innovation, competition, and consumer choice.

The issues on which the Questionnaire appears to seek responses here have been substantially tackled in the Platform-to-Business Regulation (**P2B**) that entered into force in July 2020. The Commission should assess the impact of P2B on the digital ecosystem before proposing new laws that overlap with the objectives of the P2B (e.g. ranking transparency). Otherwise, any new regulations risk being either unnecessary or ineffective to meet the objectives pursued.

P2B addresses a number of concerns that SMEs have flagged as "problematic" over the last couple of years. P2B introduces a number of benefits for SMEs: no more sudden and unexplained account suspensions (platforms are obliged to give a 2-week notice, offer possibilities to appeal and reinstate business users if suspension was made in error). Also, platforms need to disclose the main parameters they use to rank goods and services on their site, to help sellers understand how to optimise their presence. Those requirements will be further specified by the EC guidelines on ranking transparency. Platforms' business users will be offered a variety of choices when problems arise including the use of complaint-handling mechanisms that platforms are now required to set up, mediation or collective actions. It is worth highlighting that P2B applies to all platforms irrespective of their size, which indicates that the issues addressed in the regulation can arise irrespective of the platform's size.

In any event, the existence and extent of anti-competitive effects or procompetitive benefits arising from conduct by digital platforms cannot be assessed in the abstract. Those effects or benefits turn on the practices at issue, as well as the market conditions and economic context, and should be assessed on a case-by-case basis. The Questionnaire refers to data-related issues and the Inception Impact Assessment refers to self-preferencing, which we address in response to subsequent questions.

As a general matter, we have demonstrated a long-standing commitment to providing an open, transparent relationship with those who use our services. For example:

- Transparency ensures that customers benefit from understanding the criteria against which their products, services, or sites will be evaluated and ranked. Similarly, consumers benefit in understanding the ranking of search results and the key factors that help determine which results are returned for their queries. Specifically, we publish and maintain detailed information about how Google Search works including information about how we improve search quality and our approach to algorithmic ranking, including publication of our Search Quality Rater Guidelines which define our goals for Search algorithms.

- Transparency helps customers adapt to material changes in ranking or other issues. For example, when we implemented our Speed Update, we provided webmasters with six months' notice of the change, giving them time to adapt. And we have provided at least six months' notice of the upcoming introduction of the 'page experience' signal, which will further enhance users' search experience.

- Transparency helps participants understand the rules and processes of auctions. We provide publishers and advertisers with explanations of all the key elements of the ad auction process and the main parameters that influence it, such as pricing and blocking rules, our relationship with publishers and exchanges, how Ad Manager determines the best yield, and how dynamic allocation works.

- Transparency helps address questions about the fees charged when advertisers use Google's ad intermediation services. That is why we recently published two blogs (here and here) showing that Ad Manager publishers keep over 69% of digital advertising revenues generated, and news publishers keep over 95% on average.

- Transparency ensures that consumers have access to clear information concerning which data are collected and how those data are used. We explain in our Privacy Policy what data we collect and why, we explain how data are used in ads, and we give consumers the option to opt out of personalized advertising altogether.

In considering what form any new *ex ante* regulation on transparency should take, three considerations should be taken into account.

First, transparency concerns are not necessarily limited — or related — to the size of the platform at issue. For example, the consequences of unfair or inconsistent ranking decisions may be acute for a business that depends on a niche vertical search service, such as hotels, airlines, or restaurants. Likewise, concerns have been raised about comparison shopping sites that fail to disclose whether ads on their sites are influenced by payments.[13] Therefore, it will be important not to limit unduly the range of platforms that may be subject to new *ex ante* rules on transparency.

Second, there are clear and well-established limits on how far certain types of transparency can go before they jeopardize the very services to which they relate. Regulators will need to strike a careful balance that ensures that ranking results are not easily manipulated by bad actors harming both legitimate businesses and consumers and is in line with existing legislative

[13] *See e.g.*, Comparison Tools, Report from the Multi-Stakeholder Dialogue, Report presented at the European Consumer Summit, 18–19 March 2013, p. 19 ("*It is essential that CTs clearly explain the nature of any affiliate links they have with vendors whose product or services appear on their websites, because such information may be important to consumer decision making*"); and Civic Consulting, Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods, 2015, p. 6 ("*Although PCWs therefore can help consumers find cheaper offers, the mystery shopping also revealed significant shortcomings in PCW practices, including a lack of adequate information on aspects like… a lack of information about payments from traders for ranking placements and listings*").

safeguards such as the Trade Secrets Directive. For example, while it may be helpful for a search service to provide guidance on the main parameters of a site that it takes into account in ranking, it would be prejudicial to the proper and safe operation of a search service to publish details of all the technical 'proxy signals' through which these parameters are assessed. Otherwise, websites could manipulate and improve their ranking in search results by optimizing for the relevant proxy signal; *not* by increasing the quality or relevance of their site to users.[14] This would have negative consequences for example for (a) consumers who will see more irrelevant or even harmful content and (b) genuine websites who play by the rules and will be pushed down in the search results to make room for websites that manipulate search signals.

And the specific details of how a search service ranks results represents a core value of its business. Disclosing these details would allow competitors to copy innovations and free ride on investments in developing proprietary search ranking technologies.[15] In other words, there is a balance to be struck between providing business users with information on how they may be affected by changes to rankings, and preserving the quality — and incentives to invest in — search services.

Third, regulation already exists concerning the appropriate degree of transparency. Specifically, the Platform-to-Business Regulation requires online platforms to identify the "*main parameters*" that search services consider when ranking websites (Article 5(2)). At the same time, the Regulation recognizes in Recital 27 that platforms require the "*ability to act against bad faith manipulation of ranking by third parties, including in the interest of consumers, should [...] not be impaired.*" New regulations should be careful not to upset the balance between transparency, quality, and incentives to invest that the Platform-to-Business Regulation strikes. As explained in the progress report of the Commission's Expert Group for the Observatory on the Online Platform Economy, the Regulation provides for increased fairness in a variety of ways including — but not limited to — algorithmic transparency.[16] The Regulation only entered into force in July

---

[14] A good example is the PageRank signal, which examines the number and quality of links that a website receives from other websites. A user does not as such notice the number of links that a website receives. However, if a website receives a lot of links from other websites, that may indicate that the website provides useful content for users. Google published the fact that it was using this signal as a proxy for relevance or quality. Because website operators know that Google considers the number of incoming links as a signal, some websites engage in practices to manipulate that signal, rather than genuinely improving their website. For example, they buy incoming links or engage in link exchange schemes so that they appear to Google's algorithms to be of greater quality than they really are. This serves to illustrate the importance of keeping proxy signals hidden.

[15] Therefore, when we implemented our Speed Update, we explained the potential consequences of the update to webmasters without revealing the specific changes we made to our algorithms.

[16] Expert Group for the Observatory on the Online Platform Economy, Progress Report on Differentiated Treatment, pp. 32–33 ("*The Platform-to-Business Regulation provides a good starting point in this regard by, amongst others: imposing a notice period of at least 15 days before platforms (referred to as 'providers of online intermediation services' in the Regulation) can implement changes to its terms and conditions; requiring platforms to provide a business user with a statement of reasons when restricting, suspending and terminating its service; requiring platforms to set out in their terms and conditions the main parameters determining ranking and the reasons for the relative importance of those main parameters as opposed to others, a description of any differentiated treatment platforms give and a description of the access of business users to data*"); and Progress Report on Data, p. 28 ("*with the entry into force of the*

2020. It would be prudent to wait to see its impact before considering any new rules on transparency.

- **Question 10: Use and sharing of data**

Question 10 asks respondents to identify "*what practices relating to the use and sharing of data in the platforms' environment are raising particular concerns*?"

There is a strong case for data use and sharing goals to be effectively and proportionately pursued through existing means and collaborative efforts. For example, digital platforms of all sizes could work with the Commission, Member States, and industry to identify specific use cases where data access or interoperability would promote innovation, and cooperate on ways to facilitate data sharing without jeopardizing privacy or incentives to invest. Google has adopted an approach that is open but respectful of users' rights by making large-scale search datasets publicly available for free (*e.g.*, through the Google Trends and Natural Questions tools, along with multiple other free and open source datasets). And Google has developed data mobility tools that enhance user choice without sacrificing innovation or variety. Specifically, Google has played a leading role in the Data Transfer Project, together with Facebook, Microsoft, Twitter, and various other digital service providers (including Apple, which joined the project on 30 July 2019) to develop a system of data mobility. We are open to exploring other options with stakeholders that would address concerns around data access in a collaborative, proportionate and flexible manner.

However, we would caution against far-reaching regulation. Careful definition of the scope and operation of any data access rule is critical to avoid damaging both privacy and innovation.

Any new data access rules should be clear in their objectives, and should take account of the varying significance of different types of data, both in terms of (i) enhancing the competitive abilities of data recipients, and (ii) any negative consequences of data access on competition and investment. Proposals to share user-level datasets comprising both click and query data score poorly on both fronts. The evidence shows that 'more data' does not lead to improvements in rival search engines' results. For example, the Microsoft/Yahoo! deal doubled Bing's query volume overnight but, according to observers of the industry, failed to improve the relevance or monetization of Bing's search results. In other words, having more data did not lead to an improvement in rivals' performance. Rather, improvements come from technical innovation and rigorous user experiments (in 2019 alone, Google ran over 464,065 experiments, resulting in more than 3,620 improvements to Google Search).

'Platform-to-business' regulation, and in particular the provisions of Article 9 on access to data, platforms will have to provide enhanced transparency on their practices with regards to the data they collect, data collected by their business users, as well as sharing practices with third parties").

The evidence also shows that sharing user-level click and query data would not enhance competition to find the best results; rather, click data would inform rivals as to how Google answers a particular query.[17] It would therefore enable rivals to systematically clone Google's search results, reducing product diversity and chilling incentives of Google and its rivals to invest in product improvements. This is borne out in the comments of one of Google's search rivals, Mojeek, to the CMA's Interim Report on online platforms and digital advertising, which stated that it would at the same time be unfair to force [search engines] to share their product and would not contribute to new innovation.[18] And as the CMA's Final Report observes, "*there is a risk, if such a remedy included a requirement to disclose the outputs of proprietary search algorithms, which are the result of investments in search and associated infrastructure, that this could dampen incentives for Google to innovate and improve its algorithm by enabling free riding*" (para. 8.40). Moreover, sharing such granular data could expose users to privacy violations, as borne out in both historical examples[19] and a paper in Nature by an author of the EC Special Advisers' Report on digital competition.

- **Question 12: Dependency of startups or scaleups on large online platforms**

Question 12 asks whether startups and scaleups depend on large online platforms to access or expand, the difficulties this creates, and how this has changed in the last five years.

Online platforms have supported the scaling up and expansion of startups and existing businesses. The Questionnaire acknowledges that "*[o]nline platforms facilitate cross-border trading within and outside the Union and open entirely new business opportunities to a variety of European businesses and traders by facilitating their expansion and access to new markets*". This makes it all the more important to ensure that any new *ex ante* regulation preserves platforms' ability and incentive to continue helping SMEs to flourish.

Online platforms have created unprecedented market entry and expansion opportunities for SMEs, lowering barriers to entry, expanding their reach and enabling them to scale beyond their home market. Oxera found that online platforms provide a number of significant benefits for

[17] This is not a mere hypothetical concern. Indeed, Bing has already engaged in this kind of behavior. Using query information that it was able to observe from users of Microsoft browsers who had issued queries to Google, Bing extracted information about Google's ranking and imported it into its search results.

[18] Mojeek commented that "*Despite disagreeing with some of their practices, the search giants have spent billions of dollars on building and maintaining their own search index, it could therefore be seen as unfair to force them to open up what is essentially their product and share it with others, or to offer search query and click data they have obtained by way of that product… If these steps are made in the name of positive competition, it will actually just result in multiple search engines all offering the same service but under different banners. And whilst it's important that metasearch engines like DuckDuckGo and Startpage exist to offer users better privacy than mainstream search engines, they are not offering any new innovation with regards to improving the core element of search… instead we call for more search engines with independent search indexes and algorithms.*"

[19] For example, in 2006 New York Times journalists were able to re-identify 'Searcher No. 4417749' from anonymized AOL search logs.

growing businesses including: market expansion, cost reduction, information expansion and price discrimination in targeting potential customers.[20]

Google services provide significant benefits to our business users. Last year, Google's products supported at least €177 billion a year in economic activity for businesses, developers, creators, and publishers across Europe. Google Maps provides free listings for businesses, who benefit from consumers' searching for local goods and services. Google Ad campaigns help businesses scale. In the first 30 days of its ad campaign in Google's Play Store, Nordeus generated 892% more installations of its football game. RunKeeper, a fitness tracking app, gained 85,000 users in one quarter and cut its cost-per-install to less than 25 cents by advertising across using Google's Universal App Campaign that distributed apps across multiple Google services. And YouTube enables small businesses to scale.

When Google offers a new product or service (i.e. when Google enters or expands in a new sector), it creates additional business opportunities for digital companies and businesses from traditional sectors alike. Google's 2015 entry into the market for photography apps on Android created additional user attention and demand for such apps generally. This had a positive spillover effect on complementors. Following Google's entry, complementors were more likely to innovate their photography apps and to release new apps in other categories, as well.[21]

Google's open-source mobile OS, Google Android, is a prime example of how online platforms can support market entry and expansion. Since its introduction just over a decade ago, Android has supported market entry and expansion and unleashed a wave of competition, innovation, and choice. It has enabled small-scale European OEMs such as Wiko and HMD to produce powerful smartphones, and the development of the Android app ecosystem has been publicly reported to support €11.7 billion in revenue for European developers and over 1.4 million jobs.

Google's services have helped SMEs to enter and expand rapidly in new markets by improving their ability to find and connect with potential new customers. At the same time, Google must compete intensely for SMEs' custom as businesses can work with a range of platforms and providers to find consumers, distribute their services, and advertise their products online, and can shift their business easily to the platform that offers them the greatest added value. Two examples bear mention:

- **Advertising.** In advertising, the rapid growth — and increasing sophistication — of inventory has led to falling costs and greater choice for SMEs wanting to make potentially interested consumers aware of their products or services. On average, for every euro businesses spend on Google Ads, they receive €8 back in profit[22] and the 'cost per click'

---

20 Oxera, Benefits of Online Platforms, 2015.

21 *See e.g.* J. Foerderer et al., Does Platform Owner's Entry Crowd Out Innovation? Evidence from Google Photos, 29 Info. Sys. Res. 444 (2018).

22 Public First, Google's Economic Impact in Europe, p.7.

that Google charges advertisers on its owned-and-operated properties has decreased by more than 20% in recent years (per Google's 2018 Form 10-K, p. 28). Additionally, YouTube provides a valuable source of online advertising for companies in the EU, in particular enabling SMEs to market their products across the EU at relatively low cost. There are ever expanding opportunities to advertise on non-Google surfaces. Just this year, for example, Spotify announced that it would begin working with user data to offer its own personalized ads service.

- **Cloud services.** The costs of storing data have declined in spectacular fashion over time. As the technology press has reported, in 1967 "*a 1-megabyte hard drive would have set you back by $1 million. Today, that same megabyte of capacity on a hard disk drive (HDD) costs about two cents.*" There is a clear trend of companies being able to store ever more data in ever smaller formats for ever lower prices. Thus, "*from 2000 through 2016, the price of hard drive storage has declined 28% per year, while prices of NAND flash memory have declined 48% per year.*" In fact, it is easier than ever before to enter data-intensive industries because new players can benefit from advances made by existing cloud services providers, and can rent data processing capacity on demand to fit their needs.

    - **Question 13: Societal and economic impacts of digital platforms**

Question 13 asks about the societal (*e.g.*, on freedom of expression, consumer protection, media plurality) and economic (*e.g.*, on market contestability, innovation) effects, if any, of the gatekeeper role that large online platform companies exercise over the whole platform ecosystem.

Public First prepared a report that provides quantitative estimates of the economic impact of Google in Europe. The following data points in particular underscore the economic boost that Google provides:

- Many of Google's consumer products are provided free of charge, which creates value for many of our consumers who would otherwise have to pay for such services. It was found that Google's core services of Search, Maps, and YouTube have a total consumer surplus of around €420 billion per year for European consumers.

- Last year, Google's products supported at least €177 billion a year in economic activity for businesses, developers, creators, and publishers across Europe.

- Google invests significant resources in the underlying infrastructure that powers the Internet in Europe. We have invested over €7 billion in constructing data centres across Europe – currently we have four data centres, in Finland, Belgium, the Netherlands and Ireland, supporting an average of 9,600 jobs per year. We continue to invest in and expand these centres and have plans to establish a fifth centre in the Netherlands.

- Enhanced productivity from Google Search and our tools such as Docs, Sheets and Slides helps save European workers over 2,800 million hours a year, while Google Cloud has increased business productivity in Europe by over €2.4 billion, supporting increased competitiveness of European companies on the global stage.

- Google is the world's largest business purchaser of renewable energy, and has enabled more than €1.2 billion in renewable energy investment across Europe. This investment allows our data centres in Europe to be environmentally sustainable as well as contributes to maintaining Google's status as carbon neutral since 2007.

Large digital platforms — including those described as 'gatekeepers' — make a significant contribution to economic growth in Europe and other regions. As explained in our response to the Inception Impact Assessment, Google, Apple, Facebook, and Amazon are reported to be some of the largest investors in R&D, which is reflected in the 2018 Global Innovation 1000 study. Google has consistently spent over 15% of its revenues on R&D since 2016, whereas the average 'R&D ratio' in the EU is 3.4%.

Digital technology has also been crucial in helping consumers, businesses, and governments manage the effects of the COVID-19 crisis. One example of this is the free contact-tracing technology jointly developed by Apple and Google to help sustain and manage outbreaks across member states, and support the easing of lockdowns necessary to restart the European economy. As of August 19, 15 European states had launched apps using this technology. Another example is that, from March to May 2020, more than 1 million businesses posted COVID-19 updates, with millions of clicks to retailers' websites each week. Moreover:[23]

- Google Search has displayed additional information on the local vertical search units that it displays on its general search results page to present COVID-19-specific information for shops (*e.g.*, in-store shopping or curbside pickup options), restaurants (*e.g.*, dine-in, takeout, or delivery options), delivery information (*e.g.*, no-contact delivery), and on temporary closures. And Google added features that let users purchase gift cards from — or donate to — their favorite local businesses.

- As businesses adjust to remote working, we are starting to see more interest in topics such as productivity, technology, and digital transformation on Google Search. Our newly launched Teach from Home hub provides information, training, and tools to help instructors keep teaching from home.

- On YouTube, Learn@Home gathers resources for families from YouTube's most popular learning channels, and our YouTube Learning hub centralizes high-quality educational content from across YouTube. And our Grow with Google program, focused on supporting SMEs, will continue to offer free online tools and learning resources for small and medium businesses.

[23] *See also* Sundar Pichai, Coronavirus: How we're helping, 6 March 2020.

These developments show that platforms create value for consumers and SMEs, and even support them in times of crisis, including by (i) providing information for consumers directly in knowledge panels (*i.e.*, information boxes that appear on Google when users search for entities (people, places, organizations, things)) and other formats, and (ii) integrating new services on which SMEs can build their businesses.[24] They also underscore the innovative capacity and pro-competitive effects of Google's — and other digital platforms' — being able to roll out product changes and improvements at speed. It is essential that new regulation does not jeopardize these types of actions, which benefit consumers and SMEs.[25]What is more, digital services will play a central role in driving a faster, fairer and greener recovery from the COVID-19 pandemic in Europe and promoting innovation will be particularly important as the European economy sets on a path of recovery in the wake of the pandemic.

- **Question 14: The impact of online platforms on the media sector**

Question 14 asks about issues specific to the media sector that need to be addressed in light of the gatekeeper role of large online platforms.

The media sector, and news publishers in particular, have seen their print circulation and revenues from print advertising fall over the course of several decades. While these difficulties are undeniable, they are linked to structural changes in the market that have emerged over time, including increased competition in the supply of ads; increased competition in the supply of news and editorial content; and the unbundling of news media and services such as classified listings.

These changes have happened in parallel with the emergence of online platforms. Online platforms create substantial value for press publishers while providing users with the information they are looking for.

Google displays news publishers' websites as part of its search results, thereby promoting publishers' content and referring substantial traffic to them in the form of billions of free clicks each year. These clicks lead to increased ad-based and subscription-based revenue that publishers generate on their sites. Based on estimates by Deloitte of the value of a click for publishers, this traffic is worth hundreds of millions of euros a year. By contrast, the ad revenue that Google generates from results pages that show results for press publishers represents a small fraction of that sum.

---

24 Google has developed a range of free tools to help small businesses adapt: *see* Google, Open for Business.

25 The economic shock of the COVID-19 pandemic may also provide possibilities to improve our understanding of conditions and market dynamics in technology sectors (*e.g.*, how customer dependency may vary across different types of platforms). There is a strong case for the Commission being required to report on a regular basis on developments in the markets that may have implications for competition.

This value exchange also creates benefits for users by displaying search results together with previews that make it easier for users to identify the most relevant results to their query. Google creates this value for free; neither users nor referenced websites pay Google for the display of search results.

Google is committed to supporting local news in strengthening and benefitting from their online presence. During the Covid-19 crisis, we provided support to smaller publications through our Journalist Emergency Relief Fund and by providing larger publishers using Google's Ad Manager with five months of fee relief. This builds on years of work to support quality journalism through our Digital Growth Program from the Google News Initiative (**GNI**), a free training program for small-to-medium sized news publishers, available first in Europe, before being rolled out in the rest of the world. The program provides intensive training and mentoring on the fundamentals of digital business strategy, audience engagement and revenue strategy.

We recognise our responsibility to work with the Commission, news publishers and other stakeholders in preserving media pluralism. Indeed we have a shared interest in doing so - users want to use Google to find a variety of news sites.[26] Digital advertising has increased in significance as a revenue source for many media publishers and we acknowledge the importance of providing publishers with transparency and the tools to play their essential role in communicating to the EU public.

Google is therefore investing in ways to support the news industry.[27] Ads-funded tools developed by Google have given smaller media players unique opportunities to monetise their inventory. On YouTube, we surface trusted news content from EU media organisations with a top news shelf on users' homepage. Since March, we have added a COVID-19 news shelf to surface COVID-19 news stories from authoritative publishers.[28] We previously launched the YouTube Player for Publishers, providing publishers with user analytics and monetisation options to help them maximise revenue on the platform.[29] During the COVID-19 pandemic, we have shared free tools and resources to support journalists' work, including live training workshops on YouTube.[30]

---

26 Although, as shown by the CMA Final Report, Table 5.7, news publishers are not dependent on Google for traffic as Google Search only accounts for approximately a quarter of their traffic.

27 The GNI is our global effort to help news organisations thrive in the digital age through various programs and partnerships. The GNI includes the Digital News Innovation Fund, which financially supports high-quality journalism in Europe. Other investments that benefit the news industry include Subscribe with Google, which helps publishers grow by making it easier for users to sign up for a news subscription. See *Google News Initiative*. Additionally, Google's wider business is beneficial for news publishers - Google's search tools allow users to find news publishers websites at no cost to the publisher (this is despite Google not earning significant advertising revenues from search queries for news — most news queries are not suitable for the display of ads and the majority of search engine results pages resulting from a news query do not show any ads at all).

28 See *Breaking news and top news on YouTube*.

29 See *Digital News Initiative: Introducing the YouTube Player for Publishers*.

30 See *Reporting in a crisis* and *GNI Live Trainings*.

We are committed to working with news publishers to provide them with maximum possible transparency and control over how they can produce, distribute and make money from content online. We would question whether an '*ex ante*' framework with a defined, delimited remit to address economic and competition inefficiencies is best placed to deal with the sensitive political and societal issues relating to the future of the media sector.

1. Regulation of large online platform companies acting as gatekeepers

- **Questions 1–6 and 16: Scope of regulatory rules dedicated to gatekeeper platforms**

Questions 1–6 inquire about the need for dedicated regulatory rules, whether they should include prohibitions of certain practices (and if so, what type), and whether they should impose obligations on gatekeeper platforms (and if so, what type).

Question 16 then asks whether the objective of such regulatory rules should be to tackle both negative societal and negative economic effects caused by gatekeepers.

The notion of an 'online platform' is not clear-cut. The technology used to deliver goods and services is increasingly 'digital', and the distinction between online and offline is becoming ever more blurred. For example, the automotive sector has seen the development of car-sharing (and ride-sharing) platforms, autonomous vehicles, and in-vehicle operating systems, which have challenged existing business models. And traditional offline advertising is increasingly adopting programmatic solutions to deliver ads (*e.g.*, Sky AdSmart).[31]

Gatekeeper designations appear to focus on consideration of three factors: market power, gateway functionality, and dependency. We believe further guidance could be helpful in providing a more rigorous understanding of these three criteria. In our answer to Q4, we provide further detail on our position on how these designations should be applied, namely that they should be business model agnostic, be periodically reviewed and updated, and should apply to identified activities in specific markets.

We believe that if these designations are applied to a specific set of firms, this should be done in a way that minimizes the potential harms from asymmetric regulation (*i.e.*, the risk of distorting competition and exposing consumers to harm from players falling in and out of scope of new rules based on arbitrary and/or outdated designations). In some cases, it may be more effective to apply certain rules regardless of a platform's 'gatekeeper' status to ensure consistent consumer protection.

[31] For further examples of offline advertising adopting programmatic solutions, see Analysys Mason, Convergence of TV and Digital Platforms, 21 December 2017, which highlights case studies from ProSieben and others.

As the Commission considers what activities should be covered by *ex ante* regulation, the following assessments should, we think, be relevant:

- **Identification of likely problems.** The starting point for the regime should be to identify which market features or characteristics are causing competition problems, including consumer harm, that may warrant additional rules or heightened scrutiny of particular players.

- **Identification of any harmful gaps in pre-existing law.** *Ex ante* regulation could be used as a way of addressing harmful gaps in the existing law that allow perceived problems to occur and prevent them from being addressed. These gaps could be substantive (*i.e.*, existing law does not address a particular practice) or procedural (*i.e.*, issues making existing law ineffective, slow, or unduly difficult to enforce). This stage of the assessment should also take account of whether existing law can address the identified problem without needing to be supplemented by further measures.

- **Weighing up the costs and benefits of additional intervention.** Any new measures ought to promote competition and innovation. Achieving this goal requires both the costs and benefits to be taken into account and weighed up. Accordingly, the *ex ante* regulatory regime should require the Commission to test in advance whether interventions are likely to enhance competition.[32]

- **Consideration for what type of intervention is proportionate to the perceived problem.** A range of possible tools can be used to address conduct that raises concerns, from formal sanctions to guidance. In fast-moving industries, where it takes time to understand the various costs and benefits of a practice — and where the consequences of product changes are uncertain — proportionality plays a particularly important role in deciding how best to resolve a perceived concern, while preserving innovation and competition. In some cases, it may be sufficient to issue guidance on the circumstances in which a practice will raise concerns, and work with industry groups to develop relevant standards.[33]

---

[32] The fact that regulation has benefits as well as costs is well understood. *See e.g.*, T. Philippon, The Great Reversal, 2019, p. 143 (Regarding the deregulation of the airline industry that allowed EasyJet to enter the French market in 2008, and the 'unbundling' deregulation of the French telecoms industry that allowed Free Mobile to acquire a 4G license in 2011: "*I have already described in this chapter a long list of deregulation efforts spurred by the European Commission. These efforts were – and still are – critical to the success of the Single Market*"); and CMA, Regulation and Competition, January 2020, pp. 3–4 ("*greater regulation is – on average – associated with less competition. For instance, countries with lower levels of product market regulation tend to have more competitive markets and enjoy higher rates of productivity and economic growth*").

[33] *See e.g.*, J. Tirole, Competition and the Industrial Challenge for the Digital Age, April 2020, p. 26 ("*Firms that are both a marketplace/technological platform and merchants supplying this marketplace/apps cannot treat equally a rival offering that is inferior to its own. But self-preferencing has the potential to be anticompetitive,*

We think that high-level objectives and principles are better suited to fast-changing digital services than prescriptive or rigid rules, which risk becoming obsolete quickly. These principles can set general — and broadly accepted — standards that players in digital markets (or, indeed, any market) should aim to achieve. For example, the principles of 'fair trading', 'open choices', and 'trust and transparency' are reasonable goals and are relevant to a wide range of gatekeeper and non-gatekeeper platforms. Supporting guidance will be needed to ensure that companies have certainty about what the *ex ante* regulatory regime requires and what steps they need to take in order to comply.

How those principles are interpreted and applied matters at least as much as the principles themselves. Accurately distinguishing pro-competitive innovation from anti-competitive conduct is important in order to preserve the benefits that digital platforms offer to consumers and business users. If *ex ante* regulation is to be used as a tool to facilitate consensus-building and to steer the design of new products and innovations, then firms will need clear and sufficiently detailed guidance on how the rules are to be interpreted.

For example, in considering how to apply a general principle of wanting to prevent improper self-preferencing in search a number of fact specific questions may be relevant. For example: (i) Does the design improve quality and benefit consumers (and has the platform carried out testing to prove that this is the case)?[34] (ii) Does the design increase the relevance of search results by providing more relevant information? (iii) Does the design benefit third parties? (iv) Does the design allow users to choose rival services (*e.g.*, through a choice carousel)? (v) What is the overall significance of the design on the abilities of firms to compete? To be effective and practicable, a general principle would need to provide specific guidance on these kinds of questions.

These types of questions are important to keep in mind when assessing claims by certain commentators that the Commission's *Shopping* decision provides a framework for generalized bans on unequal treatment or self-preferencing. In particular, some government reports as well as the European Commission's Inception Impact Assessment, propose introducing *per se* bans on digital platforms or companies that perform a 'regulatory function' from engaging in such conduct.[35] In contrast, competition authorities have resisted introducing a blanket ban on alleged

---

and economists should put more work on designing guidelines that would facilitate the authorities' dealing with such behaviors").

[34] Similar questions are discussed in G. Federico, F. Scott Morton, and C. Shapiro, Antitrust and Innovation: Welcoming and Protecting Disruption in Innovation Policy and the Economy (Eds. J. Lerner and S. Shern, University of Chicago Press), December 2019, p. 162 ("*Whether or not consumers are harmed depends on whether the platform owner's policies increase the overall value of the platform to users, the nature of competition among substitutes for the complement, and the ability to move away from the platform (which is a function of the degree of effective interplatform competition)*").

[35] Jacques Crémer, Yves-Alexandre de Montjoye, Heike Schweitzer, *Competition Policy for the Digital Era*, p. 66 (If "*the platform performs a regulatory function, it should bear the burden of proving that* self-preferencing *has no long-run exclusionary effects on product markets*"). The Furman report refers to prohibiting situations where a "*platform with strategic market status [is] giving undue preferential prominence on its webpages to its own integrated services*", Furman report, para. 2.47. The German ARC Amendments propose to introduce stricter rules for companies with cross-market importance, including a prohibition of self-preferencing and

self-preferencing, instead emphasizing the need for case-specific analyses — a view that Google shares. On the one hand, allegations of self-preferencing may require scrutiny to ensure that competition and consumers are not being harmed; on the other hand, a blanket approach could deny users the benefits of innovation and product improvements.[36]

In particular, a ban on self-preferencing would by its nature not be fact-specific, but would apply across a category of different firms, competing in different areas, and engaged in many different forms of conduct. This could have several inadvertent repercussions: hampering vertical integration, which is presumptively efficient; eliminating synergies; and leading to delayed or mothballed product improvements.[37] The risk and costs of false positives are therefore high.

In *Streetmap.EU*, for example, the High Court of England & Wales found Google's practice of showing a Google Maps thumbnail at the top of search results pages to be a "*pro-competitive*" and "*indisputable*" product improvement. Google's introduction of the thumbnail map was not likely to harm competition and the conduct was objectively justified. This was because showing rival maps would have had a "*serious impact on the quality*" of Google's results, including delays in returning results and inaccurate maps.

Likewise, around 2006, Google introduced a weather box on its pages to provide direct weather information in response to weather-related queries. Complainants argued that by showing specialized weather results in a box, Google engaged in search bias and harmed competition. In April 2013, the Hamburg Court rejected these complaints, holding that the Weather OneBox serves "*to increase the overall attractiveness of [Google's] search engine*". The Court stressed

---

leveraging power from one market to another without the German competition agency having to prove competitive harm. *See* the draft 10th amendment of the German Act Against Restraints of Competition, published 7 October 2019.

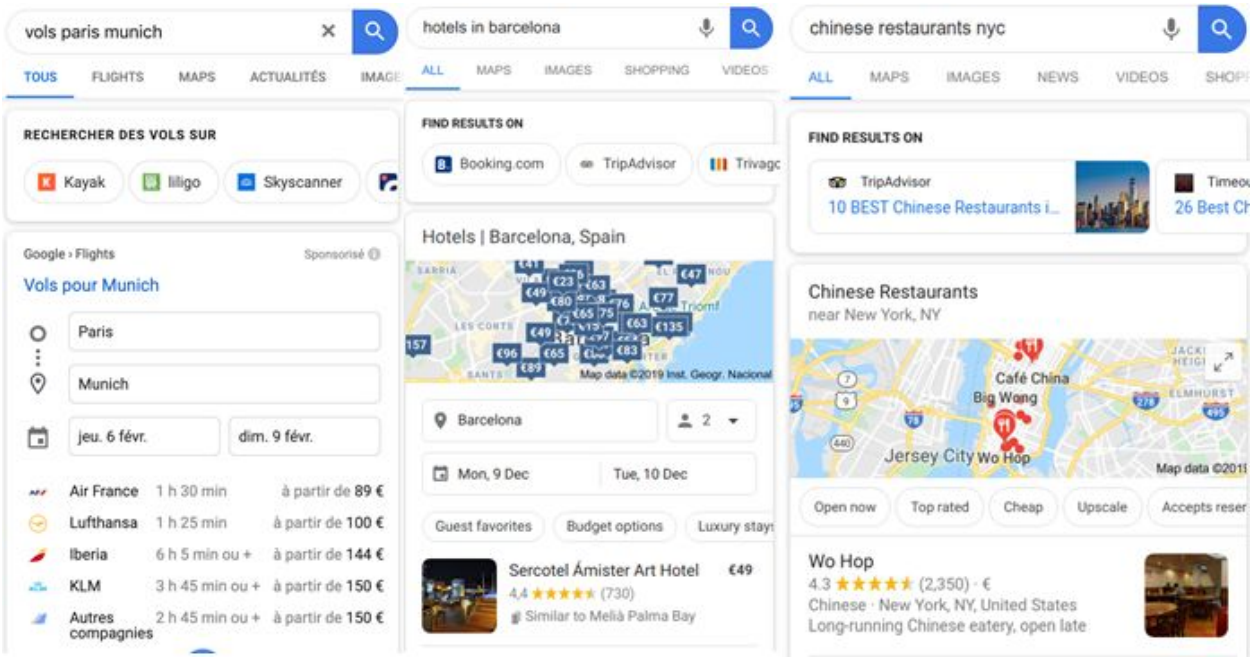
36 *Streetmap.EU v Google* [2016] EWHC 253 (Ch), para. 149 ("*Where the efficiency is a technical improvement, proportionality does not require adoption of an alternative that is much less efficient in terms of greatly increased cost or which imposes an unreasonable burden (at the very least in a case where there is no suggestion that the conduct impugned was likely to eliminate competition)*") and para. 171 ("*I consider that Google is appropriately concerned at the accuracy and relevance of the information on its SERP, and that the Maps OneBox is presented as Google's own offering. There is in my view a material difference between, on the one hand, Google displaying a blue link to a third party website which the user finds is inaccurate once it is accessed, and on the other hand, information presented directly on the Google SERP which proves irrelevant or unreliable. The quality of the SERP is (along with speed of response) the key means by which search engines compete. The Maps OneBox is not simply a convenient means of access to a full-size map, but information for the user in its own right*"). Similar issues arise in the context of local search. Google's search results pages cannot, as a technical matter, display dedicated results from third-party local search services without seriously degrading the quality of its search results, which would undermine the quality of the general search service provided to consumers. *See also* F. Curto Millet, S. Lewis, and P. Stoddart, *Local Search Quality: A Rebuttal of Kim and Luca*, SSRN, June 2019.

37 *See e.g.*, Progress Report on Differentiated Treatment, Expert Group for the Observatory on the Online Platform Economy (July 2020), p. 24: "*self favouring may improve static efficiency by eliminating double marginalisation and can also induce a platform to invest more at the platform level or at the level of integrated products/services*" (p. 24).

that "*it is reasonable for a search engine to provide a direct response to a search query rather than link to third-party pages that may or may not offer the responsive content*".

Suppose that a broad and absolute prohibition on unequal treatment had been in place in 2006, when Google began to show these search designs. Because the thumbnail map and weather box might have been characterized by complainants as a separate Google maps service and a separate Google weather service, a broad prohibition may have prevented Google from launching these indisputably beneficial and procompetitive innovations in Europe. European consumers would have thereby been deprived of the benefits of those improvements.

Another example of how different cases require case-specific analyses and solutions concerns Google's launch of choice carousels in local, hotels, jobs, and flights units. For these designs, an equal treatment remedy of the kind implemented in *Shopping* is not technically feasible. Instead, Google launched choice carousels that list vertical search services prominently above Google's specialized results units. In these choice carousels, Google shows links to vertical search services, together with logos or images, in a scrollable horizontal row above the specialized units. These choice carousels will give users additional choices without depriving them of the benefits of the existing specialized units, as shown below.



- **Questions 9–10: Regulatory interventions**

Questions 9–10 ask whether regulatory rules should allow for case-by-case remedies that apply to specific platforms.

As explained above, we support an agreed baseline of high-level principles that could be applied

across different types of platforms (*e.g.*, a measure to address actual or perceived conflicts of interest where a platform owner competes on the platform), complemented by platform-specific guidance.

Insofar as the consultation contemplates far-reaching interventions with respect to specific platforms (*e.g.*, remedies concerning data access or self-preferencing), these measures may increase the costs — and decrease the rewards — of conduct that promotes innovation and generates efficiencies, as discussed above. This, in turn, runs the risk of deterring practices that benefit European firms and consumers. Any such changes should therefore be considered only after a detailed analysis, with rights of defence, established legal standards, and obligations to respect the principle of proportionality.[38] This is a concern not only for large online platforms but also counterparties and other players (*e.g.*, advertisers, publishers, OEMs, and consumers) who would be negatively affected by cancelled or delayed product launches and investments due to the threat of such interventions.

- **Questions 7–8, 11–15, and 19–24: The appropriate regulatory authority and level of enforcement**

Questions 7–8, 11–15, and 19–24 attempt to identify who should administer an *ex ante* regime. They ask whether enforcement should be at the EU or national level, what characteristics a regulator should possess, and what tools they would require.

The Questionnaire asks which authority should administer and enforce *ex ante* regulation. We consider that we can better comment on the appropriate institutional framework when the regulatory proposals are further developed, but at this stage we can see the benefit of DG COMP having such a role: as a pan-EU authority with experience in complex legal and economic assessments, DG COMP would be well suited to this, drawing on other authorities' expertise as and when appropriate.

I. EU or national level

The Questionnaire acknowledges the "*consensus concerning the benefits for consumers and innovation, and a wide-range of efficiencies, brought about by online platforms in the European Union's Single Market*". Online platforms are not confined to individual Member States. The Questionnaire rightly concludes that "*online platforms facilitate cross-border trading within and outside the Union and open entirely new business opportunities to a variety of European businesses and traders by facilitating their expansion and access to new markets.*" In that context, any *ex ante* regulatory framework and accompanying institutional set up should support a single set of rules within the Single Market and not unduly raise compliance costs.

[38] Moreover, a sequencing of measures from the least to the most intrusive should be accompanied by procedural safeguards that would strengthen in conjunction. This seems to us an important consideration for the Commission.

Complying with one regime is more efficient and provides greater certainty than complying with several regimes in parallel. Regimes in different Member States are based on different cultures, legal systems, and standards, and conduct that is lawful in one is not always acceptable in others. These differences create considerable costs of compliance — for example in meeting different regulatory requirements and in addressing parallel investigations into the same conduct.

II. DG COMP as a responsible authority

As above, we consider that we can better comment on the appropriate institutional framework when the regulatory proposals are further developed, but at this stage we can see the benefit of DG COMP having such a role in administering *ex ante* rules.

Much of the conduct that the Consultation suggests could fall within the scope of *ex ante* regulation are competition concerns that DG COMP has addressed on numerous occasions. For example, DG COMP is currently addressing concerns related to Apple's App Store and Amazon's Marketplace, and has addressed other anti-competitive conduct issues in digital and technology markets over the course of several decades. And its merger investigations in *Microsoft/LinkedIn* and *Apple/Shazam* show that it is capable of appraising and evaluating the value and importance of data. DG COMP is therefore well-placed to make use of expertise that it has developed over many years and to administer any related *ex ante* rules. DG COMP also satisfies all of the criteria identified as relevant by the Questionnaire (Question 19):

- **Institutional cooperation.** DG COMP's position as competition enforcer requires it to liaise with EU institutions, Member States, and supranational organizations.
- **Pan-EU scope.** DG COMP currently administers the EU systems of one-stop-shop merger control and antitrust enforcement across the EU.
- **Swift and effective cross-border cooperation and assistance across Member States.** DG COMP frequently engages with Member States through the European Competition Network, and collaborates with these authorities and national judicial authorities in cartel investigations.
- **Capacity-building within Member States.** DG COMP frequently works with Member States and has contributed significantly — and given direction — to Europe's network of national competition enforcers.
- **Technical capability.** As shown above, DG COMP has shown itself capable of handling complex and sophisticated analyses across a wide range of digital and other complex sectors.
- **Cooperation with extra-EU jurisdictions.** DG COMP enjoys close relationships with competition and other regulatory authorities outside the EU with whom it frequently coordinates in cross-border merger reviews and antitrust investigations.

III. Oversight

The Questionnaire proposes several tools to facilitate oversight of the regime: (i) a reporting obligation on 'gatekeepers' to notify expansion of their activities; (ii) monitoring powers, such as reporting obligations; and (iii) investigative powers. Some form of reporting obligation is reasonable to ensure that any *ex ante* regime can be properly administered, but will need to be proportionate and viewed in light of information-gathering tools that already exist.

For example, a blanket obligation to notify any "*intention to expand activities*" would risk overlapping unnecessarily with merger control regimes. These already provide the Commission and Member States with jurisdiction over certain structural changes to markets that trigger clearly defined thresholds designed to identify those changes worthy of closer inspection. A notification obligation would also impose an unreasonable administrative burden on companies and subjects of the *ex ante* regime. Notifying any "*expansion*" of activities risks capturing the mere creation of new features and development of new products. It also risks generating considerable legal uncertainty. A notification obligation would presumably be defined by reference to a platform's activity in a market — but as the contemplated reforms to the Market Definition Notice show, digital markets are difficult to circumscribe.

A regime that takes account of the proposals we have made above would place DG COMP in a strong position to oversee markets subject to the regime, making use of the tools DG COMP already has. It enjoys significant monitoring investigative powers under both the Merger Regulation and Regulation 1/2003 which could easily be adapted to cover the *ex ante* regime and would provide a familiar legal framework for online platforms. DG COMP also has experience using these tools. It monitors market developments independently and initiates *ex officio* investigations where it identifies collusive conduct, abuse of dominance, and instances of gun-jumping.

IV. Principles for any new regulatory framework

When designing a procedural framework that covers the administration of *ex ante* regulation, Google encourages the Commission to consider the following:

- **Clarity and legal certainty.** Any gatekeeper designation should relate to identified business activities in specific markets within a corporate group so that the scope of that firm's obligations are clear. In order to achieve the requisite certainty, the regulatory instrument should specify the products and/or services that are subject to *ex ante* regulation. As regards the substantive requirements of *ex ante* regulation, sufficient practical guidance will be needed to ensure that firms understand what is required. It is vital that sufficiently detailed guidance that recognizes how platforms operate in practice is developed iteratively with regulated firms.

- **Flexibility and pro-innovation.** New technologies develop and marketplaces change quickly in the digital economy. For example, small companies can rapidly achieve a

prominent position displacing incumbents (*e.g.*, despite only being released globally in 2018, TikTok is now one of the most downloaded apps of the last decade[39] and ranked in sixth place in the global mobile app rankings by monthly active users for 2019[40]). It is therefore important that the regulatory framework has flexibility to keep gatekeeper designations under review. Inefficiencies arise — and innovation is constrained — where regulation fails to keep pace with market changes. To ensure that *ex ante* regulation remains relevant and reflects competitive realities, the regulatory authority should be under an obligation periodically to review gatekeeper designations. In addition, a large online platform that was previously designated as having "gatekeeper" status should be able to trigger a re-review of its gatekeeper designation where it considers that the factual basis on which the designation was made has substantially changed (*e.g.*, due to changes in the market such that the gatekeeper firm no longer has a position of enduring market power or control). These 'special circumstances' reviews could take place in addition to the periodic reviews proposed above.

- **Due process.** Gatekeeper designations could have serious implications, such as requiring firms to change their business practices. The framework should therefore respect due process by providing for an appeals process under which firms can appeal a gatekeeper designation decision and the scope of that decision. Appeal rights should apply when a firm is first designated as a gatekeeper, and when this designation is confirmed following a review (whether a periodic review or a review requested because of 'special circumstances'). To enable firms to assess their grounds of appeal, the regulatory authority should clearly evidence its gatekeeper designation decisions.

- **Collaboration and proportionality.** Any new *ex ante* regulation will introduce new rules whose application (at least initially) may be uncertain. Collaboration between firms and the authority will be important to protect incentives to innovate; for example, a voluntary consultation procedure under which 'gatekeeper' firms could have the option to constructively engage with, and receive feedback from, the authority with the aim of ensuring compliance with the *ex ante* rules. In addition, any new *ex ante* regulation ought to be developed incrementally in consultation with the industry and the affected firms, with reference to precedent and with examples of practical applications for the companies that they will impact. It makes sense for rules to be introduced iteratively and tested before they are enshrined in formal regulations.

- **Evidence-based processes.** An evidence-based approach to enforcement is important. Otherwise, *ex ante* regulation risks penalizing legitimate business conduct. The regulatory authority should clearly set out the evidence upon which it is relying when deciding that

---

39 *See* App Annie, A Look Back at the Top Apps and Games of the Decade, 16 December 2019.

40 *See* HootSuite, There Are More Social Media Users Today Than There Were People in 1971, January 2020; and AdWeek, App Annie: TikTok Was the Most-Downloaded App in Q1 2020, 2 April 2020.

there has been an infringement of the *ex ante* rules, so that the firm subject to that decision can effectively assess its grounds to appeal that decision.

- **Effective triage mechanisms.** Depending on the scope of new *ex ante* regulation, there is a risk that the regulatory authority becomes a 'clearing-house' for complaints about digital firms. Some of those complaints will merit investigation, others will not. We believe it will be important for the authority to have a mechanism for rejecting complaints that are without merit and demonstrating this publicly. This will dissuade abuse, and allow for more efficient use of agency resources, as well as showing that any powers deployed are used in a proportionate and fair way, thereby increasing public trust.

V. Remedies and enforcement measures

The design of enforcement is important to the nature and impact of the regime as a whole. The Commission should keep the objectives of flexibility, pro-innovation, and legal certainty front of mind when considering this question. If the objective is to implement a system that is efficient and nimble (with heavy duty enforcement in exceptional cases being left to the existing antitrust regime), then that will be facilitated by a framework that focuses on collaboration, consultation, and conflict resolution rather than fault-based enforcement. In contrast, a regime with new, far-reaching enforcement powers would need to provide for evidentiary standards in decision-making and rights of appeal that are commensurate to those powers. This is likely to slow down enforcement.

There are various possible approaches to enforcement that would retain the effectiveness of the Commission as a guide to behavior, while still providing for rapid enforcement and preserving incentives to innovate. This could include:

- **Reputational sanctions** where the regulatory authority would publish decisions finding a breach of the *ex ante* rules and maintain a public register of all upheld complaints. This is similar to the sanctions most often used by the Groceries Code Adjudicator (**GCA**) and the Advertising Standards Authority (**ASA**) in the UK.[41] A negative statement would be reputationally damaging with partners, consumers, and regulators, and because it is public it would require a response. For example, the GCA has reported a large reduction in concerns related to its code of practice while using recommendations and reputational sanctions, rather than fines or mandating behavioral change.[42]

---

41 The ASA notes that while the "*vast majority of advertisers and broadcasters agree to follow ASA rulings*," for non-compliant parties "*[o]ne of our most persuasive sanctions is bad publicity – an advertiser's reputation can be badly damaged if it is seen to be ignoring the rules designed to protect consumers*." In particular, the non-compliant advertiser's "*name and details of the problem with their advertising may be featured on a dedicated section of the ASA website, designed to appear in search engine results when a consumer searches for a company's website […]*".

42 See GCA Annual Report and Accounts 2020 (23 June 2020), section 1.1.

- **A reporting obligation** whereby firms that have been found to have breached the *ex ante* rules would be required to publish periodic reports on: (i) changes they have made to their practices that are relevant to the infringement and (ii) any measures taken to resolve the infringement. Platforms could also be required to disclose findings of infringements to customers and suppliers, as well as in merger control filings.

- **Referral of serious breaches** to the DG COMP and other regulators to investigate possible violations of the relevant laws or regulations. The Commission's decision — and evidence already gathered — could form part of the relevant regulator's case file, thereby giving the regulator a headstart in any subsequent investigation.

If, on the other hand, the regulatory authority is granted more extensive enforcement powers, it will be important that the *ex ante* rules provide for procedural fairness in decision-making and commensurate rights of appeal. Proposed enforcement powers could conceivably entail quasi-criminal financial penalties and mandatory orders that will affect how firms use their IP rights, proprietary algorithms, and assets that they have invested heavily in creating. This will have far-reaching consequences on businesses. In particular:

- Decisions prohibiting, or requiring the unwinding of, product changes or improvements that involve large-scale investments could have significant financial ramifications and hurt users that could otherwise benefit from those product improvements (*e.g.*, see our discussion of *Streetmap.EU* above). Particularly far-reaching remedies, together with the threat of fines, could be equated to criminal proceedings for the purposes of the right to a fair trial under Article 6(1) of the ECHR. Such measures therefore warrant full procedural and appeal rights.

- Since an erroneous conclusion could have serious consequences for the firm in question, as well as competition and innovation in the industry, the Commission's enforcement decisions should not be taken lightly. A merits-based appeal ensures an independent review of regulatory decision-making that should lead to better and more robust decision-making.

    - **Question 17: Guaranteeing a high standard of personal data protection and consumer welfare**

Question 17 asks how to balance personal data protection and consumer welfare with the promotion of competition and innovation in relation to the data held by online platforms.

See response to Question 10 of Section 3 above.

    - **Question 18: Media pluralism**

Question 18 asks about effective measures to promote media pluralism.

Online platforms allow for greater media plurality than could ever previously have been imagined. The production and consumption of content has been democratised, to provide unprecedented opportunities to reach global audiences. Broadcasters, writers, musicians, and others can use online platforms, such as YouTube, to connect directly with users and other creators. For example, Netherlands-born producer YoungKio started out producing music beats and building a following on YouTube, before landing a No. 1 hit across multiple EU countries after collaborating with Lil Nas X on the 2019 hit, "Old Town Road." Established news and cultural organisations have also used online platforms to improve their reach with younger people, with news content from EU media outlets such as Welt and Le Figaro frequently amassing millions of views on YouTube.

Before YouTube, the cost of producing and marketing videos was high — particularly where recouping the cost of production through advertising was limited by the small number of viewers. YouTube changed this. By creating and indexing a general repertoire of videos, YouTube provided broadcasters with access to billions of viewers and connected viewers with content on any topic imaginable.

Google Search has also provided editors and writers with a much greater opportunity to distribute their content. Anyone can start a blog or a news service, have it indexed on Google Search, and see their content presented to users in response to search queries. And through new distribution channels, such as app stores, existing media providers have a greater opportunity to share and modify their content. For example, new publishers such as Le Monde have been able to significantly increase subscriptions by making use of the new formats that Google Play facilitates.

Google recognises the challenges faced by the EU in ensuring a sustainable, pluralistic media sector. We acknowledge the increasing difficulties that news publishers, in particular, have faced, but we strongly believe that online platforms, rather than causing these difficulties, have provided press publishers with substantial value. We fully acknowledge the importance of a thriving and pluralistic media for promoting the EU's culture and safeguarding its democracy. We are continually developing new innovations and are willing to work with the Commission, media organisations and others to play our part in supporting media pluralism.

Jump to the questionnaire responses for this section

Part IV. Other Emerging Issues and Opportunities, Including Online Advertising

This section of our accompanying document provides further details on our responses to Section IV of the Commission's questionnaire on the Digital Service Act package. Our responses in the questionnaire cross-refer to sections of this document.

Introduction

Online advertising makes it easy and affordable for advertisers (in particular, SMEs) to grow and market products across Europe. Research found that 26% of EU businesses used online advertising in December 2018, including over 53% of businesses providing accommodation services, with ad targeting a key tool to reach those businesses' target audiences more efficiently.[43]

We recognise and support the Commission's ambitions to ensure that online advertising is fair, transparent and accountable, and consider this an important and necessary step to restore trust in the online advertising ecosystem. Arguably, however, to achieve these goals any intervention measures will need to apply to *all* online platforms (rather than just so-called 'gatekeeper' platforms).

It will be important that any interventions seeking to achieve more transparency and accountability are carefully designed to avoid inadvertently hampering the ability of online advertising tools to deliver the value that publishers and advertisers have come to expect. Consideration of these measures will therefore require the balancing of factors including protection of users' personal data and partners' commercially sensitive information, and potential harm to users and competition through disclosure of data signals that allow 'bad actors' to game the system, or rivals to copy innovations. We stand ready to engage with the Commission on these issues.

Questions 3 and 10 ask for an overview of the options that users have to control the ads that they see on our platforms

Privacy is core to our work at Google, and to our vision for a thriving internet where people around the world can access ad-supported content, confident that their data is protected. We recognise that, to realise this vision, people want more control and transparency over their online environment, including the advertising that is presented to them. For this reason we have

[43] Eurostat, "Internet advertising of businesses – statistics on usage of ads", December 2018.

prioritised developing tools that maximise user control over advertising, and are continuing to think up new ways of achieving these goals.[44] In particular:

- Users — whether signed-in to a Google Account, or signed-out — can easily control the ads they see (including personalised ads) simply by adjusting their preferences in the Ads Settings dashboard.[45] If a user turns off ads personalisation while signed-out, we will stop showing ads related to that user's interests on all Google services. If the user is signed-in, no ads related to their interests will be shown on Google services or partner websites and apps, including across different devices and browsers.[46] Users can also modify their browser or device-level settings to control our ability to set or read cookies or mobile advertising identifier values.[47] We are integrated with the European Digital Advertising[48] Alliance's YourOnlineChoices tool, which offers users a "one-stop shop" platform through which to exercise these controls.

- Not only can users control whether they see personalised ads, but signed-in users also have the option to adjust the data that are used for ads personalisation via their Google Account settings (such as simple on/off controls, including for Location History and Web & App Activity). Users can delete all or part of that data manually and we permit users to specify a time limit (either 3 or 18 months) for how long they want their activity to be saved. Any data older than that will be automatically deleted on an ongoing basis.

- The Privacy Checkup tool allows users to review key data collection activities and important privacy controls, including personalised ad settings. We frequently and prominently promote Privacy Checkup for both signed-in and signed-out users: this reminder appears on the Google homepage and features in the first email users receive in their new Google Account upon account creation. Users are also able to sign up for periodic reminders to take the Privacy Checkup.

- The "Reminder Ads" control enables the user to see which advertisers are remarketing to them, and provides a simple, easy way to block specific advertisers from showing

---

44 See "*Control the ads you see*" available at: https://support.google.com/accounts/answer/2662856?p=adssettings_activity&hl=en&visit_id=637298100523623429-2321023313&rd=1 and "*Greater transparency and control over your Google ad experience*".

45 Users can turn off personalised advertising at any point from their Ad Settings. This is in contrast to some social media platforms, which the CMA Final Report notes "do not give consumers control over the use of their data by allowing them to turn off personalised advertising" (¶8.83)

46 Users can also install a browser plugin to save their personalisation settings to their browser even if their cookies are deleted. See "*Save ad settings with browser plugin*" available at: https://support.google.com/ads/answer/7395996.

47 Google's ads personalisation cookies will be cleared and replaced with cookies containing the value " OPT_OUT ".

48 The relevant setting is called "*Limit Ad Tracking*" for iOS and "*Opt out of Ads Personalization*" for Android.

remarketing ads across their devices.[49] This control gives the user transparency and control at the advertiser level. This setting is also found in the Account Settings dashboard.

- Parents have the option to use YouTube Kids, the app we have created to provide families with a more contained, age-appropriate environment for their children. On YouTube Kids, we only show ads that are approved as family-friendly, and ads do not include any click-throughs to websites or product purchase options.

We continue to explore new ways to provide users with transparency and control, and we are open to constructive dialogue with the European Commission ("**Commission**") and Member State governments on how to achieve this. For example (in partnership with ad industry initiatives such as aboutads.info and YourOnlineChoices (EU), we offer users opt-out controls for almost every ad they see including:

- "Mute This Ad," (available for a large number of display ads), which enables the user to "X" out of an ad, as well as other ads that use the same web URL (either the website domain or specific pages). These ads are not shown to the user again.[50]

- Most recently, we have updated our "Why This Ad?" page (soon to be known as "About this Ad")[51] which is reached by clicking on the 3 dots, then "Why this ad" icon that appears in the corner of most ads.[52] The "Why This Ad?" page provides users with information about why they are seeing a particular ad (e.g. a camera ad was shown because they searched for cameras or visited photography websites) and a link to their privacy controls to update their ads personalisation settings to avoid seeing similar ads in future. This page will soon begin to show users the verified name of the advertiser behind each ad, giving users even more transparency and control over the ads they see.

Question 12 asks about how we detect illicit content in the ads we intermediate

We think that it is best to prevent harmful ads being served in the first place. So we work hard to help advertisers avoid making honest mistakes that lead to policy violations, including by helping them to navigate any restrictions in our Google Ads policies that may affect their ads.[53] For example:

---

49 *See "Greater control with new features in your Ad Settings".*

50 See *"More control with "mute this ad" [x] icon"*.

51 "Why this Ad" will be changing its name to "About this Ad" in September. *See "Updates on our work to improve user privacy in digital advertising".*

52 See "*Why you're seeing an ad*"; and "*Block certain ads*".

53 See, for example, "*Adult content*", "*Counterfeit goods*"; and "*Gambling and games*".

- In some cases, our algorithms are able to detect policy violations during ad creation. In those cases, we provide real-time feedback to help advertisers understand potential policy violations before they actually occur - they can then change ads right away to bring them into compliance.[54]

- We offer the Policy Manager feature within Google Ads. This allows advertisers to monitor policy restrictions of ads, keywords, and extensions across their account.[55] Over time, we plan to add new features, including recommendations for fixing ads, a history of the advertiser's appeals, and an overview of account certifications. Policy Manager allows advertisers to see additional information about what caused their ad to be disapproved by simply hovering over the ad. If advertisers disagree with an action we have taken on their ads, they can appeal the decision for another review with just a few clicks, directly within Google Ads.

In addition to these proactive measures, we use a combination of manual and automated review to detect and remove ads that violate the Google Ads policies. When we detect practices that violate our policies:

- Non-compliant ads and extensions may be 'disapproved'. A disapproved ad will not be able to run until the policy violation is fixed and the ad is approved. If an advertiser has multiple ads disapproved for certain destination-related policies, they can submit an entire campaign for review after fixing their site or app.[56]

- If an account has a history of violations or a particularly serious violation, then the account may be suspended. If this happens, all ads in the account will stop running, and we may no longer accept advertising from that partner. Advertisers have the right to appeal account suspension.

These measures have been effective. They allowed us to take down 2.7 billion ads worldwide for violating our advertising policies in 2019 — that's more than 5,000 bad ads per minute.

Maintaining trust in the digital advertising ecosystem is a top priority for us. Abuse tactics continually evolve and so we invest millions of dollars every year and employ thousands of people, including engineers, policy experts, product managers, and data scientists, to stay ahead of bad advertising practices. For example, in 2020, we assembled an internal team to track the patterns and signals of fraudulent advertisers so we could identify and remove their ads faster, including in response to the COVID-19 pandemic. As the pandemic evolved, we saw a sharp spike in fraudulent ads for in-demand products like face masks. Since January 2020, we have blocked or removed over 68 million COVID-19-related ads (including Shopping ads) from EU-based advertisers and buyers for policy violations including price-gouging, capitalising on global

---

54 See "*Our commitment to help you with policy compliance*".

55 *Ibid.*

56 See "*Submit a campaign for policy review*".

medical supply shortages and misleading claims about cures. We have also suspended more than 1000 accounts (including Merchant accounts on Shopping) from EU-based advertisers for trying to circumvent our systems, including for COVID-19-related ads and offers.

Question 14 asks about good practices to ensure that ads are not placed alongside harmful content from publishers

To maintain advertiser trust in our intermediation services and the content we monetise, we have developed and implemented Google Publisher Policies. For example, we will not display ads on websites selling illegal goods or other illicit products or activities, or which promote products using false, dishonest or deceptive claims.

Enforcement of these policies is important, when a website or app is first admitted to the intermediation network, and subsequently. If harmful content is detected, action needs to be swift to minimise damage, but publishers also need to be provided with information explaining the type of content that can be monetised through the network. We endeavour to meet these objectives when enforcing our policies as follows:

- A website or app receives policy approval (or not) when it is first set up with our publisher facing services (such as Ad Manager). If approved, it is then subject to automated continuous monitoring to verify both content and behavioural compliance (e.g. with the Ad Manager programme policies). Warnings and enforcements are served to publishers via the Policy Center if they are in breach of these policies.[57]

- On YouTube, creators who are eligible for our YouTube Partner Program gain the option to monetise their content. Automated systems and human reviewers then review the channel's content to check that it follows our guidelines.[58] We provide creators with guidance -– for example, on the importance of providing context for content with educational value — and the ability to turn off ads for individual videos. Content is then subjected to continuous automated monitoring to check compliance.

- We use a combination of automated technology combined with human review to identify policy violations. We also review content when it is flagged to us and take action against any violations discovered in a review. Terminating accounts — not just removing ads from an individual page or site — is an effective enforcement tool that we use if publishers engage in particularly serious policy violations or have a history of violating policy.

- We also give advertisers the information and tools to ensure that their ads are not associated with undesirable content. For Google Ads, we offer a variety of ad placement controls that allow small and large advertisers to reach their desired audience on the

[57] See "*Resolve violations in the Policy center*".

[58] See "*YouTube Partner Program overview & eligibility*".

desired sites with ads placed in the desired place.[59] Advertisers can exclude placement on specific sites, apps, videos, content types, or topics that an advertiser may believe are not a good fit for business. Similar controls are available in our demand-side platform ("**DSP**"), Display & Video 360 ("**DV360**").

Using these tools, in 2019, we terminated over 1.2 million accounts and removed ads from over 21 million web pages that are part of our publisher network for violating our policies.[60] Bad actors continuously seek new ways to take advantage of our users, so it is a priority to stay ahead of this. Earlier this year, for example, we faced new challenges with websites seeking to exploit the COVID-19 pandemic to promote dangerous conspiracy theories or to sell fake products to users, both of which are against our Publisher Policies. In a fluid and fast-moving environment, we worked round-the-clock to improve our detection mechanisms.

Industry collaboration is another aspect of combating harmful content. We work with a number of industry organisations, such as IAB, to address issues around quality, ad fraud and brand safety.[61]

Question 15 asks for our views on how meaningful transparency in ad placement could be achieved

As mentioned in the questionnaire, meaningful transparency in the ad placement process involves:

- Advertisers and publishers understanding *why* a particular ad won an auction and was displayed in a given slot on a given webpage, as well as *what content* appears alongside the ad; and

- Users understanding *why* a particular ad has been shown to them.

Helping advertisers and publishers understand the ad placement process

In order for advertisers and publishers to understand auction outcomes, information about key auction parameters needs to be accessible to them. We aim to make this information available to publishers and advertisers, including through blogs and Help Center articles. For example:

---

59 Google Ads also works on a cost-per-click (CPC) model which gives advertisers comfort in knowing that they are only paying for responsive sections of their desired audience.

60 See *"Stopping Bad Ads to Protect Users"*, available at: https://blog.google/products/ads/stopping-bad-ads-to-protect-users.

61 For example, BVDW (IAB Germany) has developed a Code of Conduct for Programmatic Advertising which includes guidance in the form of quality criteria for programmatic advertising. Google is a signatory for both buy and sell sides. The IAB has launched a "UK Gold Standard" with three aims: to reduce ad fraud; to improve the digital advertising experience; and to increase brand safety. Google holds the IAB UK Gold Standard accreditation for YouTube and Authorized Buyers. And we are working with WFA Global Alliance for Responsible Media (GARM) towards cross-industry standards as well.

- The maximum number of search ads slots is publicly available, and this is widely known amongst advertisers.[62]

- We publish an explanation of how we select particular ads as part of our auction process, and in particular the effect that the nature and quality of the ad (as determined by the Ad Rank algorithm) will have on where and when it is displayed.[63] In relation to search ads, our Help Center explains that Ad Rank incorporates the following factors: (i) bid; (ii) quality of ads/landing page; (iii) the context of the search; (iv) the expected impact of ad extensions / other ad formats; and (v) Ad Rank thresholds.[64]

Providing reporting metrics to advertisers and publishers to allow them to assess campaign and inventory performance is also important to aid transparency of auction outcomes. We provide a range of tools and information to advertisers and publishers to help them assess campaign and inventory performance respectively. We also provide extensive information to advertisers on the steps we take to promote brand safety for content hosted on YouTube. For example:

- **For advertisers:** We provide advertisers with the data and tools they need to verify advertising effectiveness, protect against fraud and control the content alongside which their ads are displayed. For example:

    - DV360 and our advertiser ad server, Campaign Manager report on over 100 performance metrics, including clicks, click rate, impressions and cost;

    - Advertisers can customise metrics in reporting, such as selecting the method of impression counting. This helps advertisers to tailor their ad buys along more than 100 dimensions (eg. ad type, campaign, country, device type) and prioritise the ad inventory that performs best.

    - We share minimum-bid-to-win data with all participants in the Ad Manager unified first price auction (this is the minimum bid that would have allowed the buyer to win the auction) to help them optimise their bidding strategies;

    - 48 report types, each of which has multiple fields, are available to advertisers through Google Ads. Advertisers can use these metrics to optimise their campaigns.

    - DV360, and Campaign Manager, conduct extensive filtering of invalid traffic - we do not charge advertisers for ad traffic identified as invalid.

---

62 For example, see SearchEngineLand, "*FAQ: All about the changes to Google's Ad layout on desktop search results*".

63 See "*About ad position and Ad Rank*". These policies may specify different standards for ads served in particular jurisdictions in order to comply with local advertising laws.

64 See "Ad Rank Thresholds: Definition".

- Our response to Question 14 gives a detailed overview of the measures we take to help advertisers ensure that their ads are not placed alongside harmful content. In addition, advertisers on YouTube have access to suitability settings to help them exclude content (for example, live streams), that while in compliance with our policies, may not fit an advertiser's brand or business. We constantly monitor our brand safety error rate (i.e. the number of impressions on unsafe content divided by the total number of impressions) to ensure this is below 1%. We notify advertisers when the error rate goes above 1% until it reliably falls back below 1%.[65]

- **For publishers:** We give publishers the tools they need to evaluate and compare the revenues they are earning across sales channels. For example:

  - In Ad Manager, Data Transfer Files give publishers insights into the impressions served on their websites, including the bid price, when the impression was served and the buyer's identity. This impression-level winning bid data is what is most important for publishers to understand the value of their inventory. Publishers can get additional insights from the Bid Data Transfer file, which we regularly update in response to publisher feedback.

  - Publishers can compare performance of the supply-side platforms they are using to sell their inventory through A/B testing.

We are always open to exploring additional transparency measures and are already actively involved in transparency work with a number of third party measurement providers, industry initiatives, and standards organizations (see Question 17 below).

Helping users understand why a particular ad is displayed

Transparency requires that users understand why they are seeing a particular ad. We aim to give users this insight through the measures described in response to Question 10 above. We also publish information on the categories of data advertisers can use to target ads as part of the ad placement process, enabling users to better understand reasons why certain types of ads may be shown to them.[66]

In August 2019 we published an Ads Transparency Proposal, to serve as a starting point for an industry-wide discussion about tangible ways to enhance user transparency, choice and control in digital advertising.[67] This proposes that users should be able to see: (i) what data is being collected, by whom and why; (ii) who is responsible for an ad; and (iii) what caused an ad to appear. Users should have the ability to access this information at key levels, including at the

---

65 See "YouTube brand safety: Description of methodology".

66 See "*About audience targeting*".

67 See "*Next steps to ensure transparency, choice and control in digital advertising*".

level of the individual, the webpage, the website, the browser being used, and the ecosystem generally.

Questions 16, 17 and 20 explore how increased disclosure and auditing systems could improve transparency and accountability in the online advertising value chain

As explained in the questionnaire we agree that advertisers, publishers and consumers need information about the ad placement process to inform decision making and build trust in the process. As a result we:

- Publish a number of publicly accessible blog posts and Help Center articles that explain how our advertising auctions work (see examples discussed in Question 15) — including two new blogs explaining how: (i) our display buying platforms share revenue with publishers;[68] and (ii) much revenue news publishers retain when they use Ad Manager.[69]
- Publish guidance for users on how to block unwanted ads or turn off personalised advertising;
- Offer training to publishers and advertisers on our ad products and how they work;
- Publish our annual bad ads report, explaining enforcement action we took against illegal and harmful advertising to protect users.

Collaboration with industry bodies is also important for accountability, transparency, and to achieve trust in the ad placement system. As mentioned in Question 15, we are actively involved in transparency initiatives with industry stakeholders, with the goal of increasing transparency and consistency in reporting. For example:

- Media Rating Council ("MRC"): We work closely with the MRC to ensure that our reporting is in line with industry standards and to achieve MRC accreditation. Many of the metrics reported to advertisers are accredited by the MRC.[70] Some of these entities have their measurement metrics reviewed by auditors and accredited by the MRC.[71]
- IAB Tech Lab Ads.txt project and Open RTB: We also work closely with the IAB on industry-wide standards for reporting and accountability. This includes Ads.txt, which is a publicly accessible record of authorised digital sellers for publisher inventory that programmatic buyers can reference if they wish to purchase inventory - this allows

---

68 See "*How our display buying platforms share revenue with publishers*".

69 See "*A look at how news publishers make money with Ad Manager*".

70 See, for example, "*Metrics in reports*".

71 See "*Accredited services*".

publishers to publicly declare which ad tech providers are authorised to sell their inventory. We also follow the standards in the IAB Open RTB Protocol.

- Trustworthy Accountability Group ("TAG"): TAG involves participants across the online advertising ecosystem; its Business Transparency Committee seeks "to build trust, transparency and accountability throughout the digital supply chain." They are working on "developing and promoting the adoption of standards, protocols and technologies that recognize honest industry participants and help combat illegal activity." See here for details on current transparency work, including a registry and payment ID system to help identify legitimate participants in the ad ecosystem, as well as inventory quality guidelines to provide a common framework for ad ecosystem participants to describe and disclose the characteristics of advertising inventory.

- BVDW (IAB Germany): We are a member of BVDW, which has developed a Code of Conduct for Programmatic Advertising. The voluntary commitment includes guidance in the form of quality criteria for programmatic advertising for advertisers, agencies, DSPs, supply-side platforms ("**SSPs**"), publishers, data management platforms, data providers and verification providers.

- IAB Transparency and Consent Framework ("TCF"): The TCF aims to help parties in the digital advertising chain ensure that they comply with the EU's GDPR and ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device, such as cookies, advertising identifiers, device identifiers and other tracking technologies.

We remain open to feedback and ready to engage about what more we can do to improve transparency and accountability in the Google ads ecosystem. Factors that need to be considered in these conversations about appropriate levels of public disclosure and auditing mechanisms include:

- **Gaming risks:** Disclosure of too much granular information about auction algorithms and safeguards could make it easier for bad actors to game those safeguards. Taking Google as an example - as explained in response to Question 12, we employ algorithms to help detect policy violations. Exposing these algorithms publicly would make it easier for malicious advertisers to find workarounds and post harmful ads.

- **Confidential information of business partners:** Disclosing confidential ad revenues or other information protected by contracts with business partners (e.g. detailed bidding data) could cause commercial distrust and harm companies' relationships with those partners.

- **Data privacy laws:** These restrict platforms' ability to share granular information that may constitute personal information for certain users. Disclosure of this information could breach data protection rules and best practice. For example, the user information

which we are able to share with third parties is often anonymised and/or aggregated as a result.

- **Protection of proprietary designs and data and harm to competition:** Making granular information about the ad auction publicly available could disclose proprietary algorithms to competitors, reducing uncertainty and diversity in the market. This would be harmful to competition and incentives to innovate. Consider, for instance, the investments we make in continually improving and refining our ad exchange auction algorithms. If this information (such as signals relevant to our Dynamic Allocation feature) were available to competing ad exchanges, allowing them to free-ride off our investment and copy its innovations, there would be no incentives for continued investment.

As mentioned in the questionnaire, transparency and accountability mechanisms should arguably also apply to *all platforms*, since these concerns apply regardless of the size of the platform and the business model they rely on. For example, the Guardian Media Group brought a high-profile claim against the Rubicon Project in respect of hidden fees.[72]

Our consideration of how to enhance transparency and accountability also extends to news platforms. We have a responsibility to work with the Commission, news publishers and other stakeholders in preserving media pluralism and a shared interest to do so - users want to use Google to find a variety of news sites.[73] Digital advertising has increased in significance as a revenue source for many media publishers and we acknowledge the importance of providing publishers with transparency and the tools to play their essential role in communicating to the EU public. We are therefore investing in ways to support the news industry.[74] Ads-funded tools developed by Google have given smaller media players unique opportunities to monetise their inventory. We have also launched the YouTube Player for Publishers, providing news publishers with user analytics and monetisation options to help them maximise revenue on the platform.[75] During the COVID-19 pandemic, we have shared free tools and resources to support journalists'

---

72 See "*Rubicon Project and the Guardian resolve legal dispute over hidden fees*".

73 Although, as shown by the CMA Final Report, Table 5.7, news publishers are not dependent on us for traffic as Google Search only accounts for approximately a quarter of their traffic.

74 The Google News Initiative ("GNI") is our global effort to help news organisations thrive in the digital age through various programs and partnerships. The GNI includes the Digital News Innovation Fund, which financially supports high-quality journalism in Europe. Other investments that benefit the news industry include Subscribe with Google, which helps publishers grow by making it easier for users to sign up for a news subscription. Additionally, our wider business is beneficial for news publishers - our search tools allow users to find news publishers websites at no cost to the publisher (this is despite Google not earning significant advertising revenues from search queries for news — most news queries are not suitable for the display of ads and the majority of search engine results pages resulting from a news query do not show any ads at all).

75 See "*Digital News Initiative: Introducing the YouTube Player for Publishers*".

work, including live training workshops on YouTube.[76] From the smallest blog owner to incumbent news platforms, all have an opportunity to make money using Google's tools.

Question 18 and 19 deal with information disclosures to inform consumers about political advertising that they are shown

As mentioned in the questionnaire, to provide consumers with clarity and confidence on the origins of the political advertising they view online, we publish our EU election ads policy, which outlines our restrictions for targeting election ads. We also recognise the importance of consumer control in ensuring that political advertising is accountable: our Ads Settings go beyond transparency, and give users control of the ads they see, including the option to turn off personalised ads altogether.

In addition, in compliance with the Code on Disinformation, and to ensure that consumers and researchers have the ability to scrutinise who is paying for political advertising, we produce a Political Advertising Transparency Report for each EU Member State identifying:

- the number of individual political ads served by Google;
- the amount spent on political advertising;
- top spenders on political advertising; and
- each political ad in an Ad Library (identifying the advertiser and categorised by amount spent, impressions and format).

We have designed these reports to be accessible: they are searchable and downloadable, and can be filtered by spend, number of impressions, and type of ad format. The data from the EU election advertising Transparency Report and Ad Library is also available on Google Cloud's BigQuery. Using BigQuery's API, any interested third party can write code and run their own unique queries on this data set to develop charts, graphs, tables, or other visualizations of election ads on Google platforms.

The screenshots below demonstrate, for a single Member State, the information that consumers can access about total political advertising spend from the report. They can also customise their search to look for individual advertisers or the advertisers that spend the most on political advertising. The Ad Library tool allows them to view the targeting criteria for individual ads.[77]

---

[76] See "*Reporting in a crisis*" ; and "*GNI Live Trainings*".

[77] To take another example — for a single ad served on YouTube — users would be able to view the ad and see detailed information about when the ad ran on the site, any targeting criteria (age, gender, and location), the amount spent by the advertiser (in ranges), and the number of impressions the ad received(see below screenshots for example)

Figure 1
Screenshot displaying total political advertising spend in Germany

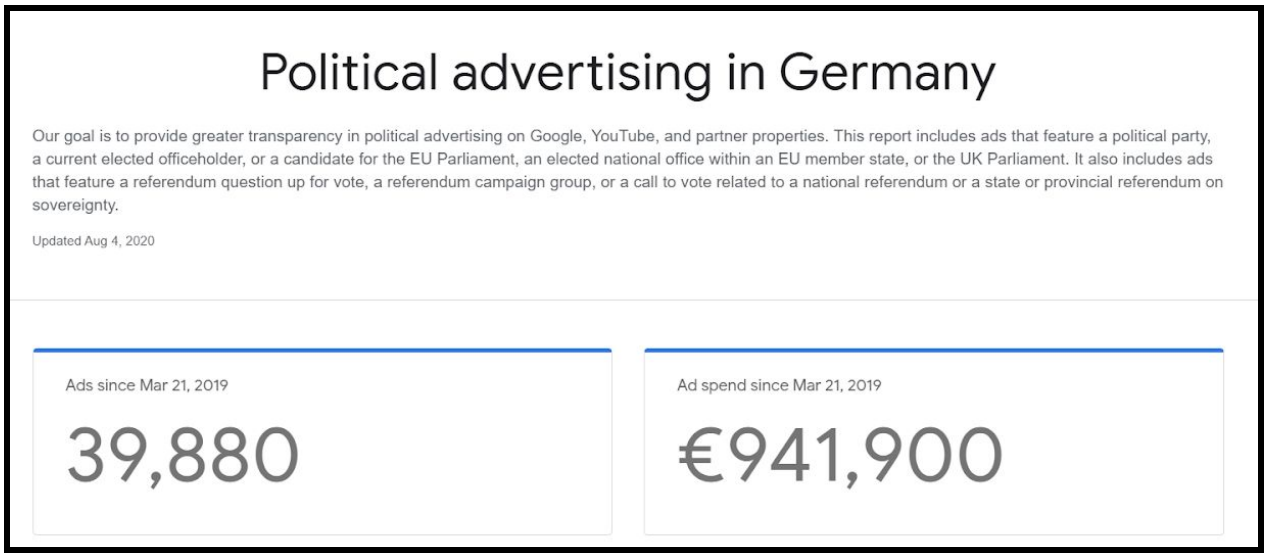


Figure 2
Screenshots of options to search by advertiser

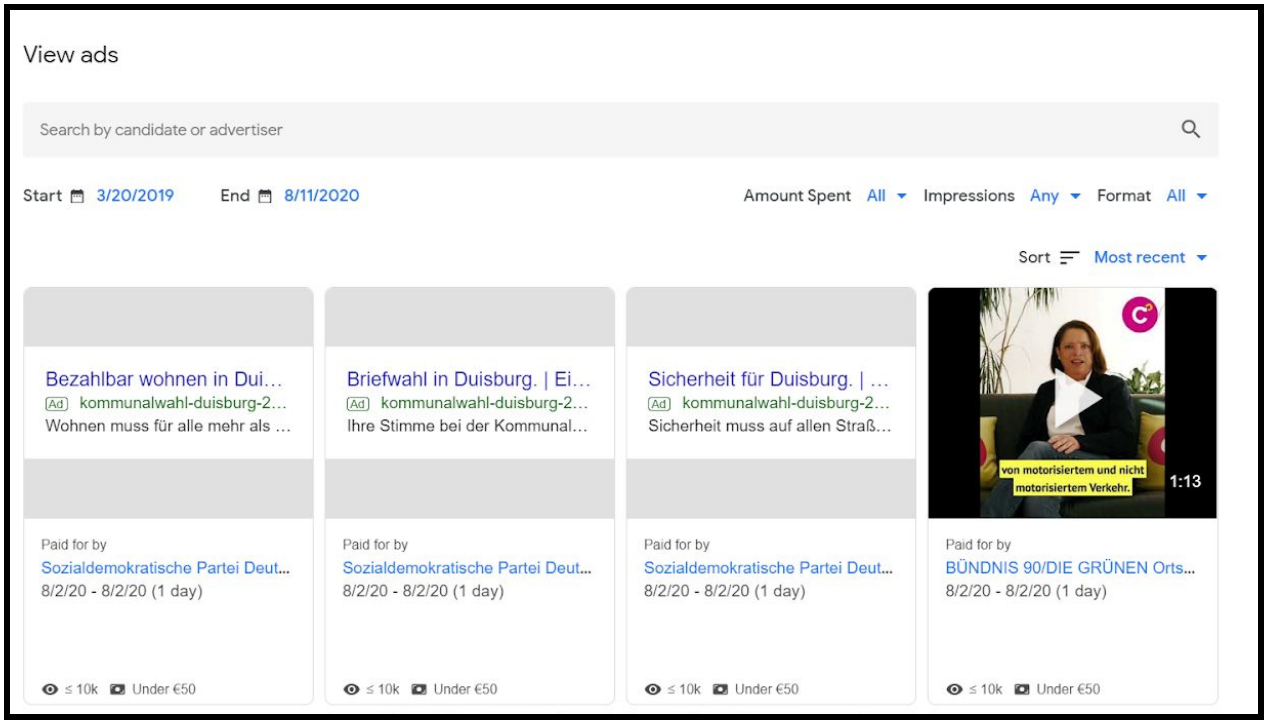
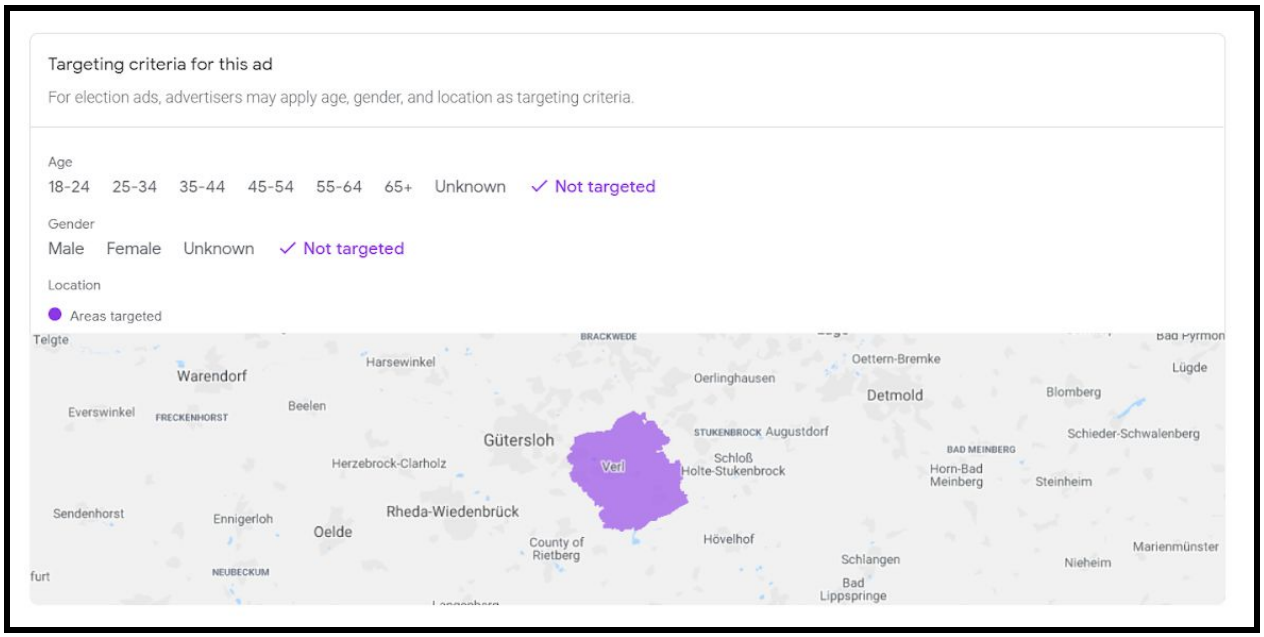


Figure 3
Screenshot of political advertising targeting criteria



The report demonstrates our commitment to working with stakeholders and providing users with a meaningful level of transparency regarding political advertising they may see on our platforms. It strikes an appropriate balance between granular detail and accessibility. Disclosure that goes further and provides consumers with access to, for example, a raw database containing all of the political advertisements on Google products, would be counterproductive as it would no longer be accessible and so fail to improve accountability to users.

As signatory of the Code on Disinformation, over the course of the past years, we have engaged with numerous stakeholders in order to explain, collect feedback, and improve our policies and tools. We have attended meetings with the European Regulators Group for Audiovisual Media Services (ERGA), during which we presented our transparency tools for political ads. We have also exchanged views with experts at numerous policy roundtables, conferences, and workshops - both in Brussels and in the EU capitals.[78]

We think that taking this feedback seriously is important for meaningful disclosure. For example, given recent concerns and debates about political advertising, and the importance of shared trust in the democratic process, in November 2019, we announced a few changes to our advertising policies in this space. Most notably, we limited election ads audience targeting to age, gender, and general location (postal code level). Political advertisers can, of course, continue to do contextual targeting, such as serving ads to people reading or watching a story about, say, the economy. This aligned our approach to election ads with long-established

[78] For more details please see our annual self-assessment report of signatories to the EU Code Of Practice on Disinformation.

practices in media such as TV, radio, and print, while allowing election ads to be more widely seen and available for public discussion.

Jump to the questionnaire responses for this section

SECTION II: Questionnaire

Part I. How to Effectively Keep Users Safe Online

1. Main Issues and Experiences

A. Measures taken against illegal offering of goods and services online and content shared by users

We recognise the concerns of the Commission, Member State governments, and EU citizens about the presence of illegal content and activity online. We have made it a central priority to address these issues, and to stay ahead of bad actors and evolving threats. Using a "people + machine" framework, we have made substantial progress in building out our systems and processes for addressing illegal activities.

We also acknowledge the need to work together to create a more responsible, innovative, and helpful internet. Our services are used around the world by users from different cultures, languages, and backgrounds. Our efforts to build an effective notice-and-takedown system are supported by the efforts of a cross-functional team, including policy specialists, lawyers, engineers, product managers, data analysts, content reviewers, operations analysts, emerging threat analysts, and many others. User safety is a central priority across all Google products. The methods we use, however, vary according to the nature of the product, the relationship to our users or customers, and the degree of knowledge or control over the content. What is appropriate for one product is not always appropriate for another. We are continually seeking to build on and improve our processes, and we are committed to an open dialogue with governments on how we can do so.

1. What systems, if any, do you operate for addressing illegal activities conducted by the users of your service (sale of illegal goods -e.g. a counterfeit product, an unsafe product, prohibited and restricted goods, wildlife and pet trafficking - dissemination of illegal content or illegal provision of services)?

A notice-and-action system for users to report illegal activities
A dedicated channel through which authorities report illegal activities
Cooperation with trusted organisations who report illegal activities, following a fast-track assessment of the notification
A system for the identification of professional users ('know your customer')
A system for sanctioning users who are repeat infringers
A system for informing consumers that they have purchased an illegal good, once you become aware of this

Multi-lingual moderation teams
Automated systems for detecting illegal activities
Other systems. Please specify in the text box below
No system in place

2. Please explain. (5000 characters maximum)

Notice-and-action system: When we receive notifications to remove allegedly illegal content, we review each notification carefully. We provide a tool to help users report content that they believe should be removed from Google's services based on applicable laws, and the form seeks appropriate information to help us resolve the matter as quickly as possible. Deciding whether content is illegal under local laws can often be challenging, and highly context-dependent.

Copyright infringements and piracy: This report details how Google fights online piracy through industry-leading tools like YouTube Content ID and our Search demotion signal, working with policymakers and setting industry standards to cut off revenues to bad actors.

Counterfeit goods: We support enforcement against counterfeit goods in a variety of ways across our products.

- For example, we have clear policies against using Google Ads to promote counterfeit goods. When abuse is brought to our attention, we respond to valid complaints regarding bad actors attempting to directly make money from counterfeit goods using Google Ads as well as Google Shopping. We also take action in response to valid complaints about the sale or promotion of counterfeit goods through content that users host with us, including on YouTube.
- Trade mark holders can now provide us notice of web pages selling counterfeit goods that appear in Google Search results, and we will remove those links from our results when we receive valid takedown requests. This removal policy is accompanied by a ranking signal that will help us further limit the visibility of sites in Google Search that are consistently found to be selling counterfeit goods.
- Finally, as a major brand owner we are active members of key industry groups, including the International Trademark Association (INTA), the International AntiCounterfeiting Coalition (IACC) and MARQUES. Within these groups we collaborate with brand owners on enforcement strategy, knowledge sharing, training and networking.

Cooperation with trusted organisations: We participate annually in the evaluation of the EU Code of Conduct on Illegal Hate Speech, where third-party organizations under the supervision of the EU Commission test YouTube's response to illegal hate speech. In addition, YouTube's Trusted Flaggers program provides robust tools for individuals, government agencies, and NGOs that are particularly effective at notifying YouTube of content that violates our Community Guidelines. Our trusted flaggers can also report new trends they observe through a dedicated form.

Know your customer: In 2018, we announced a new identity verification policy for political advertisers, where we display the identity in the ad unit so that users can learn more about the election ads they see on Google's platforms. Since introducing this program, we've verified political advertisers in 30 countries. To provide greater transparency and equip users with more information about who is advertising to them, we are extending identity verification to all advertisers on our platforms. As part of our phased approach, advertisers will be required to complete a verification

program in order to buy ads on our network. Advertisers will need to submit personal identification, business incorporation documents or other information that proves who they are and the country in which they operate. This change will make it easier for people to understand who the advertiser is behind the ads they see from Google and help them make more informed decisions when using our advertising controls. It will also help support the health of the digital advertising ecosystem by detecting bad actors and limiting their attempts to misrepresent themselves.

Automated systems: On our platforms, we enforce our policies at scale by using a combination of people and machines, and our strategies continuously evolve. We discuss the benefits and limitations of the technology elsewhere in the submission.

Multi-lingual moderation teams: To achieve accuracy and scale in our work, we invest in people and technology. We now have over 10,000 people across Google working on content moderation and removal on our platforms. This includes reviewers teams that are fluent in multiple languages, who carefully evaluate legal removal requests and flags 24 hours a day in time zones around the world. We have a robust quality review framework in place to make sure our global staff are consistently making sound decisions on reported content. They receive regular feedback on their performance. Robust wellbeing programs and psychological support are offered for our reviewers.

3. What issues have you encountered in operating these systems? (5000 characters maximum)

While we believe a notice-based system remains essential, we do encounter operational challenges.

Complexity of legal determinations and incomplete factual record

Deciding whether content is illegal under local laws is often challenging. Assessing an allegation of defamation, for example, can be very difficult for our reviewers because we typically do not have the necessary background facts of the individual case to evaluate whether the elements of the law have been met. We also see cases where the facts are clear, but the conclusion that the law would apply is uncertain. For instance, we encounter cases of political speech that is said to unlawfully harass a politician, but which implicates the speaker's fundamental right to critique their leaders. This is why we advocate for the introduction of notice formalities, and assurances that the DSA will not force services to prioritise the speed of removal over careful review balancing all involved rights, not just the right of the person requesting a removal.

In the case of counterfeit goods, there is no central repository or way for Google's systems to understand who holds the relevant trade mark rights for every product listed on the web or what products that are purportedly genuine are in fact counterfeit. This is important information that only the trademark holder knows and needs to affirm to us via a notice-and-takedown process for meaningful review and action to take place.

Non-counterfeit forms of trade mark infringement involve even more highly factual, multi-faceted determinations, which can even be challenging for the courts. Trade mark rights are specific to goods and services and the jurisdiction in which the owner, and its licensees, have obtained rights. Whether there is a likelihood of confusion between trade marks or whether goods have not been legitimately placed on the market in the EU are often very fact-specific questions. This is why in many instances it is appropriate for judges to make the determinations of infringement and then we can swiftly honor those determinations once they have been made.

Overly-broad, incomplete, or bad faith requests

Not all user reporting is reliable or actionable. Many of the complaints are an expression of disagreement with views expressed in the content, are off-topic, or even a deliberate effort to use false claims to suppress speech or valid commercial activity. Given our experience of deliberate false claims, we support penalties for bad faith requests.

We regularly receive overly-broad or unwarranted removal requests. We have encountered, for example, a reporting organisation working on behalf of a major movie studio that requested removal of a movie review on a major newspaper website; a driving school that requested the removal of a competitor's homepage from search, on the grounds that the competitor had copied an alphabetised list of cities and regions where instruction was offered; an individual who requested the removal of search results that linked to court proceedings referencing her first and last name on the ground that her name was copyrightable; a fashion company that sought removal of ads promoting authentic pre-owned handbags on trade mark grounds. Our experience supports academic analysis that found that many seek to remove potentially legitimate or protected speech.

In addition, we often see requests to take down content without a proper legal basis, or a clear indication of what is problematic or where it appears in the content (for example, a short extract of an extensive webpage or a moment in an hours-long video). We see enforcement vendors acting on behalf of trade mark holders submitting large volumes of notices with numerous deficiencies, including lack of trade mark registration details or proof of authorization to act on behalf of the trade mark holder, duplicative notices, and unwarranted notices on content permissible under our policies and the law. Our transparency report on the NetzDG in Germany shows we received over 20,000 incomplete complaints from January to June 2020. This causes a diversion of resources in addressing other, valid notices.

Finally, we have seen bad actors attempt to abuse the system. Some have submitted fabricated copyright infringement allegations as pretext for censorship or to hinder competitors. This includes requests to remove critical product reviews on the grounds that the article includes a photograph of the (allegedly copyrighted) product; and individuals copying critical news articles and backdating them to request the take down of the original article.

We aim to strike a balance between making it easy and efficient to report infringing content while also protecting free expression. We constantly work to identify abusive behavior and patterns. This is part of why we publish our Transparency Report and submit notices to the Lumen database, to help hold requesters accountable and to document cases for journalists, webmasters, and the public.

5. Please quantify, to the extent possible, the costs of the measures related to 'notice-and-action' or other measures for the reporting and removal of different types of illegal goods, services and content, as relevant. (5000 characters maximum)

We now have over 10,000 people across Google working on content moderation and have invested hundreds of millions of dollars in these efforts. We are constantly refining our practices.

6. Please provide information and figures on the amount of different types of illegal content, services and goods notified, detected, removed, reinstated and on the number or complaints received from users. Please explain and/or link to publicly reported information if you publish this in regular transparency reports. (5000 characters maximum)

We issue several transparency reports and disclose data on content moderation and content removal requests on a regular basis, including:

- Our transparency report on requests to remove content. We receive content removal requests through a variety of avenues and from all levels of government— court orders, written requests from national and local government agencies, and requests from law enforcement professionals. Sometimes users will forward us government removal requests, such as when someone attaches a court order showing certain content to be illegal. Some requests ask for the removal of multiple pieces of content, and, conversely, there may be multiple requests that ask for the removal of the same piece of content. This report enables users to break out the data by country, including removal requests, removal percentages, and category (e.g., privacy and defamation, national security, regulated goods and services). We also highlight requests that are of public interest to provide a glimpse of the diverse range of content removal requests we receive. For example, users can examine data around the more than 40,800 pieces of content notified by the French government since 2009, the percentage of requests from the Netherlands which include a court order where some content was removed, or the reasons for removal in requests from the Austrian government.
- A report on actions related to European privacy law. In a May 2014 ruling, the Court of Justice of the European Union found that individuals have the right to ask search engines like Google to delist certain results about them. This report provides data on the volume of requests, the URLs delisted, the individuals submitting requests, and the content of websites and URLs identified in requests. Google has delisted over 1.5 million URLs, and the report breaks down the percentage of URLs evaluated for delisting by the category of site identified in the request (e.g., news, social media).
- Removals under Germany's Network Enforcement Law (NetzDG). The law requires services in scope to publish a transparency report on a biannual basis. From January-June 2020, YouTube removed over 66,500 pieces of content reported by users and over 24,200 pieces of content by submitters who self-identified as reported from a reporting agency. Note that more than 76% of content reported under the NetzDG was determined not to violate our Community Guidelines or the criminal statutes referred to in NetzDG and was therefore not removed or blocked.
- Information on counterfeits. We shut down approximately 12,000 Google Ads accounts containing 10 million ads for attempting to advertise counterfeit goods in 2019. Google takes strong action against any promotion of counterfeiting on our ads platforms, and we devote significant engineering and machine learning-based tools to prevent abuse that violates our policies, including counterfeiting. Over 99% of Google Ads accounts terminated on counterfeit grounds are proactively detected by these systems and the ads in the accounts never go live. These systems are not able to know if a particular advertised good is counterfeit (only the brand owner knows), however they are able to detect fraud and spam tactics used by malicious advertisers, including counterfeiters. For any ads that aren't detected by our machine learning-based systems, we provide an easy way for brand owners to notify us through a reporting form, and we respond to reliable Google Ads counterfeit complaints within 24 hours.
- Content delistings due to copyright. Google regularly receives requests to delist content from Search results that may infringe a copyright. This report provides data on the close to 4.7 billion URLs requested to be delisted from Search from over 2.9 million unique top-level domains, by 213,483 unique copyright owners and 207,281 unique reporting organizations.
- Our annual Bad Ads Report. We blocked more than 35 million phishing ads and 19 million "trick-to-click" ads in 2019. Overall that year, we blocked and removed 2.7 billion bad ads—more than 5,000 bad ads per minute.

7. Do you have in place measures for detecting and reporting the incidence of suspicious behaviour (i.e. behaviour that could lead to criminal acts such as acquiring materials for such acts)? (3000 characters maximum)

Across our products, we work with experts to identify emerging specific threats. We operate dedicated threat intelligence and monitoring teams that provide insights and intelligence to our policy development and enforcement so they can stay ahead of bad actors. Google's Threat Analysis Group, for example, works to identify malicious actors wherever they originate, prevent their attacks, and share information on specific threats with other companies and law enforcement officials. We provide quarterly public updates about coordinated influence operations, and we issue warnings to users when we believe they may be the targets of government-backed phishing attacks.

We know that elections pose particular challenges that require all of our teams across Google and YouTube to work together. Concerns run particularly high ahead of elections, a time when secure access to authoritative information is essential, and the 2019 European Parliament elections were naturally a big focus for our teams. We launched and localised a number of useful tools, provided training for campaigners, journalists and other key actors. We created Protect Your Election, a suite of free tools to help protect high-risk users from the most pervasive digital attacks, like DDoS and phishing attacks, to which politicians, journalists, and campaigns are often most vulnerable. Our Advanced Protection Program helps combat the types of digital attacks that could threaten account and web-site security.

However, as we detail below, we remain concerned with proposals that would circumvent existing legal protections or require internet service providers to disclose user data to the government without any prior oversight by an independent authority and without proper safeguards.

B. Measures against other types of activities which might be harmful but are not, in themselves, illegal

1. Do your terms and conditions and/or terms of service ban activities such as:

Spread of political disinformation in election periods?
Other types of coordinated disinformation e.g. in health crisis?
Harmful content for children?
Online grooming, bullying?
Harmful content for other vulnerable persons?
Content which is harmful to women?
Hatred, violence and insults (other than illegal hate speech)?
Other activities which are not illegal per se but could be considered harmful?

2. Please explain your policy. (5000 characters maximum)

Google has a variety of products and services, and the measures we take may vary accordingly. Using a mix of tools, we enforce our content policies at scale and take tens of millions of actions every day against content that does not abide by the policies for one or more of our products. With our content

policies and Community Guidelines we aim to create a welcoming, responsible environment for our users.

On YouTube, we have made over thirty changes to our policies over the last year and a half. We do not permit hate speech and protect individuals or groups targeted on the basis of any of certain attributes, such as age, ethnicity, gender identity and expression, immigration, victims of major violent events, and others. We are also strengthening our approach to limiting children's access to mature content.

We have also retooled the way YouTube handles content moderation, focusing on four pillars: removing violative content, raising up authoritative content, reducing the spread of borderline content and rewarding trusted creators.

YouTube takes robust measures against coordinated disinformation campaigns. Misinformation, is of course, much more complicated. Still, we have taken a novel approach to try to reduce misinformation across the platform, using local inputs. We rely on external evaluators located around the world to provide critical input on the quality of a video, based on public guidelines. Each evaluated video receives up to nine different opinions and some critical areas require certified experts. For example, medical doctors provide guidance on the validity of videos about specific medical treatments to limit the spread of medical misinformation. Based on the consensus input from the evaluators, we use well-tested machine learning systems to build models. These models help review hundreds of thousands of hours of videos every day. Over time, as the inputs improve, the accuracy of these systems will continue to improve.

On Google Play, we have Developer Program Policies that help ensure we continue to deliver the world's most innovative and trusted apps to over a billion people. We've created standards defining and prohibiting content that is harmful or inappropriate for our users. For example, we don't allow apps that: contain or promote sexual content, such as pornography, or any content or services intended to be sexually gratifying; depict or facilitate gratuitous violence or other dangerous activities; contain or facilitate threats, harassment, or bullying; or promote violence, or incite hatred against individuals or groups based characteristics that are associated with systemic discrimination or marginalisation.

We want to support a healthy, trustworthy and transparent digital advertising ecosystem. Our Google Advertising policies are designed not only to abide by laws but to ensure a safe and positive experience for our users. For example, we prohibit ads that promote counterfeit goods, as well as those that promote hatred, intolerance, discrimination, or violence. We don't allow ads or destinations that deceive users by excluding relevant product information or providing misleading information about products, services, or businesses.

In contrast to content sharing and communications services, web search engines, like Google Search, are indexes of the web at large. We do not host this content, so our approach is based on the belief that, when it comes to questions about what information should be stripped from public availability, those lines are better drawn by the rule of law. When it comes to removing links to web pages from Google Search, we are strongly guided by local law and decisions from the courts. We have a clear process for reviewing and taking action on legal removal requests and encourage users and authorities to alert us to content they believe violates the law. We also use ranking algorithms to surface relevant and high quality information, and to help prevent poor quality or harmful content from rising in search results.

There is a very narrow category of content that we will remove from Search globally to ensure product quality and individual user safety based on exposed sensitive personally identifiable information. Upon request we will remove a narrow set of highly personal information. To avoid spammy results, we may remove sites from search results that exhibit deceptive or manipulative behavior designed to deceive users or game Search algorithms. For search features in which we have applied a design treatment that proactively highlights particular pieces of content (e.g., knowledge panels) or predicts user interest (e.g., autocomplete), we enforce feature-specific sets of content standards to prevent, for example, pornography, hate speech, or extreme graphic violence from surfacing when users have not asked for it.

3. Do you have a system in place for reporting such activities? What actions do they trigger? (3000 characters maximum)

Yes.

For YouTube, our Community Guidelines flagging system enables users to alert us to content that potentially violates our YouTube Community Guidelines. We have also developed a "Trusted Flagger" program to help encourage submissions of multiple high-quality flags about content that potentially violates our Community Guidelines. We review items that have been flagged against all of our Community Guidelines. In general, our review teams will remove content globally if it's in violation of our Community Guidelines. Our teams may also take one of several alternative actions, including:

- **Age-restricting** videos that don't violate our policies, but may not be appropriate for all audiences. Age-restricted videos are not visible to users who are logged out, are under 18 years of age, or have Restricted Mode enabled.
- **Limiting features** of content that doesn't violate our policies but is close to the removal line and could be offensive to some viewers. Such content will remain available on YouTube, but the watch page will no longer have comments, suggested videos or likes, and will be placed behind a warning message. These videos are also not eligible for ads or recommendations.
- **Demonetising** content that does not cross the removal line but are not in line with our partner program policies. We set a high standard of quality and reliability for content creators who would like to monetise or advertise their content. We have no desire to derive revenue for ourselves, or for any other business, from harmful content or behavior.
- **Account strikes or termination**, in cases of repeated abuse or of more egregious violations. In most cases the first violation of our Community Guidelines will result in a warning. Then we have a general three-strikes rule where three policy violations lead to account termination, but we may also terminate the account at first offense for egregious violations.

Similar mechanisms for flagging exist on other products. On Google Play, for example, users can report content issues or violations of our Developer Program Policy, including inappropriate content, comments, and reviews. For example, users can go to the detail page for an app or game, tap "More," and then "Flag as inappropriate," choose a reason and submit. Users who wish to report an ad can choose the type of ad and follow the prompts in this tool to alert us to ads that potentially violate our Google Ads Policies for review.

On Search, if you are unable to have a website remove exposed sensitive personally identifiable information, users can submit a request to remove this content in accordance with our policy guidelines. We also encourage users to report search results that they believe result from spam, paid links or malware and are in violation of our webmaster guidelines. We have user feedback tools for a number of our search features for which we enforce feature-specific content standards - features like autocomplete and knowledge panels.

4. What other actions do you take? Please explain for each type of behaviour considered. (5000 characters maximum)

As technology has advanced, the systems powering our review systems have too. Today's content review system uses new technological developments to detect content that may violate our policies. While breakthroughs in machine learning and other technology are impressive, the technology is far from perfect, and less accurate on more nuanced or context-dependent content. Their mandated use would be inappropriate, and could lead to restrictions on lawful content and on citizens' fundamental rights.

To enforce our policies at the scale of the web, we rely on a mix of automated and human efforts to spot problematic content. In addition to flags by individual users, sophisticated automated technology helps us detect problematic content at scale. For example, our automated systems are carefully trained to quickly identify and take action against spam. Our automated systems also flag potentially problematic content for human reviewers, whose judgement is needed for the many decisions that require a more nuanced determination. The context in which a piece of content is created or shared is an important factor in any assessment about its quality or its purpose. We are attentive to educational, scientific, artistic, or documentary contexts, including journalistic intent, where the content might otherwise violate our policies.

We use a variety of technologies. As an example, we have heavily invested in engineering resources to detect child sexual abuse material (CSAM) in ways that are precise and effective, and have long used this technology to deter, detect, and remove offenses on our platforms. CSAI Match technology allows us to more quickly detect known CSAM videos, and helps detect videos that may have been manipulated to avoid detection. We also have developed a Content Safety API which is used to more quickly identify and prioritize never-before-identified CSAM for review. Both technologies are licensed for free for qualifying companies and NGOs. For some content, for example, terrorist recruitment videos, hosting platforms like YouTube and Drive use a shared industry database of hashes (or "digital fingerprints") to increase the volume of content our machines can catch at upload.

Automated flagging by machine on YouTube. In June 2017, YouTube began to deploy machine learning technology to flag violent extremist content for human review. YouTube uses the corpus of videos already reviewed and removed for violent extremism to train machine learning technology to flag new content that might also violate the Community Guidelines. Using machine learning technology trained by human decisions means the enforcement systems adapt and get smarter over time. However, we find that these systems are most effective when there is a clearly defined target that is violative in any context. Machine automation simply cannot replace human judgment.

5. Please quantify, to the extent possible, the costs related to such measures. (5000 characters maximum)

We now have over 10,000 people across Google working on content moderation and have invested hundreds of millions of dollars in these efforts. We are constantly refining our practices to combat content that violates our policies.

6. Do you have specific policies in place to protect minors from harmful behaviours such as online grooming or bullying?
Yes | No

7. Please explain. (3000 characters maximum)

Users of our platforms must follow basic rules of conduct, including rules against sexualisation of minors, harmful or dangerous acts involving minors, inflicting emotional distress, and cyberbullying and harassment. We provide mechanisms for users to report inappropriate content or behavior toward children, including for child endangerment.

We deter, detect and report child sexual exploitation and abuse material on Google products and have invested heavily in fighting these crimes, includying by:

- Developing new technology we share for free across industry and with NGOs. This includes CSAI Match and the Content Safety API, a prioritisation tool which enables faster detection of never-before identified CSAM. We report this content to the National Center for Missing and Exploited Children (NCMEC), which then sends reports to law enforcement agencies around the world.
- Working with external organisations, as part of our shared responsibility. Google was a founding member of the Technology Coalition, where specialist child safety experts across industry meet to ensure high-impact information, expertise and knowledge sharing.
- Responding to requests from government agencies, including law enforcement. Any request that relates to an urgent investigation is given the highest priority.

We also work to prevent our platforms from being used by those who may seek to endanger minors. On YouTube, in the first quarter of 2020, we removed nearly 1.5 million videos for violations of our child safety policies— and the majority of these before they had ten views. We also removed over 96 million comments from YouTube on child safety grounds, and suspended comments on hundreds of millions of videos featuring younger minors. We have expanded our efforts around limiting recommendations of borderline content to include videos featuring minors in risky situations.

In many countries, users who type queries associated with child sexual abuse terms into Google Search are shown deterrence ads or an in-depth search result at the top of their search results that make it clear that child sexual abuse and any material that pictures or promotes such actions is illegal. These messages also include links to trusted partners to report abusive behaviour or imagery and offers advice on where to get help.

We also build products for kids and families from the ground up to help parents support safer access for their children. Family Link helps parents stay in the loop as their child explores the internet on a compatible device. YouTube Kids provides a separate YouTube experience designed especially for children, that parents can control.

Finally, Google creates educational resources, working with parents, teachers and young people to encourage safe and responsible interactions online. Our flagship global educational program is Be Internet Awesome, designed by experts to empower children to use the web more safely and wisely. The program has reached millions of users across 16 countries.

C. Measures for protecting legal content goods and services

1. Does your organisation maintain an internal complaint and redress mechanism to your users for instances where their content might be erroneously removed, or their accounts blocked?
Yes | No

2. What action do you take when a user disputes the removal of their good or content or service, or restrictions on their account? Is the content/good reinstated? (5000 characters maximum)

On YouTube, we have a process for creators to clarify enforcement actions. For example, if a creator chooses to submit an appeal about a video removed under our Community Guidelines, it goes to human review, and the decision is either upheld or reversed. The creator receives a follow up email with the result. On Google Play, a published version of a removed application won't be available on Google Play until a compliant update is submitted. App developers can also file an appeal if they believe their application was removed in error, for our review and reinstatement if found to be in line with our policies and developer distribution agreement. With Google Ads, we allow advertisers to correct policy violations in some circumstances, depending on the policy violation, or to appeal the disapproval of an ad if an advertiser believes the ad has been rejected in error.

In areas like copyright law, we remove content from our services if a takedown notice is valid. On Search, for example, when we take action in response to a copyright notice, we make a notification available to the administrator of the affected site through Google's Search Console. Following our copyright removal process, a webmaster may issue a counter notification. We evaluate all counter notifications and decide whether or not to reinstate the content. If the copyright owner still believes the content is illegal, they still have an avenue through the court systems.

We detail below considerations for designing effective counter-notice systems to ensure effective decision-making, to prevent bad-faith or invalid appeals, and to protect the identity of users who flagged illegal content, where appropriate.

Are you aware of evidence on the scale and impact of erroneous removals of content, goods, services, or banning of accounts online? Are there particular experiences you could share? (5000 characters maximum)

Our removals process aims to strike a balance between making it easy and efficient for rightholders to report infringing content while also protecting free expression on the web.

Our YouTube Community Guidelines Transparency Report, which is updated quarterly, provides data on the appeals YouTube receives for Community Guidelines video removals. From January-March 2020, we received 165,941 requests for appeal, up 52% from the previous quarter; of those, 41,059 were reinstated, up 78% from the previous quarter. (The previous quarter, from October-December 2019, we received 106,587 requests for appeal; of those, 20,868 were reinstated.) The apparent increase in successful appeals during the COVID-19 outbreak may reflect the increased deployment of machine learning to tackle challenging content during that period, and thus reinforces the view that machine automation simply cannot replace human judgment.

In the area of copyright removals, we have received requests to remove critical product reviews on the grounds that the article includes a photograph of the (allegedly copyrighted) product; individuals copying critical news articles and back dating them to request the take down of the original article. We also receive overbroad take down requests from rightholders. An anti-piracy agent of a record label requested the removal of numerous homepages including those with "coffee" in their URL on the basis that the word "coffee" appeared in the titles of their client's works (Lumen entry here). Another agency issued requests against several articles discussing a music release, presumably because "download" appeared in the titles of the articles.

In the area of trade mark and counterfeit removals, we regularly receive requests from trade mark holders to remove authentic pre-owned products or lawful parallel imports; we see assertion of trade marks comprised of descriptive terms against content using those terms descriptively and in their

ordinary meaning; and we encounter attempts to remove content providing commentary or criticism of business practices on trade mark grounds. These and many other examples, if actioned, would interfere with valid commercial activity and expression.

Our system has been effective at significantly reducing access to infringing content, but there are bad actors who attempt to abuse this system and limit access to information, which is something we actively fight against. Over the years, we've continued to invest in new tools and establish processes like the Trusted Copyright Removal Program to tackle this issue at scale, while also developing new ways to counter abuse, which continues to evolve. On YouTube, we regularly review takedown requests and push back when complaints are incomplete, suspicious, or the content is legitimate or the take down requests are abusive. In 2019, YouTube addressed a particularly egregious abuse of the take down process and filed suit against an individual who fraudulently issued take down requests in an attempt to extort users for financial gain. Such examples demonstrate why it is important that the DSA brings greater rigor to the notice requirement, including attaching penalties for cases of bad faith.

3. What are the quality standards and control mechanism[s] you have in place for the automated detection or removal tools you are using for e.g. content, goods, services, user accounts or bots? (3000 characters maximum)

We continue to believe that automated technology should be used to support the decisions that human experts make. This is especially the case when the context of a piece of content determines whether it is in violation of our policies or local laws. Where there is reasonable doubt, content flagged by machines then passes to trained teams which evaluate it before taking action in order to ensure it actually violates our policies or local laws and to protect content that has an educational, documentary, scientific, or artistic purpose.

Detecting failures and repairing complex algorithms that may be producing negative or unfair effects is an open challenge in the field of computer science. We take seriously the risk that artificial intelligence could entrench existing inequalities around race, gender and sexuality, among other areas. That's why we are researching practical approaches to mitigate against these risks. This includes developing new tools and techniques to test our machine learning systems for unintended bias, including a What-If Tool that empowers developers to visualize biases, Fairness Indicators to check ML model performance against defined fairness metrics, and an ML Fairness Gym for building model simulations that explore the potential long-run impacts of ML-based decision systems in social environments. We correct mistakes when we find them and retrain the systems to be more accurate in the future.

We know that humans can also incorporate biases and preferences when making decisions, and our reviewers go through training and testing. We have continuous quality assurance programs in place to assess decisions and identify improvement opportunities. When such opportunities arise, the reviewers are coached, given additional training and are retested before resuming reviews.

An area of particular importance where we use a combination of machine learning and human reviewers is detection of illegal child sexual abuse material (CSAM). This abhorrent content has no place in our services and we take a number of voluntary proactive steps to detect and remove both known and not previously identified CSAM. We welcome the Commission's efforts to address the concerns that the changes to the implementation of the e-Privacy code will create, potentially limiting our ability to continue the important work we do in identifying known and new content. Any proposed solution needs to be technology neutral to ensure that the much needed innovation in this space is not curtailed.

4. Do you have an independent oversight mechanism in place for the enforcement of your content policies?
Yes | No

5. Please explain. (5000 characters maximum)

We are subject to independent assessments by the Global Network Initiative (GNI). In the latest assessment period — the GNI's third assessment of Google — the GNI Board determined that our company is making good-faith efforts to implement the GNI Principles on Freedom of Expression and Privacy with improvement over time.

Companies participating in the GNI are independently assessed periodically on their progress in implementing the GNI Principles, which are rooted in the rule of law and internationally recognised laws and standards for human rights. The independent assessments were conducted by assessors accredited by the GNI Board as meeting independence and competency criteria.

In addition, YouTube participates in the EU Code of Conduct on Countering Illegal Hate Speech Online. The Code requires services to have rules and community standards that prohibit hate speech and put in place systems and teams to review content that is reported to violate these standards. Implementation of the Code is evaluated through a regular monitoring exercise set up in collaboration with a network of organisations located in the different EU countries. Using a commonly agreed methodology, these organisations test how the IT companies are implementing the commitments in the Code. In the last monitoring round, evaluators found that YouTube assessed 81% of notifications from participating trusted flaggers within 24 hours.

Finally, we participated in the independent assessment of the EU Code of Practice against Disinformation, in supporting the European Commission's evaluation of the Code effectiveness.
The assessment of the independent contractor analysed the terms of service, policies, and tools adopted by online platforms to implement the commitments made in the Code in the first year of its implementation.

D. Transparency and cooperation

1. Do you actively provide the following information (multiple choice):

Information to users when their good or content is removed, blocked or demoted
Information to notice providers about the follow-up on their report
Information to buyers of a product which has then been removed as being illegal

2. Do you publish transparency reports on your content moderation policy?
Yes | No

3. Do the reports include information on:

Volumes of takedowns and account suspensions following enforcement of your terms of service?

Volumes of takedowns following a legality assessment?
Notices received from third parties?
Referrals from authorities for violations of your terms of service?
Removal requests from authorities for illegal activities?
Volumes of complaints against removal decisions?
Volumes of reinstated content?
Other, please specify in the text box below

4. Please explain. (5000 characters maximum)

Google is committed to providing a high level of transparency.

In 2010, we released the first online Transparency Report. Since then, we've developed new and improved ways of sharing information with users, including data that sheds light on how policies and removal actions affect privacy, security, and access to information online. Recently, for example, we announced a new feature called "About this ad," which will show users the verified name of the advertiser behind each ad. We have summarised the important events in the origin, development, and evolution of Google's Transparency Report here.

Our policies work best when users are aware of the rules and understand how we enforce them. That is why we work to make this information clear and easily available to all. We develop comprehensive help centers, community guidelines websites, and blog posts that detail the specific provisions of our policies. In addition, we regularly release reports that detail how we enforce those policies or review content reported to be in violation of local law.

- The YouTube Community Guidelines enforcement report contains data on actions YouTube takes with regard to content on the platform that violates our policies. This includes: flagging (human and automated); video, channel, and comment removals; appeals and reinstatements; and highlighted policy verticals. In 2019, more than 30 million videos were removed from YouTube for violating our Community Guidelines. Between April and June 2020, for example, YouTube removed over 11.4 million videos for violating our Community Guidelines. Of these, 95% were first flagged by machines rather than humans. Of those detected by machines, 53% never received a single view, and just over 81% received fewer than 10 views.
- Our annual Bad Ads Report outlines the scale of our work to enforce our advertising policies, including the number of ads that were removed, the number of pages that we stopped showing ads on, the number of advertiser and publisher accounts that were terminated throughout the year, and the number of updates we made to our policies over the course of the year.
- In 2019, in addition to 2.7 billion bad ads removed, we suspended nearly 1 million advertiser accounts for policy violations. On the publisher side, we terminated over 1.2 million accounts and removed ads from over 21 million web pages that are part of our publisher network for violating our policies.
- Google Play's policies prohibit numerous types of deceptive behaviors and misleading content, especially as they relate to the dissemination of apps concerning medicine or personal health. When developers are found to infringe these policies, their apps may be

removed from the Google Play store. Throughout 2019, Google Play stopped over 790,000 policy-violating apps before they were ever published to the Play store.

- In 2019, Google Maps detected and removed more than 75 million policy-violating reviews and 4 million fake business profiles, and took down more than 580,000 reviews and 258,000 business listings that were directly reported to us for violating our policies. We also reviewed and removed more than 10 million photos and 3 million videos that violated our content policies on Google Maps, and disabled more than 475,000 user accounts that were found to be abusive.
- Our transparency report on Germany's Network Enforcement Law (NetzDG) details how we evaluate content referred to us under NetzDG and under our own YouTube Community Guidelines. If the content violates our YouTube Community Guidelines we remove it globally. If the content does not fall under these policies, but we identify it as illegal according to one of the 21 statutes of the StGB to which NetzDG refers or any other local law, we locally block it.
- We provide a publicly accessible, searchable, and downloadable Google Transparency Report of election ad content and spending on our platforms. Given recent concerns and debates about political advertising, and the importance of shared trust in the democratic process, we hope to improve voters' confidence in the political ads they may see on our ad platforms.
- With the Political Ads Transparency Report in 2018, we launched our first ever election advertising transparency report and an accompanying creative library. For the EU, this includes ads that feature a political party, a current elected officeholder, a candidate for the EU Parliament, or an elected national office within an EU Member State, with country-level data for each Member State. It also includes ads that feature a referendum question up for vote, a referendum campaign group, or a call to vote related to a national referendum or a state or provincial referendum on sovereignty.

We will continue building on these transparency efforts, as they are an important component of ensuring an informed public dialogue about the role that our services play in society.

5. What information is available about the automated tools you use for identification of illegal content, goods or services and their performance, if applicable? Who has access to this information? In what formats? (5000 characters maximum)

In our YouTube Community Guidelines enforcement reports and on the site How YouTube Works, we explain how we use automated tools on YouTube. In addition, our transparency report on Germany's Network Enforcement Law (NetzDG) details how we use automated tools. As we detail elsewhere in this report, we must ensure new transparency requirements don't risk commercially-sensitive information, violate user privacy or data disclosure laws, nor allow bad actors to game our systems.

For the purpose of detecting child sexual abuse material (CSAM), we use a combination of automated tools and human reviewers. We make this cutting-edge technology available to other companies and NGOs to support the fight against CSAM. For example, CSAI Match is a first-of-its-kind fingerprinting and matching service that detects CSAM in video files. It builds on technology like PhotoDNA which can only be used for still images. This technology is unique in its resistance to manipulation and obfuscation of content, and it dramatically increases the number of violative videos that can be detected compared to previous methods. CSAI Match is used by companies and organisations like Adobe, Reddit, Tumblr, and Thorn amongst others. Other organisations are able to apply to use. Since this technology was publicly introduced in 2015, Google has voluntarily shared over 100,000 video hashes with industry (through NCMEC) to allow other companies to prevent the distribution of these videos on their platforms as well.

Content Safety API enables us to find and report new CSAM that was not possible using hash matching alone, and helps reviewers to find CSAM content seven times faster. We provide this technology for free to industry and NGO partners. The Content Safety API increases the capacity to prioritise and select content for review, thus expediting the identification of this content and reports, and enabling the review of abusive content in a way that requires fewer people to be exposed to it. Though automated systems have important limitations, as discussed further elsewhere in this submission, these tools have made an important impact. The image review classifier has enabled Google to find and report almost 100% more CSAM per year than would have been possible using hash matching alone.

6. How can data related to your digital service be accessed by third parties and under what conditions?

Contractual conditions
Special partnerships
Available APIs (application programming interfaces) for data access
Reported, aggregated information through reports
Portability at the request of users towards a different service
At the direct request of a competent authority
Regular reporting to a competent authority
Other means. Please specify

7. Please explain or give references for the different cases of data sharing and explain your policy on the different purposes for which data is shared. (5000 characters maximum)

Special Partnerships: We establish cross stakeholder partnerships for several issues and within this fora, share data in order to keep our platforms safe for online users. These partnerships include:

- The Global Internet Forum to Counter Terrrorism (GIFCT): This multi-stakeholder forum includes a wide range of companies, governments and civil society organisations committed to preventing terrorists and violent extremists from exploiting digital platforms. To enhance our collective efforts, we share hashes of known violent extremist and terrorist content through a ThreatExchange platform, including a hash-sharing database. The ThreatExchange platform is a structured API with privacy controls for organisations to share threat data.
- The Technology Coalition (TC): The Technology Coalition was formed in 2006 and comprises tech industry leaders who are represented by individuals who specialise in online child safety issues. The TC recently launched Project Protect, a global initiative with the aim of fostering industry collaboration on tech innovation, research, data transparency, information and knowledge sharing and collective action.
- CSAM datasharing with law enforcement through the National Center for Missing and Exploited Children: NCMEC: we report Child Sexual Abuse Material (CSAM) to NCMEC through CyberTipline and this in turn is shared with law enforcement agencies around the world. NCMEC makes CyberTipline reports available to more than 100 law enforcement agencies around the world through a Virtual Private Network (VPN) owned and operated by NCMEC.

- We are dedicated to following advertising regulations for ads related to healthcare and medicine. Google contracts with Legitscript, the leading expert in online pharmacies, to monitor pharmacy ads, and to reduce rogue pharmacy content on YouTube.

Regular Reporting to a Competent Authority: Google signed both the EU Code of conduct on countering illegal hate speech online and the The EU Code of Practise on Disinformation, which include monitoring mechanisms. To this end, we regularly provide data in aggregate to the EU through a network of collaborating organisations on our efforts to counter hate speech and disinformation online.

Lumen project: As part of our efforts to remain transparent, a copy of legal notices we receive may be sent to the Lumen project for publication with personal contact information redacted (you can view an example here). Lumen is an independent research project managed by the Berkman Klein Center for Internet & Society at Harvard Law School. The Lumen database houses millions of content takedown requests that have been voluntarily shared by various companies, including Google. Its purpose is to facilitate academic and industry research concerning the availability of online content.

E. Google's COVID-19 Efforts

Since the outbreak of COVID-19, teams across Google have launched over 200 new products, features and initiatives and are contributing over $1 billion in resources to help our users, clients, partners, and governments through this unprecedented time. Our major efforts are focused around: providing trusted information to our users, helping people adapt to a changing world, and contributing to recovery efforts across the globe.

Helping the world make sense of information during a health crisis requires a broad-based response, involving governments, health authorities, scientists, journalists, public figures, technology platforms and many others. Our efforts include:

- Offering $250 million in ad grants to help the World Health Organisation and more than 100 global government agencies (including $50 million to EU governments and agencies) provide critical information on how to prevent the spread of COVID-19 and other relief measures to local communities.
- Committing $50 million to the global COVID-19 response from Google.org, with a focus on health and humanitarian efforts, distance learning, and economic relief and recovery. This includes $8 million to support the WHO's critical work and a public matching campaign to match donations from the public.
- Supporting coronavirus fact-checking and verification efforts through more than $6.5 million in funding from the Google News Initiative to fact-checkers and nonprofits fighting misinformation around the world, with an immediate concentration on COVID-19. In addition, we're working to increase access to data, scientific expertise and fact checks through support for collaborative databases and providing insights to fact-checkers, reporters and health authorities including sharing localised data from Google Trends on COVID-19 down to the city level.
- Helping publishers deal with the challenges of reporting on COVID-19 through a new Journalism Emergency Relief Fund to deliver urgent aid to thousands of small, medium

and local news organisations globally. The funding ranges from thousands of dollars for small hyper-local newsrooms to tens of thousands for larger newsrooms, with variations per region. We also provided five months of ad fee relief to larger publishers using the Google Ads Manager during this period.

In the section below, we detail the trends we've observed on illegal and harmful content and activity related to COVID-19, and the actions we've taken.

In the course of the pandemic, we have prioritised providing trusted information to our users, to help keep them safe, informed, and connected during this rapidly evolving period of uncertainty. This has included amplifying authoritative voices, working directly with authorities such as the World Health Organisation to surface their messages across our platforms. Reflecting the exceptional nature of the crisis, we also took extraordinary efforts to surface authoritative content from national and local institutions, such as national health authorities, recognising the trust that citizens have in these local bodies. We've built a comprehensive Search experience and a dedicated website (google.com/covid19) to provide trusted information directly to those searching for answers around COVID-19 on the web. When users search for health-related topics on YouTube, they are presented with a health information panel at the top of the screen with information from authoritative sources such as the World Health Organisation.

In relation to illegal and harmful activities related to COVID-19, on YouTube we worked actively to remove policy violative content relating to COVID-19; reduce borderline content about COVID-19 (i.e., not violative, but in a gray area, including potentially harmful misinformation); and raise authoritative content from local and global health authorities on the YT homepage, through featured playlists, or as a video ad on YouTube at no cost to these organisations. From February to June 2020:

- We've reviewed over 2M videos related to dangerous or misleading coronavirus information.
- We've removed over 200K videos related to dangerous or misleading coronavirus information.
- While automated flagging systems are not a panacea, they continue to improve and were used to help address violative content in this context: of the removed videos on COVID-19 as of June, over 95% were first flagged through YouTube's automated flagging systems.
- YouTube's COVID-19 information panels delivered more than 300B impressions across search, watch page and home page and global watchtime on authoritative news content grew by more than 75% in the first three months of 2020.

To help people adapt to the changing world, we have also provided tools and resources to help businesses and organisations continue to function through lockdowns. We have dedicated particular attention to education, recognising the real risk that children may fall behind due to the absence of formal schooling. On YouTube, we launched Learn@Home, a website with learning resources and content for families. YouTube has also partnered with a vast range of artistic, cultural and religious institutions to ensure that EU culture can continue reaching large audiences. This included, for example, a YouTube-exclusive performance from opera singer, Andrea Bocelli, live from Milan's Duomo Cathedral, which has been viewed 41 million times. Following the cancellation of this year's Eurovision Song Contest, YouTube and the European

Broadcasting Union partnered to produce a two-part original series honouring the Eurovision 2020 songs and artists.

Looking to the future, we have pledged to help 10 million people and businesses in Europe, the Middle East and Africa benefit from digital before the end of 2021. In "Europe's Moment: Repair and Prepare for the Next Generation" the European Commission described the need for a "digital transition" which they described as "even more important now than before the crisis started." With some 60 million jobs said to be at risk across Europe today, we could not agree more. This is the moment to ensure that as economies recover, opportunities are distributed fairly and that no one is denied the opportunity to thrive after coronavirus for lack of the right technology.

Firstly, it is necessary to invest in people and their skills to achieve a sustainable, inclusive economic recovery. We launched Grow with Google with the goal of training one million Europeans in digital skills. Today we have trained over 70 million people around the world, including 14 million in EMEA, and during this period of Covid-related disruption, we saw a 300% increase in those taking part in our training programs. Now, we are paying for 100,000 Google professional certificates on the Coursera platform which are designed to lead to digital-based jobs.

The skills required to thrive after coronavirus need to be spread beyond just the biggest companies. Smaller businesses, after all, are the backbone of the European economy, accounting for 99% of all businesses and 85% of all new jobs on the continent. Because of that, Google has provided $340 million worth of free advertising to SMEs across the world, $1 billion to support nonprofits and we have made some of our most popular tools both more useful and accessible for small businesses. We made our premium video conferencing service, Google Meet, free for all to use. We made changes to tools like Search and Maps so that businesses could more easily update their customers about changes to their opening hours and other information, as well as making it easier to receive donations, sell gift cards and take orders online.

Now we are investing further to help businesses digitise faster, including enabling access to free tools and capital for underserved businesses. Where they are not already online, we are helping them build a digital presence. Then, with tools like Grow my Store and Google my Business - now updated with COVID-related information and insight - we are helping them find new customers online and we've added over 10 features to support businesses affected by COVID-19 since February.

Artificial intelligence (AI) also promises to be of great help. It offers the potential to transform how businesses reach new customers, how they increase their sales and how they become more efficient and profitable. That's why we support the European Commission's plans to channel recovery funding towards breakthrough digital technologies like AI. It is why we are now accelerating the launch of our own "AI for Business" tool: a new checkup tool which provides businesses with a customised report laying out the best applications of AI for them and practical suggestions on how to implement changes

We remain fundamentally optimistic about the future - about the role technology will have to help people, businesses and communities recover. Online tools have been a lifeline for people and businesses in lockdown and those tools can help people learn new skills and find new jobs.

But as our economies begin their recovery from coronavirus, the responsibility to ensure we can all thrive is shared. Governments, businesses and individuals must work together to help everyone benefit.

Illegal goods

10. What good practices can you point to in handling the availability of illegal goods online since the start of the COVID-19 outbreak? (5000 characters maximum)

Since the beginning of the COVID-19 outbreak, we've closely monitored advertiser behavior to protect users from ads looking to take advantage of the crisis.

We have a dedicated COVID-19 task force that's been working around the clock. They have built new detection technology and have also improved our existing enforcement systems to stop bad actors. These often come from sophisticated actors attempting to evade our enforcement systems with advanced tactics. These ads promoted products listed significantly above market price, misrepresented the product quality to trick people into making a purchase or were placed by merchants who never fulfilled the orders.

These concerted efforts are working. Over the past months, we've blocked or removed **over 200 million coronavirus-related ads globally**, including Shopping ads, for policy violations including price-gouging, capitalising on global medical supply shortages, fraudulent ads for in-demand products like face masks, and making misleading claims about cures. Of these, **over 68 million coronavirus-related ads blocked or removed were for EU-based advertisers.** We have also **suspended more than 1000 accounts from EU-based advertisers**, including Merchant accounts on Google Shopping, for trying to circumvent our systems, including for ads and offers related to COVID-19. More information about these policies can be found here.

Simultaneously, the coronavirus has become an important and enduring topic in everyday conversation and we're working on ways to allow advertisers across industries to share relevant updates with their audiences. We've specifically helped NGOs, governments, hospitals and healthcare providers run Public Service Announcement ads. For example YouTube's information panels from Health Authorities delivered more than 300 billions of impressions across search, watch pages and home-page from February to June 2020. We continue to take a measured approach to adjusting our enforcement to ensure that we are protecting users while prioritising critical information from trusted advertisers.

Since the start of the pandemic, we have also been working closely with Commissioner Reynders, the Commission's DG JUST and the CPC Network, exchanging intelligence and observations regarding the new trends and how we are addressing them.

Illegal content

18. How has the dissemination of illegal content changed since the outbreak of the COVID-19 pandemic? Please explain. (3000 characters maximum)

We saw a significant rise in online scams related to COVID-19. Common types of scams include:

- Falsely representing health organisations: Scammers posing as local health services or the WHO offering cures, tests or other COVID-19 information.
- Websites selling fraudulent products: Sites offering hand sanitiser, self-testing kits, face masks, or other in-demand products that never arrive.
- Posing as government sources: Scams claiming to issue updates and payments on behalf of the government.

- Fraudulent financial offers: Scammers posing as banks, investors or debt collectors, with offers designed to steal financial information.
- Fake charitable donation requests: Scammers requesting COVID-19 donations to charities, hospitals and local health services.

19. What good practices can you point to in handling the dissemination of illegal content online since the start of the COVID-19 outbreak? (3000 characters maximum)

We have doubled down on our efforts to protect users in response to the new and increased threats arising during the pandemic, developing our understanding of bad actors' evolving tactics and refining our processes for identifying them. Working with our partners in the European Commission and in Member State governments across Europe, we have also seen enhanced cooperation between relevant stakeholders on key issues. We believe this cooperative framework can present a model for tackling illegal content in future.

Detection and Removals: Hackers frequently look at crises as an opportunity and we see clear and exceptional spikes in unlawful activity when such crises occur, and COVID-19 is no different. Across Google products, we're seeing bad actors use COVID-related themes to create urgency so that people respond to phishing attacks and scams. Our security systems have detected examples ranging from fake solicitations for charities and NGOs, to messages that try to mimic employer communications to employees working from home, to websites posing as official government pages and public health agencies. Recently, our systems have detected 18 million malware and phishing Gmail messages per day related to COVID-19 (of the more than 100 million phishing emails that Gmail blocks every day), in addition to more than 240 million COVID-related daily spam messages. Our machine learning models have evolved to understand and filter these threats, and we continue to block more than 99.9 percent of spam, phishing and malware from reaching our users.

We use a combination of internal investigative tools, information sharing with industry partners and law enforcement, as well as leads and intelligence from third-party researchers. To help support this broader security researcher community, Google is providing more than $200,000 in grants as part of a new Vulnerability Research Grant COVID-19 fund for researchers.

Activities which could cause harm but are not, in themselves, illegal

4. In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of the COVID-19 pandemic? Please explain. (3000 characters maximum)

We have seen misinformation worldwide arising out of the pandemic, which our dedicated COVID-19 taskforce has been tracking since February. We have made tackling coronavirus-related misinformation a central priority of our response to the pandemic. This includes tackling false or unsubstantiated information about the origins of coronavirus, for example conspiracy theories that it was created in a lab to fulfill a specific social or political agenda. It also includes content that promotes medically unsubstantiated methods, including those that claim to prevent the coronavirus in place of seeking medical treatment, or explicitly disputes the efficacy of global or local health authority advice regarding social distancing that may lead people to act against that guidance.

Since the outbreak of COVID-19, our efforts have been focused on providing trusted information to our users, and helping our users, governments, YouTube creators and artists connect with each other and adapt to a changing world.

5. What good practices can you point to in handling such harmful activities since the start of the COVID-19 outbreak? (3000 characters maximum)

We are continuously working to ensure our products are serving users as they seek information about COVID-19. We have been:

- **Amplifying authoritative voices**, working directly with authorities such as the World Health Organisation to spread their messages across our platforms. We've built a comprehensive Search experience and a dedicated website (google.com/covid19).
- **Empowering authorities to disseminate their messages through** $250M in ad grants to the World Health Organization (WHO) and more than 100 government agencies globally, including $3 million in ad grants to the EU Commission and $1 million to the European Parliament.
- **Highlighting timely and trusted news and guidance across** Google News **and** YouTube**.** The results have been impressive. We have seen over 300 billion impressions on YouTube so far.

We're also providing information that helps people navigate a shifting world by:

- **Helping people find the resources they need**, from COVID-19 testing sites, shelters and food banks, virtual healthcare options, and unemployment benefits through Maps and Search.
- **Helping people understand changes in services**, from providing updated business hours and services available, as well urging those searching for medical help to call ahead, in Google Maps and Search.

Our policies and systems also help us address harmful activities:

- Our **Google Ads** policies do not allow ads that potentially capitalise on or lack reasonable sensitivity towards a sensitive event, and we began treating the COVID-19 crisis as a sensitive event all around the world, including in the EU, by the end of January 2020. We recently expanded our Ads policies to prohibit dangerous content about a health crisis that contradicts scientific consensus.
- When we highlight information on medical topics across Search, we strive to show information that reflects scientific consensus and evidence-based best practices.
- On **YouTube**, we clarified that we will ban videos that promote medically unsubstantiated methods. We have also worked to improve our machine learning detection and updated our YouTube recommendation systems to reduce recommendations of content that could misinform users, including around mortality and infection rates or conspiracy theories around the origin of COVID-19. (Note that overall consumption of borderline content or harmful misinformation is significantly below 1% of all consumption of content from recommendations.)
- We have refined our systems for identifying patterns of coordinated inauthentic behaviour, to take action to detect and remove coordinated and deliberate **disinformation**.

We are also partnering with global fact checking organizations through a $6.5M fund and supporting the creation of high-quality local news through the Google News Initiative's Journalism Emergency Relief Fund.

2. Clarifying responsibilities for online platforms and other services

1. What responsibilities should be legally required from online platforms and under what conditions?

Legend:

- A = Yes, by all online platforms, according to the activities they intermediate (e.g. content hosting, selling goods or services);
- B = Yes, only by larger online platforms;
- C = Yes, only platforms at particular risk of exposure to illegal activities by their users;
- D = Such measures should not be legally required

Maintain an effective 'notice and action' system for reporting illegal goods or content	**A**
Maintain a system for assessing the risk of exposure to illegal goods or content	**C**
Have content moderation teams, appropriately trained and resourced	**A**
Systematically respond to requests from law enforcement authorities	**A**
Cooperate with national authorities and law enforcement, in accordance with clear procedures	**A**
Cooperate with trusted organizations with proven expertise who can report illegal activities for fast analysis ('trusted flaggers')	**D**
Detect illegal content, goods or services	**D**
Request professional users to identify themselves clearly ('know your customer' policy)	**C**
Inform consumers when they become aware of product recalls or sales of illegal goods	**D**
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	**D**
Be transparent about their content policies, measures and their effects	**A**
Maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions	**A**
Other. Please specify	

2. Please elaborate, if you wish to further explain your choices. (5000 characters maximum)

In general, we recommend a **consistent set of rules for all market players**. We acknowledge that not all services have the same level of resources, but we believe that, to be truly effective, the regulatory regime must protect against illegal content migrating to less regulated platforms. This is not a theoretical risk. Analysts have observed, for example, terrorist groups targeting smaller platforms. And in 2019, 164 online companies submitted reports of child sexual abuse imagery to the National Center for Missing and Exploited Children.

However, regulation should not create undue burden for businesses, including for smaller companies. Today, the European Commission refers to "a large diversity of online platforms in Europe, with almost 10,000 high-growth SMEs." To ensure these platforms can rapidly scale while remaining safe for their users, we believe the core pillars of the current liability framework need to be maintained, alongside proportionate but effective notice-and-action rules that ensure platforms take responsibility for illegal content.

Cooperation with Law Enforcement: We appreciate that law enforcement agencies have legitimate interests in obtaining digital evidence to protect public safety. We receive law enforcement requests from all over the world, and we have a dedicated team that responds to them around the clock, every day of the year. We respond to over one hundred thousand such requests each year, and report on them in our Transparency Report. Our Law Enforcement Request System (LERS) allows a verified law enforcement agent to securely submit a legal request for user data, view the status of the submitted request, and download the response submitted by Google. We may also proactively contact relevant authorities if we become aware of an imminent threat to life and the immediate disclosure of user data could avert that threat, such as in missing persons cases or in suicide threats.

We also understand that the process for governments to obtain digital evidence can be cumbersome. That's why we support initiatives that make this process simpler but which maintain procedural safeguards. The European Commission's proposal for an Electronic Evidence ("e-Evidence") Regulation, if passed, would enable government authorities to obtain digital evidence from service providers, streamlining and harmonising the process without sacrificing privacy safeguards.

We remain concerned, however, with proposals that would circumvent existing legal protections or require internet service providers to disclose user data to the government without any prior oversight by an independent authority, due process and without proper safeguards. Such proposals would improperly shift the function of law enforcement investigation from government to private actors. Policymakers should give this careful consideration, and focus on meaningful reforms, including through passage of the EU's e-Evidence proposal.

Detect illegal content, goods or services. We do not believe that it is proportionate to introduce requirements aimed at the detection of illegal activity, which could amount to a de facto general monitoring obligation.

Know Your Customer policy: We recognise the desire for greater transparency around advertisements that run on our platforms. We announced a new advertiser identity verification initiative, which will require advertisers to complete a verification program in order to buy ads on our network. Advertisers will need to submit personal identification, business incorporation documents or other information that proves who they are and the country in which they operate. As this initiative is rolled out, users will start to see disclosures that list this information about the advertiser behind the ads they see.

Counter-notice: We write below about the ways to strengthen the notice system by introducing clear formalities. However, we note here that counter-notice systems may present challenges, and it is important to ensure that service providers do not become arbitrators or mediators between the original complainant and the content uploader. It is also important to remember that the design of a counter-notification system could lead to unforeseen problems. For example, it may risk the identity and anonymity of users who flagged illegal content during the course of a counter-notice procedure. The risks only increase when the user has flagged content posted by violent individuals or groups. In addition, to help protect against a flood of invalid counter-notices, any framework should require filers to make good faith validations or risk penalties for material misrepresentation. It should also draw sensible restrictions around who is eligible to submit a counter-notice — e.g., the content uploader affected by a removal.

While we have developed a **Trusted Flaggers program**, for example, by providing special tools to alert us to content that may violate our YouTube Community Guidelines, we think these relationships should be encouraged rather than mandated by law.

3. What information would be, in your view, necessary and sufficient for users and third parties to send to an online platform in order to notify an illegal activity (sales of illegal goods, offering of services or sharing illegal content) conducted by a user of the service?

Precise location: e.g. URL
Precise reason why the activity is considered illegal
Description of the activity
Identity of the person or organisation sending the notification. Please explain under what conditions such information is necessary
Other, please specify

4. Please explain. 3000 characters maximum)

Clear notice requirements would provide services with the legal clarity they need to operate, and for internet services to remain vibrant places for education, culture, and free speech.

The current system could be strengthened by introducing clear formalities for notice, and where appropriate, counter-notice. Formal notice should include, at minimum, requirements to:

- **Clearly identify the content at issue** by URL, video timestamp, or other unique identifier. Depending on the content at issue, this may also require a screenshot to identify the content (e.g., display of a particular advertisement on a web page).
- **State the law and basis of the legal claim**. This should set out the nature of the infringement and the law(s) being asserted, and the country in which the rights are being asserted. If the rights are registered, notice should specify the registration information (e.g., trade mark(s) at issue; countries of registration or use rights).
- **Clearly identify the sender of notice** where the nature of the rights asserted requires identification of the rightholder. Identification would require a full legal name and contact email address. Additional information, such as a physical address may be required if it is a business, in the context of complaints about advertising. In some cases, the relationship to the owner of the relevant legal right(s) is needed, e.g., for an agency or attorney acting on behalf of a rightsholder or unrelated third party. Proof of nationality may also be needed in some cases, for example, for certain data protection rights, which vary depending on the Member State.
- **Attest to the good faith and validity of the claim**, that the information contained in the notice is "true and correct," along with a statement attesting to the notifier's authority to submit a notice. This helps review teams process information more efficiently and responsibly, and penalties should attach to abuse by fraudulent or bad-faith notices.
- **Acknowledge rights impacted**: The notifier may need to submit a statement acknowledging that a copy of the notice may be sent to the original content creator.

It is important to keep a clear distinction between standardised notice forms regarding illegal content and the simple 'click to flag' buttons that allow users to highlight potential violations of our policies that does not require the detailed information set out above.

5. How should the reappearance of illegal content, goods or services be addressed, in your view? What approaches are effective and proportionate? (5000 characters maximum)

While we have voluntarily implemented tools for detecting the reappearance of specific types of illegal content, goods and services, we do not believe its use should be mandated. It would perversely incentivise companies to block lawful content to protect themselves from potential sanction, threatening legitimate speech and impacting the fundamental rights of European citizens. Moreover, it is not always precise, and can fail if the content is even only slightly modified.

Such an outcome would amount to a general monitoring obligation, which is duly prohibited by Article 15 of the e-Commerce Directive. The CJEU has noted the impact that general monitoring obligations could have on the freedom to receive and impart information, including by blocking lawful communications of users, and also on the freedom to conduct a business. Similarly, organisations dedicated to promoting and protecting fundamental rights and freedoms in the digital environment have stated that "general monitoring would undermine free expression and privacy by imposing ongoing and indiscriminate control of online content with mandatory use of technical filtering tools."

We believe that notice and takedown must remain the core legal standard.

6. Where automated tools are used for detection of illegal content, goods or services, what opportunities and risks does their use represent as regards different types of illegal activities and the specificities of the different types of tools? (3000 characters maximum)

We remain concerned about the risks to fundamental rights from mandated use of automation in content moderation. While breakthroughs in machine learning and other technology are impressive, the technology is far from perfect. Misclassification of content remains a challenge, and machine learning tools are vulnerable to adversarial examples, even based on tiny changes to images that are imperceptible to the human eye. In addition, such technology is still unable to discern differences in context that can be critical to determining whether content is legal or not. Consider a video of military conflict. In one context, the footage might be documentary evidence of atrocities in areas where journalists have great difficulty and danger accessing. In another context, the footage could be promotional material for an illegal organisation. Even a highly trained reviewer could have a hard time telling the difference, and machines are even more limited.

On **YouTube**, we use hashes to catch copies of known violative content before it is available to view. For some content, like child sexual abuse images (CSAI) and terrorist recruitment videos, we contribute to shared industry databases of hashes to increase the volume of content our machines can catch at upload. This generally works well when exact copies of, for example, the *exact* same terrorist propaganda video is re-uploaded. Otherwise it can be extremely challenging. As highlighted above, content that is illegal when uploaded by a terrorist organisation may be permissible when used as part of a news report. Not only that, when the content deviates even just slightly, it can be hard for automated tools to detect the content.

In the area of copyright, we have built a set of copyright management tools, including a €90 million investment in building YouTube's Content ID system. When a video is uploaded, it is compared to our database of millions of "fingerprints" corresponding to copyrighted works. Using the system, rightholders can be automatically notified of user-uploaded videos that contain their creative work and can choose in advance what they want to happen when those videos are detected: authorise the videos, block them, or monetise the videos by placing ads on them.

7. How should the spread of illegal goods, services or content across multiple platforms and services be addressed? Are there specific provisions necessary for addressing risks brought by: a. Digital services established outside of the Union? b. Sellers established outside of the Union, who reach EU consumers through online platforms? (3000 characters maximum)

We believe that, to be truly effective, the regulatory regime must protect against illegal content migrating to less regulated platforms by ensuring a consistent set of rules for all market players. Analysts have observed, for example, terrorist groups targeting smaller platforms, and we have been working within the industry to support smaller actors via the Global Internet Forum to Counter Terrorism.

Within the EU, another related problem is the spread of illegal goods, services or content across multiple Member States. A specific provision that can help in this regard is the country of origin principle, which is a cornerstone of the internal market and enables effective enforcement.

8. What would be appropriate and proportionate measures that digital services acting as online intermediaries, other than online platforms, should take – e.g. other types of hosting services, such as web hosts, or services deeper in the Internet stack, like cloud infrastructure services, content distribution services, DNS services, etc.? (5000 characters maximum)

What makes sense for content-sharing platforms may not be appropriate, or technically feasible, for a search engine, or a platform that hosts mobile apps.

Cloud providers are more limited in what they can do to address illegal content stored at the direction of their customers or their customers' users, given the technical architecture of their services designed with privacy protections and the contractual obligations they hold towards their customers' data. Cloud customers own their data and cloud providers process it based on their instructions. To expect the same as that requested of public-facing content sharing services not only is not technically feasible, it would also give rise to unjustified privacy, security, and commercial interferences. For example, it is often impossible for a cloud provider to remove individual pieces of content from a platform run by a customer, making it so that the only way a cloud provider could disable access to specific content is by disabling the entire project or platform.

In Section II we propose a way to update the harmonised, graduated, and conditional exemption scheme to reflect the nature of today's services. As part of that proposal, we suggest that digital infrastructure services, such as DNS services, would be required to meet equivalent conditions to the existing Article 12 to benefit from the liability exemptions. We also suggest that the DSA clarify that caching services includes search engine services, and should fall under a liability regime equivalent to the existing Article 13. Finally, we recommend a separate category of service for cloud providers, including software as a service ("SaaS") providers. Where a third party digital service provider uses a cloud provider, that third party should remain responsible for compliance with the law. Equally, where a third party business uses a SaaS provider and has authority and control over content, that third party should remain responsible for compliance with the law regarding that content.

Regulation must also ensure respect for user privacy, where users communicate privately or in small groups, and where they use anonymisation or pseudonymisation.

9. What should be [the] rights and responsibilities of other entities, such as authorities, or interested third-parties such as civil society organisations or equality bodies in contributing to tackle illegal activities online? (5000 characters maximum)

Tackling illegal content is a societal challenge, and we acknowledge the need for companies, governments and civil society to work together towards reaching our shared goals.

Policymakers must consider the full toolkit of approaches to address illegal activities and online harms, beyond just regulating platforms. In particular, we support efforts to increase resources for national authorities and law enforcement in taking direct action against users who violate the law. Governmental and law enforcement action is necessary to stop these users from engaging in illegal activities offline and online, and to prevent them from being able to create and share this content online in the first place.

In areas like illegal terrorist content and violent extremism, governments can complement civil society and private sector action by focusing resources on the offline networks that lead to indoctrination and recruitment; by ensuring they are making use of democratic processes to list/proscribe designated terrorist organisations and individuals; and by investing in programs that target social marginalisation. When it comes to counterfeit goods, EU authorities could also devote more resources to combatting manufacture where it occurs, as stronger measures to prevent production offline would help reduce their appearance online. Google will continue to support law enforcement and respond to valid legal requests for information.

We should also work to educate and equip users with the necessary tools to recognise and deal with a range of content challenges online. We continue to support community efforts, including through a €10m Google.org Impact Challenge on Safety to support organisations across Europe that are working on challenges related to hate, extremism, and child safety, both online and offline. By funding new and existing community projects across Europe, we hope to support initiatives to counter hate and extremism, and help young people to become confident digital citizens.

10. What would be, in your view, appropriate and proportionate measures for online platforms to take in relation to activities or content which might cause harm but are not necessarily illegal? (5000 characters maximum)

The Commission rightly notes, in its Inception Impact Assessment, that the Digital Services Act should "respect the important distinction" between illegal and lawful-but-harmful content. As the Center for Democracy & Technology has noted, "it is inconsistent with [human rights and rule-of-law] principles for governments to leverage private companies to limit speech that authorities cannot directly restrict." The European Court of Human Rights has confirmed that freedom of expression includes the right to "offend, shock or disturb." Handyside v. United Kingdom, 24 Eur. Ct. H.R. (ser. A) at 23 (1976). Finally, the changing nature of and norms around harmful content make it unsuitable for the liability regime. Misclassifying harmful content as illegal would subvert the legislative process and lead to a democratic deficit. Where Member States believe a category of content is sufficiently harmful, the Government may make that content illegal, through democratic processes and in a necessary and proportionate manner.

It is important to keep in mind that content that is appropriate on some sites may be inappropriate on others; what may be appropriate for some users may be inappropriate for others. Rather than dictating content policies, regulation could require that services come up with appropriate guidelines, publish them, enforce them, and offer users an opportunity to appeal.

We acknowledge and agree that transparency and empowering users must be central to any effective approach to addressing the spread of harmful content that protects fundamental rights. We are engaged in ongoing and evolving efforts to provide further, cross-industry transparency through self- and co-regulatory initiatives, including the Code of Practice on Disinformation and the Code of Conduct on Illegal Hate Speech. As an example of where transparency can make a difference, we have produced a Political Advertising Transparency Report for each EU Member State with granular data on who is paying for political advertising and how this is being targeted. The Audiovisual Media Services Directive also encourages the introduction of co-regulatory codes and collaboration between regulators and Video Sharing Platforms.

These efforts are continuing to evolve and build momentum, for example the newly established European Digital Media Observatory can serve as a platform for cooperation between online platforms and researchers to help develop a stronger shared understanding of and response to online disinformation. The Audiovisual Media Services Directive is still yet to be transposed in many Member States, and we would advise caution against imposing a new framework while existing frameworks have not been fully implemented and tested.

11. In particular, are there specific measures you would find appropriate and proportionate for online platforms to take in relation to potentially harmful activities or content concerning minors? Please explain. (3000 characters maximum)

We have a responsibility to help our users to be safe and responsible users of the internet. The internet offers important benefits for children, and efforts must ensure protection for their safety as well as their ability to access information, seize educational opportunities, communicate with friends or families, or gain access to culture and entertainment.
We believe it is important to maintain a degree of flexibility in the way that services are developed, to ensure that children are adequately protected without unintentionally curtailing their online access and digital development.

This balance can only be achieved if products are designed in a way that takes into account the needs of young users. We have led the way in designing products and tools that are designed with the interests of young people in mind. This includes the launch and development of the YouTube Kids platform, which provides a restricted version of YouTube for families with appropriate content for kids, built in timers for use, no public comments, easy flagging and a parent approved content mode. Our Family Link app lets parents set digital ground rules as their children learn, play, and explore online.

We've also heard from parents that it's difficult to dig through all the content available on Play and in response we have recently launched a new Kids tab on Google Play filled with "Teacher approved" apps that are both enriching and entertaining.

We help young people navigate the online world through our online resilience and digital literacy programs Be Internet Awesome, and we empower parents to keep their children safe through our Family Link and YouTube Kids apps, as discussed above.

12. Please rate the necessity of the following measures for addressing the spread of disinformation online. Please rate from 1 (not at all necessary) to 5 (very necessary) each option below.

Transparently inform consumers about political advertising and sponsored content, in particular during electoral periods	**5**
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with users' complaints	**4**
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives	**5**
Transparency tools and secure access to platforms' data for trusted researchers in order to monitor inappropriate behaviours and better understand the impact of disinformation and the policies designed to counter it	**3**
Transparency tools and secure access to platforms' data for authorities in order to monitor inappropriate behaviours and better understand the impact of disinformation and the policies designed to counter it	**3**
Adapted risk assessments and mitigation strategies undertaken by online platforms	**5**
Ensure effective access and visibility of a variety of authentic and professional journalistic sources	**3**
Auditing systems over platforms' actions and risk assessments	**2**
Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on manipulation and amplification of disinformation.	**2**
Other, please specify	

14. In special cases, where crises emerge and involve systemic threats to society, such as a health pandemic, and fast-spread of illegal and harmful activities online, what are, in your view, the appropriate cooperation mechanisms between digital services and authorities? (3000 characters maximum)

The coronavirus pandemic has provided an important model for enhanced cooperation between digital services and authorities in the event of a crisis. We offered $250M in ad grants to governments and health organisations. Through a joint effort with Apple, we helped governments and health agencies reduce the spread of COVID-19 through an exposure notification API, with user privacy and security core to the design. We also established regular dialogue between senior individuals at Google and political leaders and officials in the Commission and in EU Member State governments. We coordinated closely with the Commission's VP Jourová and DG Connect, and agreed to start providing monthly reports on our actions to promote authoritative content and counter harmful

disinformation. This type of voluntary cooperation, which was enabled by the Code of Practice on disinformation, is an efficient and desirable model for addressing similar issues.

As part of industry steps to implement the Christchurch Call, the Global Internet Forum to Counter Terrorism (GIFCT) developed the Content Incident Protocol (CIP) to assess and respond to the online proliferation of content produced by a perpetrator during the course of a real-world attack. GIFCT member companies have developed, refined and tested the protocol through workshops with Europol and the New Zealand government. To date, we have initiated the CIP assessment process nearly 80 times, and activated it twice in response to terrorist and violent extremist events across the world. The first CIP was activated on October 9, 2019, following the shooting in Halle, Germany when the perpetrator filmed his attack and copies of the original livestream circulated on non-GIFCT member platforms. The second CIP was activated on 21 May 2020, following a shooting in Arizona, U.S., due to the existence of an apparently perpetrator-filmed video depicting murder and attempted murder which spread onto GIFCT member companies' platforms. Ultimately, GIFCT shared hashes, or digital fingerprints, related to both incidents so that member companies could quickly detect and remove any instances of the content on their respective platforms.

We appreciate that law enforcement agencies have legitimate interests in obtaining digital evidence to protect public safety. We receive law enforcement requests from all over the world, and we have a dedicated team that responds to them around the clock, every day of the year. We may also proactively contact relevant authorities if we become aware of an imminent threat to life and the immediate disclosure of user data could avert that threat, such as in missing persons cases or in suicide threats. We would remain concerned, however, with proposals that would circumvent existing legal protections or require internet service providers to disclose user data to the government without any prior oversight by an independent authority and without proper safeguards.

Fundamental rights

A range of fundamental rights are affected by the regulation of intermediaries. This includes the freedom to conduct a business; the freedom of expression and freedom of thoughts; the freedom of the arts and sciences; the freedom to receive and impart information and ideas without interference by public authority, and regardless of frontiers; the right to an effective remedy; and protection of personal data and privacy.

We want to ensure our services remain a place where Europeans can exercise their freedom to receive and impart information— to learn, to share, to enjoy arts and culture, and to participate in democratic political debate.

15 & 16. What would be effective measures service providers should take, in your view, for protecting the freedom of expression of their users? Please explain. (3000 characters maximum)

Standing up for free expression means enabling access to lawful content that some people may find offensive, frivolous, or controversial. Doing so preserves citizens' rights to freedom of expression, and enables the free flow of information that is so essential to creativity and innovation.

The Council of Europe's Committee of Ministers issued recommendations on the roles and responsibilities of internet intermediaries. It made clear that the responsibility of intermediaries to

respect human rights and to employ adequate measures applies regardless of their size, sector, operational context, ownership structure, or nature. Among the recommendations for intermediaries, the Committee stressed the importance of terms of service that are publicly available in clear, plain language and accessible formats; of carefully assessing the human rights impact of automated content management, and to ensure human review where appropriate; and the importance of ensuring users have access to an effective remedy.

At Google, we have studied these recommendations carefully and assessed how our own services meet these standards. For example, we regularly review our machine learning systems to reduce the risk of unintended algorithmic bias in content moderation, and provide our users with comprehensive transparency reports providing an explanation of how we use technology to detect content in breach of our standards.

We remain concerned about regulation that would restrict the ability of services to maintain diligence in assessing content. We wrote above about the risks to fundamental rights from mandated use of automation in moderation. Here we also note **the risks to fundamental rights where companies are forced to prioritise speed of removal over careful decision-making**. We encounter many grey-area cases that require appropriate time to evaluate the law and context, and we remain concerned about recent laws that enable imposition of large penalties if short, fixed turn-around times are not met.

As the Commission has noted, such requirements could lead to "excessive content deletions." The French Constitutional Council recently ruled on France's Act to Combat Hateful Content on the Internet that "the short deadline given to operators to make such removal, in addition to the difficulty for them to determine whether or not statements are manifestly illicit, will prompt them to withdraw any content notified as potentially illicit." Ultimately, the Council said, the combination of short removal times and penalties "undermines freedom of expression and communication in a way that is not necessary, adapted, and proportionate." Any new standard should safeguard fundamental rights by ensuring an appropriate balance between speed and accuracy of removal.

17. Are there other concerns and mechanisms to address risks to other fundamental rights such as freedom of assembly, non-discrimination, gender equality, freedom to conduct a business, or rights of the child? How could these be addressed? (5000 characters maximum)

Yes.

The e-Commerce Directive has helped enable fundamental rights. Cornerstone principles such as the country-of-origin principle, the guarantee of the freedom of establishment, and the guarantee of freedom to provide digital services cross-border in the Union have all supported the **freedom to conduct a business**. It has led to the growth of a wide variety of online services and business models, and enabled businesses to provide services across borders without confronting internal barriers, fulfilling the original rationale of this fundamental freedom— to support free and unburdened economic initiative. These services have helped promote free expression, media pluralism, educational opportunities, creativity, culture, and the arts for users throughout the European Union.

We also note the risks to fundamental rights from barriers that constrain the **arts and scientific developments**. Article 13 of the Charter of Fundamental Rights of the European Union states that "the arts and scientific research shall be free of constraint," a right "deduced primarily from the right to freedom of thought and expression." The Commission should study the risks that barriers and constraints on digital services could limit scientific development, creativity, and contributions to and enjoyment of the arts by European citizens.

There is a risk that a mandate or over-reliance on automation could impact on different social groups more severely, where services do not have sufficient safeguards against issues such as algorithmic bias in place. This would create risks for the **fundamental right to non-discrimination.**

The UN Special Rapporteur's 2018 report to the United Nations Human Rights Council ("Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression") examines the regulation of user-general online content. The Special Rapporteur issued recommendations to States:

- States should repeal any law that criminalises or unduly restricts expression, online or offline.
- Smart regulation, not heavy-handed viewpoint-based regulation, should be the norm, focused on ensuring company transparency and remediation to enable the public to make choices about how and whether to engage in online forums.
- States should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy.
- States should refrain from imposing disproportionate sanctions, whether heavy fines or imprisonment, on Internet intermediaries, given their significant chilling effect on freedom of expression.
- States and intergovernmental organisations should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship.
- States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression. They should avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users.
- States should publish detailed transparency reports on all content-related requests issued to intermediaries and involve genuine public input in all regulatory considerations.

The Council of Europe's Committee of Ministers recommendations on the roles and responsibilities of internet intermediaries also included a set of guidelines for States. It noted the State's duty to protect human rights and also the responsibility of intermediaries to respect human rights, reinforcing the importance of rule of law and due process. Among its guidelines, the Committee wrote that:

- State authorities should **obtain an order by a judicial authority or other independent administrative authority,** whose decisions are subject to judicial review, when demanding intermediaries to restrict access to content;
- States should **make available, publicly and in a regular manner**, comprehensive information on the number, nature and legal basis of **content restrictions or disclosures of personal data that they have applied** in a certain period through requests addressed to intermediaries.

The Committee also cautioned that **disproportionate sanctions would likely lead to the restriction of lawful content and to have a chilling effect on the right to freedom of expression**.

18. In your view, what information should online platforms make available in relation to their policy and measures taken with regards to content and goods offered by their users? Please elaborate, with regards to the identification of illegal content and goods, removal, blocking or demotion of content or goods offered, complaints mechanisms and reinstatement, the format

and frequency of such information, and who can access the information. (5000 characters maximum)

We believe it important to have clear policies that explain what our users can and cannot do, so that everyone plays by the same rules. In accordance with the Platform to Business Regulation that came into force in July, we maintain clear rules which outline what types of content and behaviors are acceptable for each product or service. Known as content policies or Community Guidelines, we aim to make them clear and easily accessible to all users and content creators.

For each product and service, we tailor these policies to strike an appropriate balance between providing access to a diversity of voices and limiting harmful content and behaviors. These rules of the road articulate the purpose and intended use of a given product or service and represent a crucial part of what makes that product unique. They also explain what types of content and behaviors are not allowed, and the process by which a piece of content, or its creator, may be removed from the service. We want to make it easy for good-faith actors to understand and abide by our rules, while making it challenging for bad actors to flout them.

Our policies work best when users are aware of the rules and understand how we enforce them. **That is why we work to make this information clear and easily available to all.** We develop comprehensive help centers and blog posts that detail the specific provisions of our policies. We recently launched a site, How YouTube Works, to explain what we're doing to foster a responsible platform that the users, creators and artists who make up our community can rely on. In addition, we regularly release reports that detail how we enforce those policies or review content reported to be in violation of local law.

Sometimes we make mistakes in our decisions on how we enforce our policies, which may result in the unwarranted removal of content from our services. That is why creators have the opportunity to appeal that decision. For example, if a YouTube creator's channel receives a strike, we will send an email, notifications on mobile and desktop, and an alert in the creator's channel settings. We inform the creator that they have 30 days after the warning or strike was issued to appeal. Based on this experience, we would welcome the opportunity to participate in discussions on how similar mechanisms in the DSA can remain flexible and accessible for users.

As discussed in the section on notice formalities, we believe it is important to **keep a clear distinction between standardised notice forms regarding illegal content and the simple 'click to flag' buttons that allow users to highlight potential violations of our Community Guidelines**, which do not require the same level of detailed information or identification.

Finally, we want our users to have the best possible experience while they're using our services. While regulatory oversight can set out the minimum standards, it should leave room for services to be able to design and implement user-friendly experiences to achieve them. A one-size-fits-all approach would create confusion for our users and limit the effectiveness of flagging, notification, and enforcement systems.

19. What type of information should be shared with users and/or competent authorities and other third parties such as trusted researchers with regard to the use of automated systems used by online platforms to detect, remove and/or block illegal content, goods, or user accounts? (5000 characters maximum)

Our transparency reports provide detailed insights into our efforts to remove illegal content. As detailed elsewhere, we must ensure new transparency requirements do not violate user privacy or data disclosure laws, nor allow bad actors to game our systems. This would undermine our efforts to

keep users safe and protect the integrity of our platforms. Exposing the code, even if just to a small group in a controlled setting, magnifies security risks, such as hacking and fraud, through gaming the system.

20. In your view, what measures are necessary with regard to algorithmic recommender systems used by online platforms? (5000 characters maximum)

We believe it is important to give our users a helpful sense of what data is used for what purposes and how, and an understanding of how the algorithm works in organising and prioritising content for them. We recognise that users are seeking more transparency and control over their online experience, including the role of algorithms, and we have developed a number of tools for users.

Challenges

We acknowledge the desire of the Commission and others to provide users with transparency over why they are being recommended certain content. We are willing to be a constructive participant in dialogue over practical mechanisms that provide meaningful transparency to users, while avoiding the risks of poorly designed requirements. In particular,
we must ensure new transparency requirements do not risk commercially-sensitive information, violate user privacy or data disclosure laws, nor allow bad actors to game our systems.

We have seen before that opening up our systems too far allows bad actors to game our systems through manipulation, spam, fraud and other forms of abuse. It's a daily challenge. We learned this lesson the hard way. Back in 1999, Google's founders published a seminal paper on PageRank, a key innovation in Google's algorithm. Once that paper was published, spammers tried to game Google by paying each other for links.

Algorithmic transparency in the form of disclosure of raw code and data raises a number of risks, including the possible disclosure of commercially-sensitive information and undermining our efforts to keep users safe and protect the integrity of our platforms. Exposing the code, even if just to a small group in a controlled setting, magnifies security risks, such as hacking and fraud, through gaming the system. There is a real risk that transparency could end up harming consumers and citizens more than helping them, making systems less safe and harder to protect. It would also fail to meet the goals of bringing meaningful insight about the systems, as disclosing code or data in its raw form — complex computer instructions and technical detail — would not allow for adequate understanding.

Any requirements for algorithmic transparency should go through consultation with companies and experts, to ensure such measures are effective, lawful, respectful of privacy, and do not compromise commercially-sensitive information or risk opening up algorithms for abuse.

Resources

Our How Search Works site provides extensive information to anyone interested in learning more about how Google Search works. The site includes information about how we improve search quality and our approach to algorithmic ranking, including publication of our Search Quality Rater Guidelines which define our goals for Search algorithms. We also work hard to inform website owners in advance of significant, actionable changes to our Search algorithms and provide extensive tools and tips to empower webmasters to manage their Search presence - including interactive websites, videos, starter guides, frequent blog posts, users forums and live expert support.

For many years Google has offered a feature called Why this ad, where users can get more information on some of the factors that were used to select the ad for them, or choose to stop seeing that ad. There are over 15 million user interactions per day with Why this ad.

We have recently rolled out a new site How YouTube Works, where users can find information on our recommendations systems. Recommendations help users discover more of the videos that they love, whether it's a great new recipe to try or a new song. We share recommendations both on YouTube's homepage and in the 'Up next' section. We're constantly testing, learning and adjusting to recommend videos that are relevant to our users. We take into account many signals, including watch and search history (if enabled) as well as the channels to which users are subscribed. We also consider context, such as the user's country and time of day, to for example, help us show users locally relevant news.

Another factor that YouTube's recommendation systems consider is whether others who clicked on the same video watched it to completion – a sign that the video is higher quality or enjoyable – or just clicked on it and shortly after starting to view the video, clicked away. We also ask users directly about their experience with individual videos and our recommendation systems using random surveys that appear on their homepage and elsewhere throughout the app. We use this direct feedback to fine-tune and improve these systems for all users.

We are also exploring new ways to give users even more control over what they are seeing online. On YouTube, users can choose topics that users are interested in (such as 'Travel' or 'Science'), to guide what is recommended to that user. It is also possible to directly request 'Don't recommend channel' to ensure that videos from specific channels do not show again in users' recommendations.

22. Please explain. What would be the benefits? What would be concerns for the companies, consumers or other third parties? (5000 characters maximum)

As we set out above, law enforcement agencies have legitimate interests in obtaining digital evidence to protect public safety and we support initiatives that make this process simpler while maintaining procedural safeguards. The European Commission's proposal for an electronic evidence ("e-evidence") regulation, if passed, would enable government authorities to obtain digital evidence from service providers, streamlining and harmonizing the process without sacrificing privacy safeguards.

As we also set out above, we remain concerned about proposals that would circumvent existing legal protections or require internet service providers to disclose user data to the government without any prior oversight by an independent authority and without proper safeguards. Such proposals would improperly shift the function of law enforcement investigation from government to private actors. Any data disclosure for the supervisory purposes identified should align with and not reduce the level of protection provided for in the e-evidence regulation.

In terms of voluntary disclosure, we would also be concerned about new data sharing obligations that would impede existing practices, in particular for companies that already voluntarily refer information where there are imminent threats to life.

We welcome the Commission's efforts in this area and remain dedicated to discovering ways how we can better share insights with researchers and authorities within the privacy legal framework on a voluntary basis. We believe the newly established European Digital Media Observatory can serve as a platform for cooperation between online platforms and researchers.

23. What types of sanctions would be effective, dissuasive and proportionate for online platforms which systematically fail to comply with their obligations (See also the last module of the consultation)? (5000 characters maximum)

Most online platforms will have user experience and well-being at the center of what they do and will, therefore, already be incentivised to put in place robust compliance programmes to meet their obligations.

If it is deemed necessary to use the threat of sanctions in order to encourage compliance, then such sanctions should be proportionate and limited to cases of sustained failure to comply with the obligations. The sanctions framework should not be one that is likely to lead to the restriction of lawful content, nor should it have a chilling effect on the right to freedom of expression.

Jump to overview for this section

Part II. Reviewing the Liability Regime of Digital Services Acting as Intermediaries

The current legal framework has supported innovation from companies throughout Europe, and allowed users throughout the EU to benefit from those services. We also acknowledge that regulatory changes may be needed in light of the digital transformation of the last two decades. As such changes are considered, we must be careful to not unravel the benefits the current framework has delivered.

Online intermediaries have been able to generate value for businesses and consumers across Europe because of the legal certainty provided by the limited liability regime in the e-Commerce Directive. Legal certainty enables innovative technologies and business models to grow, and it will be instrumental to the EU's ambitions to encourage the scaling up of European digital companies able to compete on a global scale in the coming decades.

The liability regime should continue to be graduated, reflecting the degree of knowledge and control that intermediaries have regarding content on their services. It should be based on notice and takedown of illegal content, prohibit general monitoring requirements, incentivize additional action, and retain the country of origin principle.

The updated liability regime should continue to take into account the fundamentally different roles played by different online service providers and platforms. It is critical to avoid an overly broad and indiscriminate approach. For example, what makes sense for content-sharing

platforms may not be appropriate or technically feasible for a search engine or for a platform that hosts mobile apps. Regulation should also ensure respect for user privacy, where users communicate one-on-one or in small groups, and where they use anonymization or pseudonymization.

1. How important is the harmonised liability exemption for users' illegal activities or information for the development of your company?

Please rate from 1 star (not important) to 5 stars (very important)	★★★★★

2. The liability regime for online intermediaries is primarily established in the e-Commerce Directive, which distinguishes between different types of services: so called 'mere conduits', 'caching services', and 'hosting services'. In your understanding, are these categories sufficiently clear and complete for characterising and regulating today's digital intermediary services? Please explain. (5000 characters maximum)

A harmonized, graduated, and conditional exemption scheme continues to be needed as a foundational principle of the internet. This principle, however, needs to be updated and reinforced to reflect the nature of today's services. The current three-level system - of mere conduit, caching and hosting service - needs to be expanded to include explicitly other services. In some cases, the conditions for services to benefit from a liability exemption should be expanded, as set out below.

Digital infrastructure services: it should be clarified that Article 12's "mere conduit" category encompasses services such as domain name services, in addition to services consisting of the transmission in a network of information provided by a user of the service, or the provision of access to a network. Such services would still be required to meet equivalent conditions to the existing Article 12 to benefit from the liability exemptions.

Search engines: As correctly noted by Advocate General Maduro (in C-236/08 to C-238/08), the nature of a search engine service is such that it most logically falls under the e-Commerce Directive's Article 13 for caching services. Similar to search engines, which are indexes of the web at large, caching services are defined as those consisting of the automatic and intermediate storage of information hosted by a third party, where the information stored is updated to reflect updates to the information hosted by the third party. The services are performed to make the onward transmission of that information to users of the service more efficient upon request. The Digital Services Act should codify this understanding, and make clear that caching services, including search engine services, should fall under a liability regime equivalent to the existing Article 13, without prejudice to recent EU legislative developments such as the General Data Protection Regulation.

Cloud providers are limited in what they can do to address illegal content stored at the direction of their customers or their customers' users, given the technical architecture of their services, privacy protections, and the contractual obligations they hold towards their customers' data. Cloud customers own their data and cloud providers process it based on their instructions. To expect the same of cloud providers as of public-facing content sharing services is not only technically infeasible, it would also give rise to unjustified privacy, security, and commercial interferences. For example, it is often impossible for a cloud provider to remove individual pieces of content from a platform run by a customer, such that the only way a cloud provider could disable access to specific content is by disabling the entire project or platform. An overbroad obligation imposed on cloud service providers could lead to their business customers having their entire online presence terminated as the result of an allegation of unlawful content somewhere on their site.

We believe cloud providers, including software as a service ("SaaS") providers, should fall into a separate category of service. This would reflect the reality that factually and contractually, such providers do not have the requisite authority and control over content such that they should have responsibility for removing specific content from a third party's service.

Where a third party digital service provider uses a cloud provider, that third party should remain responsible for compliance with the law. Equally, where a third party business uses a SaaS provider and has authority and control over content, that third party should remain responsible for compliance with the law regarding that content.

Platform services: As discussed below, we would recommend moving away from the distinction in some case law between "active" and "passive" hosts, which has created significant uncertainty and liability risk for common features of current services. It should be clear that hosting services can continue to benefit from a limitation of liability, by retaining the requirement in Article 14 of the e-Commerce Directive for services to act expeditiously, upon obtaining actual knowledge of illegal activities, to remove or to disable access to the information concerned. We remain concerned about the risks to fundamental rights where companies are forced to prioritize speed of removal over careful decision-making and where staydown obligations are proposed. We have also cautioned about the limits of technology, and the risks of mandating use of detection tools. To the extent some hosts are expected to go beyond notice and takedown of specifically identified illegal material, we believe any requirement be limited to best efforts for identical copies of content that was previously notified in an adequately substantiated manner. We would remain concerned about any requirement that would require general monitoring to implement.

3. Are there elements that require further legal clarification? (5000 characters maximum)

As noted, the liability regime should continue to be based around clearly defined, and clearly notified, illegal content. As the Commission noted in its 2017 Communication, "a more aligned approach would make the fight against illegal content more effective...It would also benefit the development of the Digital Single Market and reduce the cost of compliance with a multitude of rules for online platforms, including new entrants." Precise notice is essential, not least because Member States define illegal content in a variety of ways.

4. Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected. (5000 characters maximum)

Yes.

Today, an intermediary that engages in such voluntary moderation risks being labelled as an "active" service provider, or otherwise being deemed to have knowledge of all of the content on its platform. This current risk of liability creates a perverse incentive for intermediaries to either refrain from engaging in reasonable proactive moderation, or to over-remove content in the course of moderating.

The current prohibition on imposing general monitoring obligations does not mean that intermediaries should not take reasonable steps to voluntarily moderate the content on their platforms, with the aim of removing harmful material.

Through the Digital Services Act, intermediaries can be incentivized to engage in the responsible use of voluntary actions for content moderation, above and beyond what is required by legislation. For

example, an intermediary should be able to voluntarily review content in respect of one type of unlawfulness (e.g., illegal terrorist content) without being deemed to have knowledge of all of the other potential ways in which that same content might be unlawful (e.g., defamation).

This would not free online services from their wider responsibilities within the new regulatory framework. Ultimately, a regulatory framework can clearly lay out responsibilities under a notice & action system and further incentivize online service providers to take additional action against unlawful content and activity on their services, in a manner that preserves the foundational legal principles of the open internet.

5. Do you think that the concept characterising intermediary service providers as playing a role of a 'mere technical, automatic and passive nature' in the transmission of information (recital 42 of the e-Commerce Directive) is sufficiently clear and still valid? Please explain. (5000 characters maximum)

No.

The concept set out in Recital 42 of the e-Commerce Directive, which, as noted in the Institute of Information Law's 2019 report on Hosting Intermediary Services and Illegal Content Online (pg 31), was arguably meant only in reference to Articles 12 (mere conduit) and 13 (caching), has led to confusion and misinterpretation. The unhelpful distinction in some case law between "active" and "passive" hosts creates significant uncertainty and liability risk for common features of current services. Member State courts have not reached consensus on what this distinction means in practice and which services are, or are not, "active". This is perhaps unsurprising given that the active vs. passive distinction has distracted from the central question of whether the host has actual knowledge or awareness relating to the specific information or activity in issue.

The recent Advocate General Opinion in joined cases Peterson vs. YouTube (C-682/18) and Elsevier vs. Cyando (C-683/18) provides welcome guidance in this area and reaffirms the correct 'knowledge or awareness' test for applying Article 14 of the e-Commerce Directive. In particular, AG Saugmandsgaard highlights that "Optimising access to the content should not, in particular, be confused with optimising the content itself." (Para 83). Optimising access to information, which includes providing in-product search functions, or categorising information, or providing automated recommendations, does not give a host knowledge of the content of that information. Only when a host acquires "intellectual control" of the information, and hence "appropriates" that information can it be said to be playing an active role sufficient to give it the appropriate level of knowledge or awareness (e.g., Para 152). Equally, in general, the appropriate level of knowledge or awareness must be knowledge or awareness of the specific unlawful information in issue, not general and abstract knowledge or awareness (e.g., Para 171-172).

It should also be noted that the Advocate General shares the view that where a hosting provider carries out certain proactive "checks, such as those made by YouTube via Content ID, to detect the presence of illegal information on its servers" this should not be sufficient to cause the provider to be considered to play an "active role" in relation to the stored information (Para 166).

We believe the Digital Services Act should move away from the unclear concept of "active" and "passive" hosts, and replace it with more appropriate concepts reflecting the technical reality of today's services, building instead on notions such as actual knowledge or awareness, and the degree of control.

6. The E-commerce Directive also prohibits Member States from imposing on intermediary service providers general monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users. In your view, is this approach, balancing risks to different rights and policy objectives, still appropriate today? Is there further clarity needed as to the parameters for 'general monitoring obligations'? Please explain. (5000 characters maximum)

Yes, this approach remains not only appropriate, but also vital.

We wrote in our submission to the Commission's Inception Impact Assessment about the ways that fundamental rights are respected by maintaining the prohibition on general monitoring obligations. As noted by organizations dedicated to promoting and protecting fundamental rights and freedoms in the digital environment, "general monitoring would undermine free expression and privacy by imposing ongoing and indiscriminate control of online content with mandatory use of technical filtering tools."

We believe there is an important distinction between the voluntary actions that services take to detect and remove content, and a broad requirement to apply monitoring, reinforced with sanctions. At Google, we recognize the benefits and limitations of automated tools, and apply a range of safeguards, for example flagging content for human review where the context of content could determine its legality. A legal requirement to apply such tools risks incentivising companies towards prioritizing removal over accuracy, and could effectively amount to an obligation to screen all content. Joris van Hoboken and Daphne Keller have written about the concern that when platforms have to review and face over-removal incentives for every word users post, "the number of unnecessary takedowns can be expected to rise."

We remain concerned about provisions designed to prevent future infringements, which often amount to de facto general monitoring obligations. The concern is even more acute for vague notions of a duty of care on platforms not to harm users, which would mean a service would have to check all the content on a platform and assess that content in light of all laws and rights. Van Hoboken and Keller identify the concern that general monitoring obligations "may also give platforms reason to allow only approved, pre-screened speakers". With over 500 hours of video uploaded to YouTube every minute, hundreds of trillions of pages on the Web, and hundreds of new web pages published every second, it is not hard to imagine how general monitoring requirements that encourage editorial control, over caching sites or hosting content on an open platform, would undermine the right to protection of personal data, the freedom to receive or impart information and the freedom to conduct a business.

Jump to overview for this section

Part III. What Issues Derive from the Gatekeeper Power of Digital Platforms?

1. To what extent do you agree with the following statements?

	Fully agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Fully disagree	I don't know/No reply
Consumers have sufficient choices and alternatives to the offerings from online platforms.			x			
It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies ("multi-home").			x			
It is easy for individuals to port their data in a useful manner to alternative service providers outside of an online platform.			x			
There is sufficient level of interoperability between services of different online platform companies.			x			
There is an asymmetry of information between the knowledge of online platforms about consumers, which enables them to target them with commercial offers, and the knowledge of consumers about			x			

market conditions.						
It is easy for innovative SME online platforms to expand or enter the market.			x			
Traditional businesses are increasingly dependent on a limited number of very large online platforms.			x			
There are imbalances in the bargaining power between these online platforms and their business users.			x			
Businesses and consumers interacting with these online platforms are often asked to accept unfavourable conditions and clauses in the terms of use/contract with the online platforms.			x			
Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers).			x			
Large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital)			x			

to expand into other activities.						
When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from smaller innovative market operators.			x			

Main features of gatekeeper online platform companies and the main criteria for assessing their economic power

1. Which characteristics are relevant in determining the gatekeeper role of large online platform companies? Please rate each criterion identified below from 1 (not relevant) to 5 (very relevant):

Large user base	★★★
Wide geographic coverage in the EU	★★★
They capture a large share of total revenue of the market you are active/of a sector	★★★
Impact on a certain sector	★★★
They build on and exploit strong network effects	★★★
They leverage their assets for entering new areas of activity	★★★
They raise barriers to entry for competitors	★★★
They accumulate valuable and diverse data and information	★★★
There are very few, if any, alternative services available on the market	★★★
Lock-in of users/consumers	★★★

Other	★★★

2. If you replied "other", please list *3000 character(s) maximum*

When assessing the factors that determine whether an online platform should be designated as a gatekeeper, it is important that the Commission does not rely on individual factors in isolation. For example, a "large user base" on its own is not indicative of economic power where users multi-home, barriers to entry are low, or where multiple platforms compete for user attention. Similarly, almost any company that operates in more than one market will (by definition) "leverage assets [to enter] new areas of activity", including assets such as pre-existing partner relationships, technical knowledge, understanding of customer preferences, and financial resources (*e.g.*, a ridesharing company will likely have relevant experience and expertise for food delivery). Incorporating particular services into a platform's offering, such as search engines, app stores, and ads intermediation says little about the strength of the platform unless it can and does leverage in specific anti-competitive ways between these different services. The ability to leverage assets from one market to another alone should not be indicative of gatekeeper status.

Gatekeeper designations appear to focus on consideration of three factors: market power, gateway functionality, and dependency. We believe further guidance could be helpful in providing a more rigorous understanding of these three criteria. Firstly, The UK CMA's investigation into online auction platform services has found that a range of different types of platform could have market power in different circumstances *vis-à-vis* different platform participants, which should be reflected in the gatekeeper assessment. Secondly, platforms operating a range of different business models might be said to act as gateways for businesses to reach consumers. Large smartphone manufacturers, for example, determine how users engage with particular apps or services. Vertical search services — not only general search services — can also act as important gateways (online travel agencies are likely to be significant sources of business for airline and hotel bookings). Thirdly, on economic dependence, the gatekeeper assessment should take into account that all platforms through which a materially significant proportion of business (e.g. in the form of highly valuable traffic) is channeled ought to be treated as satisfying this criterion.

In determining the appropriate criteria for gatekeeper assessments and designations, we think four principles ought to be considered. First, gatekeeper designations should be business model agnostic. Second, gatekeeper assessments should be reviewed periodically. Third, gatekeeper designations should apply to identified activities in specific markets. Fourth, some rules ought to apply on a sector-wide basis.

We expand on this response in the accompanying paper uploaded in response to this consultation.

3. Please explain your answer. How could different criteria be combined to accurately identify large online platform companies with gatekeeper role?

3000 character(s) maximum

We believe that any gatekeeper designations should be applied in a way that minimizes the potential harms from asymmetric regulation (*i.e.*, the risk of distorting competition and exposing consumers to harm from players falling in and out of scope of new rules based on arbitrary and/or outdated designations). In particular, the criteria for identifying 'gatekeeper power' should be independent of the particular business model that a platform uses, making no distinction as between platforms that operate business models based on advertising, subscriptions, sales commissions, or sales of hardware.

Gatekeeper designations appear to focus on consideration of three factors: market power, gateway functionality, and dependency. We set out some initial suggestions on how these criteria could be further defined and made more rigorous in our response to Q2. If gatekeeper designations are based on such factors, the Commission would need to ensure that there is clear guidance for firms, and consistent application of these factors across varying contexts and business models.

We expand on this response in the accompanying paper uploaded in response to this consultation.

4. Do you believe that the integration of any or all of the following activities within a single company can strengthen the gatekeeper role of large online platform companies ('conglomerate effect')? Please select the activities you consider to strengthen the gatekeeper role:

online intermediation services (i.e. consumer-facing online platforms such as e-commerce marketplaces, social media, mobile app stores, etc., as per Regulation (EU) 2019/1150 - see glossary)
search engines
operating systems for smart devices
consumer reviews on large online platforms
network and/or data infrastructure/cloud services digital identity services
payment services (or other financial services) physical logistics such as product fulfilment services data management platforms
online advertising intermediation services
Other - please list

1000 character(s) maximum

Gatekeeper designations should apply to identified business activities in specific markets within a corporate group. Large digital platforms tend to operate across multiple markets and sectors, with varying degrees of competitive strength in each. In certain sectors, the platform may have market power; in others, it may be a new entrant or marginal player (and may even struggle to compete and subsequently leave the market). Conversely, companies with a smaller market capitalization may nonetheless hold market power in particular markets where they operate. Accordingly, gatekeeper designations ought to be evaluated by reference to specific business activities in specific markets; not by reference to the position of the entire company or corporate group.

As outlined in our response to Q2, we believe that providing further, rigorous guidance on key concepts such as market power, gateway functionality, and economic dependence would be a more practical and future-proofed alternative to defining 'gatekeepers' in terms of product integration.

The provisions of any new *ex ante* regulation ought, therefore, only to apply to firms in markets where they are found to have 'gatekeeper' power.

We expand on this response in the accompanying paper uploaded in response to this consultation.

Emerging issues

The following questions are targeted particularly at businesses and business users of large online platform companies.

2. As a business user of large online platforms, do you encounter issues concerning trading conditions on large online platform companies?

Yes | No
Please see answer to question 3

3. Please specify which issues you encounter and please explain to what types of platform these are related to (e.g. e-commerce marketplaces, app stores, search engines, operating systems, social networks). *5000 character(s) maximum*

For the purposes of this consultation, we believe we can contribute most constructively to the debate as a platform operator rather than as a business user. We have therefore focused in our accompanying paper on what we consider to be the right conceptual framework for addressing perceived concerns relating to online platforms insofar as they relate to competition.

As a general matter, we believe any new *ex ante* regime should use the existing competition-based framework of legal precedent and economic methodologies to focus on economic effects. Assessments of whether a company's conduct is pro- or anti-competitive are legally and technically complex. The contemplated *ex ante* regulatory regime would, we think, be less well-placed to address other potential societal effects of a platform's conduct, which raise separate issues.

Clearly not everything relating to digital platforms involves competition law, for example (i) concerns over the use of personal data for political campaigning; (ii) concerns about fake news or media plurality; and (iii) concerns about controversial content. Many of these broader societal issues are

complex and require their own set of expertise, and, as with the GDPR, are already governed by existing frameworks and regulators. We believe a clearly delimited focus on economic issues is necessary to deliver a practical framework that supports the growth of the EU digital economy.

We expand on this response in the accompanying paper uploaded in response to this consultation.

4. Have you been affected by unfair contractual terms or unfair practices of very large online platform companies? Please explain your answer in detail, pointing to the effects on your business, your consumers and possibly other stakeholders in the short, medium and long-term? *5000 character(s) maximum*

Please see the response to question 3. As a general matter, the issues on which the Questionnaire appears to seek responses here have been substantially tackled in the Platform-to-Business Regulation (P2B) that entered into force in July 2020. The Commission should assess the impact of P2B on the digital ecosystem before proposing new laws that overlap with the objectives of the P2B (e.g. ranking transparency). Otherwise, any new regulations risk being either unnecessary or ineffective to meet the objectives pursued.

The regulation addresses a number of concerns that SMEs have flagged as "problematic" over the last couple of years. P2B introduces a number of benefits for SMEs: no more sudden and unexplained account suspensions (platforms are obliged to give a 2-week notice, offer possibilities to appeal and reinstate business users if suspension was made in error). Also, platforms need to disclose the main parameters they use to rank goods and services on their site, to help sellers understand how to optimise their presence. Those requirements will be further specified by the EC guidelines on ranking transparency. Platforms' business users will be offered a variety of choices when problems arise including the use of complaint-handling mechanisms that platforms are now required to set up, mediation or collective actions. It is worth highlighting that P2B applies to all platforms irrespective of their size, which indicates that the issues addressed in the regulation can arise irrespective of the platform's size.

We expand on this response in the accompanying paper uploaded in response to this consultation.

The following questions are open to all respondents.

9. Are there specific issues and unfair practices you perceive on large online platform companies? *5000 character(s) maximum*

As explained in response to Question 4, the P2B regulation addresses a number of concerns that SMEs have flagged as "problematic" over the last couple of years, in particular as regards transparency.

As a general matter, we have demonstrated a long-standing commitment to providing an open, transparent relationship with those who use our services, including to help customers adapt to material changes in ranking; understand the rules and processes of auctions; address questions about the fees charged when advertisers use Google's ad intermediation services; and ensure that

consumers have access to clear information concerning which data are collected and how those data are used.

In considering what form any new *ex ante* regulation on transparency should take, three considerations should be taken into account.

First, transparency concerns are not necessarily limited — or related — to the size of the platform at issue. For example, the consequences of unfair or inconsistent ranking decisions may be acute for a business that depends on a niche vertical search service, such as hotels, airlines, or restaurants.

Second, there are clear and well-established limits on how far certain types of transparency can go before they jeopardize the very services to which they relate. Regulators will need to strike a careful balance that ensures that ranking results are not easily manipulated by bad actors harming both legitimate businesses and consumers. For example, while it may be helpful for a search service to provide guidance on the main parameters of a site that it takes into account in ranking, it would be prejudicial to the proper and safe operation of a search service to publish details of all the technical 'proxy signals' through which these parameters are assessed. Otherwise, websites could manipulate and improve their ranking in search results by optimizing for the relevant proxy signal; *not* by increasing the quality or relevance of their site to users.

Third, regulation already exists concerning the appropriate degree of transparency. Specifically, the Platform-to-Business Regulation requires online platforms to identify the "*main parameters*" that search services consider when ranking websites (Article 5(2)). At the same time, the Regulation recognizes in Recital 27 that platforms require the "*ability to act against bad faith manipulation of ranking by third parties, including in the interest of consumers, should [...] not be impaired.*"

We expand on this response in the accompanying paper uploaded in response to this consultation.

10. In your view, what practices related to the use and sharing of data in the platforms' environment are raising particular challenges? *5000 character(s) maximum*

There is a strong case for data use and sharing goals to be effectively and proportionately pursued through existing means and collaborative efforts. For example, digital platforms of all sizes could work with the Commission, Member States, and industry to identify specific use cases where data access or interoperability would promote innovation, and cooperate on ways to facilitate data sharing without jeopardizing privacy or incentives to invest. Google has adopted an approach that is open but respectful of users' rights by making large-scale search datasets publicly available for free (e.g., through the Google Trends and Natural Questions tools, along with multiple other free and open source datasets). And Google has developed data mobility tools that enhance user choice without sacrificing innovation or variety. Specifically, Google has played a leading role in the Data Transfer Project, together with Facebook, Microsoft, Twitter, and various other digital service providers (including Apple, which joined the project on 30 July 2019) to develop a system of data mobility. We are open to exploring other options with stakeholders that would address concerns around data access in a collaborative, proportionate and flexible manner.

However, we would caution against far-reaching regulation. Careful definition of the scope and

operation of any data access rule is critical to avoid damaging both privacy and innovation.

Any new data access rules should be clear in their objectives, and should take account of the varying significance of different types of data, both in terms of (i) enhancing the competitive abilities of data recipients, and (ii) any negative consequences of data access on competition and investment. Proposals to share user-level datasets comprising both click and query data score poorly on both fronts. The evidence shows that 'more data' does not lead to improvements in rival search engines' results. For example, the Microsoft/Yahoo! deal doubled Bing's query volume overnight but, according to observers of the industry, failed to improve the relevance or monetization of Bing's search results.

The evidence also shows that sharing user-level click and query data would not enhance competition to find the best results; rather, click data would inform rivals as to how Google answers a particular query. It would therefore enable rivals to systematically clone Google's search results, reducing product diversity and chilling incentives of Google and its rivals to invest in product improvements. Moreover, sharing such granular data could expose users to privacy violations, as borne out in both historical examples and a paper in Nature by an author of the EC Special Advisers' Report on digital competition.

We expand on this response in the accompanying paper uploaded in response to this consultation.

11. What impact would the identified unfair practices can have on innovation, competition and consumer choice in the single market? *3000 character(s) maximum*

See the response to questions 9 and 10. The specific details of how a search service ranks results represents a core value of its business. Disclosing these details would allow competitors to copy innovations and free ride on investments in developing proprietary search ranking technologies. In other words, there is a balance to be struck between providing business users with information on how they may be affected by changes to rankings, and preserving the quality — and incentives to invest in — search services.

More generally large digital platforms — including those described as 'gatekeepers' — make a significant contribution to economic growth in Europe and other regions, particularly through investing in innovation. As explained in our response to the Inception Impact Assessment, Google, Apple, Facebook, and Amazon are reported to be some of the largest investors in R&D, which is reflected in the 2018 Global Innovation 1000 study. Google has consistently spent over 15% of its revenues on R&D since 2016, whereas the average 'R&D ratio' in the EU is 3.4%.

We expand on this response in the accompanying paper uploaded in response to this consultation.

12. Do startups or scaleups depend on large online platform companies to access or expand? Do you observe any trend as regards the level of dependency in the last five years (i.e. increases; remains the same; decreases)? Which difficulties in your view do start-ups or scale-ups face when they depend on large online platform companies to access or expand on the markets? *3000 character(s) maximum*

Online platforms have created unprecedented market entry and expansion opportunities for SMEs, lowering barriers to entry, expanding their reach and enabling them to scale beyond their home market.

Google services provide significant benefits to our business users. Last year, Google's products supported at least €177 billion a year in economic activity for businesses, developers, creators, and publishers across Europe. Google Maps provides free listings for businesses, who benefit from consumers' searching for local goods and services. And Google Ad campaigns and YouTube help businesses scale. Google's services have helped SMEs to enter and expand rapidly in new markets by improving their ability to find and connect with potential new customers.

At the same time, Google must compete intensely for SMEs' custom as businesses can work with a range of platforms and providers to find consumers, distribute their services, and advertise their products online, and can shift their business easily to the platform that offers them the greatest added value. One example is advertising, where the rapid growth — and increasing sophistication — of inventory has led to falling costs and greater choice for SMEs wanting to make potentially interested consumers aware of their products or services. The 'cost per click' that Google charges advertisers on its owned-and-operated properties has decreased by more than 20% in recent years, and there are ever expanding opportunities to advertise on non-Google surfaces. Just this year, for example, Spotify announced that it would begin working with user data to offer its own personalized ads service.

We expand on this response in the accompanying paper uploaded in response to this consultation.

13. Which are possible positive and negative societal (e.g. on freedom of expression, consumer protection, media plurality) and economic (e.g. on market contestability, innovation) effects, if any, of the gatekeeper role that large online platform companies exercise over whole platform ecosystem? *3000 character(s) maximum*

Public First prepared a report that provides quantitative estimates of the economic impact of Google in Europe. It made several important findings.

First, many of Google's consumer products are provided free of charge, which creates value for many of our consumers who would otherwise have to pay for such services. It was found that Google's core services of Search, Maps, and YouTube have a total consumer surplus of around €420 billion per year for European consumers.

Second, in 2019, Google's products supported at least €177 billion a year in economic activity for businesses, developers, creators, and publishers across Europe.

Third, Google invests significant resources in the underlying infrastructure that powers the Internet in Europe. We have invested over €7 billion in constructing data centres across Europe – currently we have four data centres, in Finland, Belgium, the Netherlands and Ireland, supporting an average of 9,600 jobs per year.

Fourth, enhanced productivity from Google Search and our tools such as Docs, Sheets and Slides helps save European workers over 2,800 million hours a year, while Google Cloud has increased business productivity in Europe by over €2.4 billion.

Fifth, Google is the world's largest business purchaser of renewable energy, and has enabled more than €1.2 billion in renewable energy investment across Europe. This investment allows our data centres in Europe to be environmentally sustainable as well as contributes to maintaining Google's status as carbon neutral since 2007.

Digital technology has also been crucial in helping consumers, businesses, and governments manage the effects of the COVID-19 crisis. One example of this is the free contact-tracing technology jointly developed by Apple and Google to help sustain and manage outbreaks across member states, and support the easing of lockdowns necessary to restart the European economy. Another example is that, from March to May 2020, more than 1 million businesses posted COVID-19 updates, with millions of clicks to retailers' websites each week.

It is essential that new regulation does not jeopardize these types of actions, which benefit consumers and SMEs. What is more, digital services will play a central role in driving a faster, fairer and greener recovery from the COVID-19 pandemic in Europe and promoting innovation will be particularly important as the European economy sets on a path of recovery in the wake of the pandemic.

We expand on this response in the accompanying paper uploaded in response to this consultation.

14. Which issues specific to the media sector (if any) would, in your view, need to be addressed in light of the gatekeeper role of large online platforms? If available, please provide additional references, data and facts. *3000 character(s) maximum*

The media sector, and news publishers in particular, have seen their print circulation and revenues from print advertising fall over the course of several decades. While these difficulties are undeniable, they are linked to structural changes in the market that have emerged over time, including increased competition in the supply of ads; increased competition in the supply of news and editorial content; and the unbundling of news media and services such as classified listings.

Although, these changes have happened in parallel with the emergence of online platforms, those online platforms create substantial value for press publishers while providing users with the information they are looking for.

Google displays news publishers' websites as part of its search results, thereby promoting publishers' content and referring substantial traffic to them in the form of billions of free clicks each year. These clicks lead to increased ad-based and subscription-based revenue that publishers generate on their sites. Based on estimates by Deloitte of the value of a click for publishers, this traffic is worth hundreds of millions of euros a year. By contrast, the ad revenue that Google generates from results pages that show results for press publishers represents a small fraction of that sum.

This value exchange also creates benefits for users by displaying search results together with previews that make it easier for users to identify the most relevant results to their query. Google creates this value for free; neither users nor referenced websites pay Google for the display of search results.

Google is committed to supporting local news in strengthening and benefitting from their online presence. During the Covid-19 crisis, we provided support to smaller publications through our Journalist Emergency Relief Fund and by providing larger publishers using Google's Ad Manager with

five months of fee relief. This builds on years of work to support quality journalism through our Digital Growth Program from the Google News Initiative, a free training program for small-to-medium sized news publishers, available first in Europe, before being rolled out in the rest of the world. The program provides intensive training and mentoring on the fundamentals of digital business strategy, audience engagement and revenue strategy.

We expand on this response in the accompanying paper uploaded in response to this consultation.

Regulation of large online platform companies acting as gatekeepers

1. Do you believe that in order to address any negative societal and economic effects of the gatekeeper role that large online platform companies exercise over whole platform ecosystems, there is a need to consider dedicated regulatory rules?

I fully agree
I agree to a certain extent
I disagree to a certain extent
I disagree
I don't know

2. Please explain *3000 character(s) maximum*

We believe that the right approach is to consider the need for dedicated regulatory rules on a case by case basis. As the Commission considers what activities should be covered by *ex ante* regulation, the following assessments should, we think, be relevant:

(i) Identification of likely problems. The starting point for the regime should be to identify which market features or characteristics are causing competition problems, including consumer harm, that may warrant additional rules or heightened scrutiny of particular players.

(ii) Identification of any harmful gaps in pre-existing law. *Ex ante* regulation could be used as a way of addressing harmful gaps in the existing law that allow perceived problems to occur and prevent them from being addressed. These gaps could be substantive (i.e., existing law does not address a particular practice) or procedural (i.e., issues making existing law ineffective, slow, or unduly difficult to enforce). This stage of the assessment should also take account of whether existing law can address the identified problem without needing to be supplemented by further measures.

(iii) Weighing up the costs and benefits of additional intervention. Any new measures ought to promote competition and innovation. Achieving this goal requires both the costs and benefits to be taken into account and weighed up. Accordingly, the *ex ante* regulatory regime should require the Commission to test in advance whether interventions are likely to enhance competition.

(iv) Consideration for what type of intervention is proportionate to the perceived problem. A range of possible tools can be used to address conduct that raises concerns, from formal sanctions to

guidance. In fast-moving industries, where it takes time to understand the various costs and benefits of a practice — and where the consequences of product changes are uncertain — proportionality plays a particularly important role in deciding how best to resolve a perceived concern, while preserving innovation and competition. In some cases, it may be sufficient to issue guidance on the circumstances in which a practice will raise concerns, and work with industry groups to develop relevant standards.

We expand on this response in the accompanying paper uploaded in response to this consultation.

3. Do you believe that such dedicated rules should prohibit certain practices by large online platform companies with gatekeeper role that are considered particularly harmful for users and consumers of these large online platforms?

Yes | No | I don't know

4. Please explain your reply and, if possible, detail the types of prohibitions that should in your view be part of the regulatory toolbox. *3000 character(s) maximum*

We acknowledge that in certain cases platform size can be relevant to an assessment of potential for harm, and we understand the Commission's objective of apportioning responsibility commensurate with a company's position in the market. We would flag the risk of making the scope of certain rules too narrow and missing an opportunity to extend consistent protection and greater certainty to consumers and businesses, especially where certain concerns apply regardless of the size of the service provider or its business model. For example, the Guardian Media Group brought a high-profile claim against the Rubicon Project in respect of alleged hidden fees. Where a platform's gatekeeper/non-gatekeeper status is less relevant to protecting consumers and businesses, the benefits of new rules would be maximized by ensuring a consistent application across all players in the sector.

We think *ex ante* rules addressing the following kinds of issues are potential candidates for a more expansive application given the types of issues they seek to address and the potential benefits.

- **Data portability.** Data portability regimes most effectively facilitate user switching, multi-homing, and innovation when the maximum number of platforms take part. Rules on data portability or mobility should therefore apply on an industry-wide basis. For example, participation in data mobility systems, such as the Data Transfer Project,[2] could be mandated for some use cases that have been demonstrated to materially encourage entry and expansion.
- **Fee transparency.** Customers have an interest in fee transparency, regardless of the size or market position of the particular platform. There is no compelling reason why some platforms should be afforded discretion to maintain opaque fee structures whereas others should be subject to transparency requirements. As the Rubicon Project example above shows, this risks leading to uneven protection for consumers and businesses, creating uncertainty and eroding trust in digital services.
- **Data privacy.** The GDPR is not limited to 'gatekeeper' firms; it is an industry-wide regulation and any enhancements or supplements to the GDPR that are included in *ex*

ante rules ought to apply equally to non-gatekeeper firms.

- **Choice of services.** Users of any platform — large or small — may have an interest in being presented with a choice of frequently used services, particularly if there is otherwise a risk of their being defaulted to sub-optimal services. These issues can arise on a range of different platforms — mobile, desktop, web-based services, and more. And it may distort competition if some platforms are permitted to 'nudge' consumers towards a particular service, but others are not.

We expand on this response in the accompanying paper uploaded in response to this consultation.

5. Do you believe that such dedicated rules should include obligations on large online platform companies with gatekeeper role?

Yes | No | I don't know

6. Please explain your reply and, if possible, detail the types of obligations that should in your view be part of the regulatory toolbox. *3000 character(s) maximum*

While recognising that it may sometimes be appropriate to apply case-by-case remedies to specific gatekeepers, we would encourage the Commission to also take account of the risk that applying regulations to only certain firms in a given sector could: (i) raise the costs — and limit the activities — of those companies relative to their rivals, thereby distorting competition; (ii) expose customers of out-of-scope companies to harm; (iii) create a regulatory framework that is complex to administer; and (iv) reduce companies' incentives to grow beyond a certain size.

Moreover, accurately distinguishing pro-competitive innovation from anti-competitive conduct is important in order to preserve the benefits that digital platforms offer to consumers and business users. For example, in considering how to apply a general principle of wanting to prevent improper self-preferencing in search, a number of fact specific questions may be relevant. For example: (i) Does the design improve quality and benefit consumers (and has the platform carried out testing to prove that this is the case)? (ii) Does the design increase the relevance of search results by providing more relevant information? (iii) Does the design benefit third parties? (iv) Does the design allow users to choose rival services (e.g., through a choice carousel)? (v) What is the overall significance of the design on the abilities of firms to compete? To be effective and practicable, a general principle would need to provide specific guidance on these kinds of questions.

These issues help explain why competition authorities have resisted introducing a blanket ban on alleged self-preferencing, instead emphasizing the need for case-specific analyses — a view that Google shares. On the one hand, allegations of self-preferencing may require scrutiny to ensure that competition and consumers are not being harmed; on the other hand, a blanket approach could deny users the benefits of innovation and product improvements

We expand on this response in the accompanying paper uploaded in response to this consultation.

7. If you consider that there is a need for such dedicated rules setting prohibitions and obligations, as those referred to in your replies to questions 3 and 5 above, do you think there is a need for a specific regulatory authority to enforce these rules?

Yes | No | I don't know

8. Please explain your reply. *3000 character(s) maximum*

We consider that we can better comment on the appropriate institutional framework when the regulatory proposals are further developed, but at this stage we can see the benefit of DG COMP having such a role: as a pan-EU authority with experience in complex legal and economic assessments, DG COMP would be well suited to this, drawing on other authorities' expertise as and when appropriate.

Much of the conduct that the Consultation suggests could fall within the scope of *ex ante* regulation are competition concerns that DG COMP has addressed on numerous occasions. For example, DG COMP is currently addressing concerns related to Apple's App Store and Amazon's Marketplace, and has addressed other anti-competitive conduct issues in digital and technology markets over the course of several decades. And its merger investigations in Microsoft/LinkedIn and Apple/Shazam show that it is capable of appraising and evaluating the value and importance of data. DG COMP is therefore well-placed to make use of expertise that it has developed over many years and to administer any related ex ante rules.

We expand on this response in the accompanying paper uploaded in response to this consultation.

9. Do you believe that such dedicated rules should enable regulatory intervention against specific large online platform companies, when necessary, with a case by case adapted remedies?

Yes | No | I don't know

10. If yes, please explain your reply and, if possible, detail the types of case by case remedies.

3000 character(s) maximum

We support an agreed baseline of high-level principles that could be applied across different types of platforms (e.g., a measure to address actual or perceived conflicts of interest where a platform owner competes on the platform), complemented by platform-specific guidance.
Insofar as the consultation contemplates far-reaching interventions with respect to specific platforms (e.g., remedies concerning data access or self-preferencing), these measures may increase the costs — and decrease the rewards — of conduct that promotes innovation and generates efficiencies. This, in turn, runs the risk of deterring practices that benefit European firms and consumers.

Any such changes should therefore be considered only after a detailed analysis, with rights of defence, established legal standards, and obligations to respect the principle of proportionality. This is a concern not only for large online platforms but also counterparties and other players (e.g.,

advertisers, publishers, OEMs, and consumers) who would be negatively affected by cancelled or delayed product launches and investments due to the threat of such interventions.

We expand on this response in the accompanying paper uploaded in response to this consultation.

11. If you consider that there is a need for such dedicated rules, as referred to in question 9 above, do you think there is a need for a specific regulatory authority to enforce these rules?
Yes | No

12. Please explain your reply *3000 character(s) maximum*

Please see the response to Question 8

13. If you consider that there is a need for a specific regulatory authority to enforce dedicated rules referred to questions 3, 5 and 9 respectively, would in your view these rules need to be enforced by the same regulatory authority or could they be enforced by different regulatory authorities? Please explain your reply. *3000 character(s) maximum*

Please see the response to Question 8.

14. At what level should the regulatory oversight of platforms be organised?

At national level
At EU level
Both at EU and national level
I don't know

15. If you consider such dedicated rules necessary, what should in your view be the relationship of such rules with the existing sector specific rules and/or any future sector specific rules? *3000 character(s) maximum*

A *ex ante* regulatory instrument could be used as a way of addressing harmful gaps in the existing law that allow perceived problems to occur and prevent them from being addressed. These gaps could be substantive (i.e., existing law does not address a particular practice) or procedural (i.e., issues making existing law ineffective, slow, or unduly difficult to enforce). In particular, the Commission should take account of whether existing law can address the identified problem without needing to be supplemented by further measures.

We expand on this response in the accompanying paper uploaded in response to this consultation.

16. Should such rules have an objective to tackle both negative societal and negative economic effects deriving from the gatekeeper role of these very large online platforms? Please explain your reply. *3000 character(s) maximum*

Not everything relating to digital platforms involves competition law, for example (i) concerns over the use of personal data for political campaigning; (ii) concerns about fake news or media plurality; and (iii) concerns about controversial content. Many of these broader societal issues are complex and require their own set of expertise, and, as with the GDPR, are already governed by existing frameworks and regulators. We believe a clearly delimited focus on economic issues is necessary to deliver a practical framework that supports the growth of the EU digital economy.

We expand on this response in the accompanying paper uploaded in response to this consultation.

17. Specifically, what could be effective measures related to data held by very large online platform companies with a gatekeeper role beyond those laid down in the General Data Protection Regulation in order to promote competition and innovation as well as a high standard of personal data protection and consumer welfare? *3000 character(s) maximum*

Please see the response to Question 10 of the 'emerging issues' section.

18. What could be effective measures concerning large online platform companies with a gatekeeper role in order to promote media pluralism, while respecting the subsidiarity principle? *3000 character(s) maximum*

Online platforms allow for greater media plurality than could ever previously have been imagined. The production and consumption of content has been democratised, to provide unprecedented opportunities to reach global audiences. Broadcasters, writers, musicians, and others can use online platforms, such as YouTube, to connect directly with users and other creators. Established news and cultural organisations have also used online platforms to improve their reach with younger people, with news content from EU media outlets such as die Welt and Le Figaro frequently amassing millions of views on YouTube.

By creating and indexing a general repository of videos, YouTube provided broadcasters with access to billions of viewers and connected viewers with content on any topic imaginable. Likewise, Google Search has provided editors and writers with a much greater opportunity to distribute their content. Anyone can start a blog or a news service, have it indexed on Google Search, and see their content presented to users in response to search queries. And through new distribution channels, such as app stores, existing media providers have a greater opportunity to share and modify their content.

Google recognises the challenges faced by the EU in ensuring a sustainable, pluralistic media sector. We acknowledge the increasing difficulties that news publishers, in particular, have faced, but we strongly believe that online platforms, rather than causing these difficulties, have provided press publishers with substantial value. We fully acknowledge the importance of a thriving and pluralistic media for promoting the EU's culture and safeguarding its democracy. We are continually developing new innovations and are willing to work with the Commission, media organisations and others to play

our part in supporting media pluralism.

We expand on this response in the accompanying paper uploaded in response to this consultation.

19. Which, if any, of the following characteristics are relevant when considering the requirements for a potential regulatory authority overseeing the large online platform companies with the gatekeeper role:

Institutional cooperation with other authorities addressing related sectors – e.g. competition authorities, data protection authorities, financial services authorities, consumer protection authorities, cyber security, etc.
Pan-EU scope
Swift and effective cross-border cooperation and assistance across Member States
Capacity building within Member States
High level of technical capabilities including data processing, auditing capacities
Cooperation with extra-EU jurisdictions
Other

20. If other, please specify *3000 character(s) maximum*

DG COMP satisfies all of the criteria identified as relevant by the Questionnaire:

(i) Institutional cooperation. DG COMP's position as competition enforcer requires it to liaise with EU institutions, Member States, and supranational organizations.

(ii) Pan-EU scope. DG COMP currently administers the EU systems of one-stop-shop merger control and antitrust enforcement across the EU.

(iii) Swift and effective cross-border cooperation and assistance across Member States. DG COMP frequently engages with Member States through the European Competition Network, and collaborates with these authorities and national judicial authorities in cartel investigations.

(iv) Capacity-building within Member States. DG COMP frequently works with Member States and has contributed significantly — and given direction — to Europe's network of national competition enforcers.

(v) Technical capability. As shown above, DG COMP has shown itself capable of handling complex and sophisticated analyses across a wide range of digital and other complex sectors.

(v) Cooperation with extra-EU jurisdictions. DG COMP enjoys close relationships with competition

and other regulatory authorities outside the EU with whom it frequently coordinates in cross-border merger reviews and antitrust investigations.

We expand on this response in the accompanying paper uploaded in response to this consultation.

21. Please explain if these characteristics would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing? *3000 character(s) maximum*

Please see the response to Question 20.

22. Which, if any, of the following requirements and tools could facilitate regulatory oversight over very large online platform companies (multiple answers possible):

Reporting obligation on gatekeeping platforms to send a notification to a public authority announcing its intention to expand activities

Monitoring powers for the public authority (such as regular reporting) Investigative powers for the public authority

Other

23. Other – please list *3000 character(s) maximum*

The design of enforcement is important to the nature and impact of the regime as a whole. The Commission should keep the objectives of flexibility, pro-innovation, and legal certainty front of mind when considering this question. If the objective is to implement a system that is efficient and nimble (with heavy duty enforcement in exceptional cases being left to the existing antitrust regime), then that will be facilitated by a framework that focuses on collaboration, consultation, and conflict resolution rather than fault-based enforcement. In contrast, a regime with new, far-reaching enforcement powers would need to provide for evidentiary standards in decision-making and rights of appeal that are commensurate to those powers. This is likely to slow down enforcement.

There are various possible approaches to enforcement that would retain the effectiveness of the Commission as a guide to behavior, while still providing for rapid enforcement and preserving incentives to innovate. This could include:

(i) Reputational sanctions where the regulatory authority would publish decisions finding a breach of the *ex ante* rules and maintain a public register of all upheld complaints. A negative statement would be reputationally damaging with partners, consumers, and regulators, and because it is public it would require a response.

(ii) A reporting obligation whereby firms that have been found to have breached the ex ante rules would be required to publish periodic reports on: (i) changes they have made to their practices that are relevant to the infringement and (ii) any measures taken to resolve the infringement. Platforms could also be required to disclose findings of infringements to customers and suppliers, as well as in

merger control filings.

(iii) Referral of serious breaches to the DG COMP and other regulators to investigate possible violations of the relevant laws or regulations. The Commission's decision — and evidence already gathered — could form part of the relevant regulator's case file, thereby giving the regulator a headstart in any subsequent investigation.

We expand on this response in the accompanying paper uploaded in response to this consultation.

24. Please explain if these requirements would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?

3000 character(s) maximum

If the regulatory authority is granted more extensive enforcement powers, it will be important that the *ex ante* rules provide for procedural fairness in decision-making and commensurate rights of appeal. Proposed enforcement powers could conceivably entail quasi-criminal financial penalties and mandatory orders that will affect how firms use their IP rights, proprietary algorithms, and assets that they have invested heavily in creating. This will have far-reaching consequences on businesses. In particular:

(i) Decisions prohibiting, or requiring the unwinding of, product changes or improvements that involve large-scale investments could have significant financial ramifications and hurt users that could otherwise benefit from those product improvements (e.g., see our discussion of Streetmap.EU above). Particularly far-reaching remedies, together with the threat of fines, could be equated to criminal proceedings for the purposes of the right to a fair trial under Article 6(1) of the ECHR. Such measures therefore warrant full procedural and appeal rights.

(ii) Since an erroneous conclusion could have serious consequences for the firm in question, as well as competition and innovation in the industry, the Commission's enforcement decisions should not be taken lightly. A merits-based appeal ensures an independent review of regulatory decision-making that should lead to better and more robust decision-making.

We expand on this response in the accompanying paper uploaded in response to this consultation.

25. Taking into consideration the parallel consultation on a proposal for a New Competition Tool focusing on addressing structural competition problems that prevent markets from functioning properly and tilt the level playing field in favour of only a few market players. Please rate the suitability of each option below to address market issues arising in online platforms ecosystems. Please rate the policy options below from 1 (not effective) to 5 (most effective).

	1 (not effective)	2 (somewhat effective)	3 (sufficiently effective)	4 (very effective)	5 (most effective)	Not applicable/No relevant

						experience or knowledge
1. Current competition rules are enough to address issues raised in digital markets						x
2. There is a need for an additional regulatory framework imposing obligations and prohibitions that are generally applicable to all large online platforms with gatekeeper power						x
3. There is a need for an additional regulatory framework allowing for the possibility to impose tailored remedies on						x

individual large online platforms with gatekeeper power, on a case- by-case basis						
4. There is a need for a New Competition Tool allowing to address structural risks and lack of competition in (digital) markets on a case-by- case basis.						x
5. There is a need for combination of two or more of the options 2 to 4.						x

26. Please explain which of the options, or combination of these, would be, in your view, suitable and sufficient to address the market issues arising in the online platforms ecosystems. *3000 character(s) maximum*

We believe that a combination of the options listed above could address perceived concerns relating to digital platforms. Which tool is most suitable in a given case will depend on the particular issue at hand.

27. Are there other points you would like to raise? *3000 character(s) maximum*

When designing a procedural framework that covers the administration of ex ante regulation, Google

encourages the Commission to consider the following:

(i) Clarity and legal certainty. Any gatekeeper designation should relate to identified business activities in specific markets within a corporate group so that the scope of that firm's obligations are clear.

(ii) Flexibility and pro-innovation. New technologies develop and marketplaces change quickly in the digital economy. It is therefore important that gatekeeper designations are reviewed periodically.

(iii) Due process. Gatekeeper designations could have serious implications, such as requiring firms to change their business practices. The framework should therefore respect due process by providing for an appeals process under which firms can appeal a gatekeeper designation decision and the scope of that decision.

(iv) Collaboration and proportionality. Any new *ex ante* regulation will introduce new rules whose application (at least initially) may be uncertain. Collaboration between firms and the authority will be important to protect incentives to innovate. Any new *ex ante* regulation ought to be developed incrementally in consultation with the industry and the affected firms.

(v) Evidence-based processes. An evidence-based approach to enforcement is important. Otherwise, *ex ante* regulation risks penalizing legitimate business conduct. The regulatory authority should clearly set out the evidence upon which it is relying when deciding that there has been an infringement of the *ex ante* rules.

(vi) Effective triage mechanisms. There is a risk that the regulatory authority becomes a 'clearing-house' for complaints about digital firms. Some of those complaints will merit investigation, others will not. We believe it will be important for the authority to have a mechanism for rejecting complaints that are without merit and demonstrating this publicly.

We expand on this response in the accompanying paper uploaded in response to this consultation.

Jump to overview for this section

Part IV. Other Emerging Issues and Opportunities, Including Online Advertising

1. When you see an online ad, is it clear to you who has placed the advertisement online?

Yes, always
Sometimes: but I can find the information when this is not immediately clear
Sometimes: but I cannot always find this information
I don't know
No

3. What information is publicly available about ads displayed on an online platform that you use? *3000 character(s) maximum*

We strive to provide users with transparency into the ads they see. Our Help Center offers information about ads served from Google's network, including Google services, like Google Search, YouTube or Gmail, as well as non-Google websites and apps that partner with us to show ads. Information about ads displayed on our services, like Google Search, YouTube or Gmail, can also be found by clicking on the 3 dots, then on the "Why this Ad" icon (soon to be renamed 'About this Ad'). Interested parties may also use the AdChoices icon for information about ads displayed (this is provided for non-Google websites and apps that partner with us).

We expand on this response in Section IV of the accompanying paper uploaded in response to this consultation.

4. As a publisher, what type of information do you have about the advertisement placed next to your content/on your website? *3000 character(s) maximum*

We aim to be a trustworthy and reliable trading partner, providing publishers with transparency, flexibility and the ability to review and control the types of ads that appear on their websites or apps.

One of the primary tools for our publishers is our Ad Review center. The Ad Review center allows publishers to review individual ads after the ads are shown and decide whether they want to continue showing those ads on their pages.

Publishers can review the ad type, buyer, the site on which the ad was served, and the number of impressions per day over the last 30 days. Additionally, publishers can view a full size preview of the ad shown on their website and information such as its size, type, destination URL, Google ads account or ad network.

In addition to reviewing ads, partners can use the Ad Review center to block and report bad ads in real-time. Publishers can also set limitations as to which categories of ads that appear on their site or app. For Google Ad Manager, the Protections feature enables publishers to block or allow advertisers, brands, certain ad technologies, categories, and ad types. For AdSense, publishers can block URLs, specific ad networks, specific categories of ads via Blocking controls.

7. As an advertiser or an agency acting on the advertisers' behalf (if applicable), what type of information do you have about the ads placed online on your behalf? *3000 character(s) maximum*

This question is addressed to advertisers and agencies, therefore we have not responded to it.

Details on the information we provide to advertisers about advertising on our platforms is included in Section IV of the accompanying paper uploaded in response to this consultation.

10. *[No question 9 in consultation]* **As an online platform, what options do your users have with regards to the advertisements they are served and the grounds on which the ads are being served to them? Can users access your service through other conditions than viewing advertisements? Please explain**. *(3000 character(s) maximum)*

Users can access some Google services without receiving any ads (such as YouTube, which can be accessed ad-free via a subscription to YouTube Premium). But our key goal is to make products accessible to everyone - so many products, including Search, Chrome, Maps, and Gmail, are available for free, without subscription or paywalls, and their operation is funded by the sale of ad space. Our goal is to provide users with useful information. On Google Search, sometimes that information comes in the form of an ad, which we show along with search results. If the search is not a "commercial query" (searches that indicate someone is interested in purchasing something, like tickets or shoes), we often do not show any ads at all — in fact, no ads are shown for the large majority of searches. No Google service requires a user to see personalised ads (users can turn off personalized advertising at any point from their Ad Settings).

We expand on this response in Section IV of the accompanying paper uploaded in response to this consultation.

11. Do you publish or share with researchers, authorities or other third parties detailed data on the advertisements published, their sponsors and viewership rates? Please explain. *(3000 character(s) maximum)*

We do not generally publish or share with researchers, authorities or other third parties detailed data on the advertisements published on our platforms, the advertiser or viewership rates (save for the data that we provide to the advertiser to assess the performance of their campaign(s)). We recognise though that there may sometimes be legitimate public interest purposes for researchers and other third parties to gain access to specific datasets, and we are willing to discuss the terms on which that can happen, taking into account the risks for user privacy and of inadvertently exposing the sensitive data of Google's business partners.

For example, our Political Ads Transparency Report data is fully available to the public. These data can be downloaded as a CSV from the Political Advertising on Google Transparency website and are published as a public data set on Google Cloud BigQuery. To develop the Political Ads Transparency Report, we conducted over 80 global user and expert interviews to understand what type of data was going to be most useful for users of this Transparency Report, including for academic researchers. Even now the Report is live, we provide opportunities for user feedback via the "send feedback" form and a pop-up satisfaction survey on the Transparency Report website, which we review quarterly. This feedback is used to guide the development of the report so it is as useful as possible to third parties and researchers that seek access to this information.

12. What systems do you have in place for detecting illicit offerings in the advertisements you intermediate? *(3000 character(s) maximum)*

We want to support a healthy digital advertising ecosystem that is trustworthy and transparent. We therefore publish detailed ads policies ("**Google Ads policies**") that are designed to protect all stakeholders in the ads ecosystem. To ensure a safe and positive experience, we require that advertisers comply with the Google Ads policies and all applicable laws and regulations. Ads, extensions, destinations, and other content that violate these policies will be blocked on the Google Ads platform and associated networks.

We expand on this response in Section IV of the accompanying paper uploaded in response to this consultation.

14. *[Note: there is no Q13 in the consultation doc]* **Based on your experience, what actions and good practices can tackle the placement of ads next to illegal content or goods, and/or on websites that disseminate such illegal content or goods, and to remove such illegal content or goods when detected?** *(3000 character(s) maximum)*

Maintaining trust in the ads ecosystem requires setting limits on the content that is monetised. In order to reassure advertisers that their brands are not being tainted by harmful or illegal content, advertising intermediation should apply rules about the content that can be displayed on websites and apps that use the intermediation service.

Further information about the steps we take to protect advertisers from having their ads associated with harmful content is provided in Section IV of the accompanying paper uploaded in response to this consultation.

15. From your perspective, what measures would lead to meaningful transparency in the ad placement process? *(3000 character(s) maximum)*

Meaningful transparency in the ad placement process involves:

- Advertisers and publishers understanding *why* a particular ad won an auction and was displayed in a given slot on a given webpage, as well as *what content* appears alongside the ad; and
- Users understanding *why* a particular ad has been shown to them.

We are already actively involved in transparency work with a number of third party measurement providers, industry initiatives, and standards organizations and are open to exploring additional transparency measures that we can take.

Further information about measures to achieve more transparency is provided in Section IV of the accompanying paper uploaded in response to this consultation.

16. What information about ads displayed online should be made publicly available? *(3000 character(s) maximum)*

Sufficient information should be made publicly available to allow advertisers, publishers and consumers to understand how advertising auctions work, how advertising revenues are distributed, how personalisation of advertising works, and how users are protected from illegal and harmful advertising.

We recognise and support transparency that improves accountability and trust for advertisers, publishers and users. We are open to feedback on additional transparency measures that may help to achieve this, but any conversation about transparency measures must also acknowledge the need to minimise the risk of sharing personal user data or commercially sensitive information.

See Section IV of the accompanying paper uploaded in response to this consultation for more detail on the information we disclose to promote transparency, and the factors that need to be balanced when deciding on appropriate levels of disclosure.

17. Based on your expertise, which effective and proportionate auditing systems could bring meaningful accountability in the ad placement system? *(3000 character(s) maximum)*

We believe that giving publishers and advertisers the tools and information to audit how their campaigns and inventory are performing is an important mechanism to ensure accountability in the ad placement system. Collaboration with industry bodies is also important - as mentioned in Section IV of our accompanying paper, we are actively involved in transparency initiatives with a number of industry stakeholders.

Importantly, any audit mechanisms would need to balance the following conflicting interests:

- The desire from industry stakeholders to have more visibility into auction decision-making and verify that this is fair and objective;
- Protection of proprietary algorithms and commercially sensitive information and data signals, as disclosure of such information to competitors would reduce incentives to innovate. This would harm competition, as well as exposing users to potential harm from 'bad actors' who may seek to manipulate the system to bypass legitimate safeguards (as explained in response to Question 16);
- Protection of users' personal data, which may be included in a bid request or applied by an participant in the auction for targeting purposes. Unauthorised disclosure of this data could violate privacy laws.

See Section IV of the accompanying paper uploaded in response to this consultation for more detail on this topic.

18. What is, from your perspective, a functional definition of 'political advertising'? Are you aware of any specific obligations attaching to 'political advertising' at a European or national level? *(3000 character(s) maximum)*

As signatory of the EU Code of Practice on Disinformation ("**Code on Disinformation**"), in January 2019, in time for the elections of the EU Parliament, we published our EU election ads policy, which requires verification and in-ad "paid for by" disclosures for all EU election ads. At the time of launch, the election ads policy focused on European Parliamentary elections, and applied to ads featuring a political party, a current elected officeholder, or a candidate for the EU Parliament. On September 3 2019, we announced the expansion of our EU election advertising policy to cover referenda, including all national level referenda and state or jurisdiction level official referenda that concern sovereignty.

This definition now also covers ads that feature "*a political party, a current officeholder, or candidate for an elected national office within an EU member state.*" We consider that the definition applied in our policies is a functional definition of 'political advertising'

With regards to obligations on a national level within the EU, in France in accordance with the law on "Informational Content Ads" — referring to the promotion of informational content in relation to a debate of general interest — we have stopped allowing informational content ads in France starting with the 2019 EU parliamentary elections period.

See Section IV of the accompanying paper uploaded in response to this consultation for more detail on this topic.

19. What information disclosure would meaningfully inform consumers in relation to political advertising? Are there other transparency standards and actions needed, in your opinion, for an accountable use of political advertising and political messaging? *(3000 character(s) maximum)*

We recognise the importance of meaningful transparency to provide consumers with clarity and confidence on the origins of the political advertising they view online. To achieve this goal, and as mentioned in Question 18, in January 2019, in time for the elections of the EU Parliament, we published our EU political content ads policy. This policy outlines our restrictions for targeting election ads, so that consumers have a clear understanding of the limited criteria that can be used for these purposes. In addition, we produce a Political Advertising Transparency Report for each EU Member State

Further information on the steps we take to meaningfully inform consumers in relation to political advertising is provided in Section IV of the accompanying paper uploaded in response to this consultation.

20. What impact would [have], in your view, enhanced transparency and accountability [mechanisms have?] in the online advertising value chain, on the gatekeeper power of major online platforms and other potential consequences such as media pluralism? *(3000 character(s) maximum)*

We recognise that there is an ongoing challenge to reassure stakeholders about transparency in the online advertising value chain. As discussed above, finding the right level of transparency requires the balancing of various factors. Any transparency and accountability measures should arguably also apply to *all platforms*, since concerns often apply regardless of the size of the platform and the business model they rely on.

Assuming transparency mechanisms find the right balance and apply to all platforms, we believe there is value in addressing concerns about transparency and accountability in online advertising. Establishing stakeholder trust is a key challenge that platforms like Google face: reliable verification

that auctions are working fairly and objectively would therefore be helpful in resolving these concerns.

Further information on this topic, and the consequences for preserving media pluralism, is provided in Section IV of the accompanying paper uploaded in response to this consultation

21. Are there other emerging issues in the space of online advertising you would like to flag? *(3000 character(s) maximum)*

We recognise and support the Commission's ambitions to ensure that online advertising is fair, transparent and accountable. But before introducing interventions in this sector, we urge the Commission to assess the risk of such interventions inadvertently hampering a valuable tool that creates value for advertisers, publishers and the EU economy (particularly following the impact of Covid-19) (see further Section IV of the paper uploaded in response to this consultation).

More specifically, we wish to focus here on concerns among some publishers and advertisers about the transparency of advertising intermediary fees, including our take rate. In this regard, we want to highlight the findings of the CMA Final Report. This found that:

- The take rates of our online advertising products are similar to the average take rates of competitors and our average winning margin is similar to that of non-Google DSPs (para 5.242). Therefore, the CMA Final Report concluded there is no evidence that we are charging hidden fees.

- There is significant variation in our overall take rate and Google Ads' take rate on a per publisher basis (CMA Report, Appendix R, para. 20). These take rates are (i) significantly lower than those suggested by some stakeholders, and (ii) broadly in line with what non-Google intermediaries charge for similar services. The CMA concludes that the evidence does not support the claims alleged by certain media publishers that we have a systematic advantage over other bidders (for instance as a manifestation of a gatekeeper role in the online advertising value chain) (Appendix R, paras. 21, 28).

(For a more general discussion please see the Progressive Policy blog at: https://www.progressivepolicy.org/blogs/the-uk-online-ad-market/.)

We understand the broader issues raised by the CMA report about the difficulty for advertisers and publishers to independently audit the fees they are charged, but we think these findings provide important context to this debate. As set out elsewhere, we recognise that there is an ongoing challenge to reassure stakeholders about transparency in the online advertising value chain. Finding the right level of transparency requires the balancing of various factors and we are open to a dialogue on how this balance can be achieved.

Jump to the overview for this section

Part VI. What Governance for Reinforcing the Single Market for Digital Services?

Main issues

1. How important are digital services such as accessing websites, social networks, downloading apps, reading news online, shopping online, selling products online in your daily life or your professional transactions?

-

Overall	★★★★★
Those offered from outside of your Member State of establishment	★★★★★

---

4. To what extent are the following obligations a burden for your company in providing its digital services, when expanding to a/several EU Member State(s)?
Please rate the following obligations from 1 (not at all burdensome) to 5 (very burdensome).

	1 (not at all burdensome)	2	3 (neutral)	4	5 (very burdensome)	I don't know / No answer
Different processes and obligations imposed by Member States for notifying, detecting and removing illegal content /goods/services					X	
Requirements to have a legal representative or an establishment in more than one Member State					X	
Different procedures and points of contact for obligations to cooperate with authorities					X	
Other types of legal requirements. Please specify below						

5. Please specify
3000 character(s) maximum

The trend towards Member States imposing varying obligations around notifying, detecting and removing illegal content, goods and services has created undue burdens. A framework allowing firms to comply with one set of processes for undertaking and reporting on these activities would reduce regulatory complexity—strengthening the single market for digital services and helping users understand the rules, roles and responsibilities in the regulatory scheme.

Establishing compliance systems for fragmented process rules requires extensive work, whatever the size of the company. We recognise the importance of dedicating resources to internal compliance systems for national process rules; but each variation increases complexity, increasing compliance risks for platforms and risking confusion for users across member states. And a framework that permits 27 different sets of process rules may become unworkable: compliance systems may become incoherent if rules vary. For example, if every country requires a separate transparency report, and each requires different definitions, metrics or reporting methods, these variations may result in incompatible instructions or processes for those processing cases, or engineering challenges around standardisation. Each variation also risks limiting meaningful comparison between member states.

Reforms supporting the ability of firms to comply with one set of process rules in the EU will therefore strengthen the single market. The eCD's country-of-origin principle has been fundamental in supporting innovation and growth in digital services. It should be retained and better supported in new regulatory schemes for the systems online platforms adopt to help keep users safe: country-of-origin can promote certainty and growth, by providing clarity to users and service providers on which member state is providing oversight of those systems.

Through the DSA, the Commission may wish to consider explicitly removing process rules around illegal content, goods and services from the scope of country-of-origin derogations. If it does so, the Commission may wish to consider a degree of minimum harmonisation in this area, with cooperation aimed at driving consistency (e.g. guidelines) between national regulatory bodies.

Requirements to have a legal representative or establishment in more than one Member State are unduly burdensome; this is the foundational premise of the country-of-origin principle. Such requirements represent an unjustifiable legal obstacle that hampers the exercise of the freedom of establishment and the freedom to provide services.

Different procedures and points of contact for obligations to cooperate with authorities are also unduly burdensome. As set out above, we support initiatives that make cooperating with legal enforcement authorities simpler but which maintain procedural safeguards. We support harmonised frameworks that facilitate expeditious and privacy protective procedures, including single points of contact.

6. Have your services been subject to enforcement measures by an EU Member State other than your country of establishment?
Yes | No | I don't know

7. Please specify the grounds on which these measures were taken (e.g. sale of illegal goods on our service, obligations related to tackling disinformation) and what was your experience?
3000 character(s) maximum

Google seeks to comply with all local laws, but has been subject to enforcement measures by EU Member States other than its country of establishment.

11. What has been the impact of COVID-19 outbreak and crisis management measures on your business' turnover

Significant reduction of turnover
Limited reduction of turnover
No significant change
Modest increase in turnover
Significant increase of turnover
Other

12. Please explain
3000 character(s) maximum

The macroeconomic environment caused by the pandemic created headwinds for our business. In the second quarter 2020, total revenues were down 2% year-on-year, and flat on a fixed FX basis.

13. Do you consider that deepening of the Single Market for digital services could help the economic recovery of your business?
Yes | No | I don't know

14. Please explain
3000 character(s) maximum

As we set out in this response, we support measures that strengthen the single market, including those that increase certainty for businesses about the rules and processes online intermediaries should follow as they provide services online. Increased legal certainty creates conditions that allow companies of all sizes to innovate on the scope and nature of the content, goods and services they offer online, supporting economic growth across all member states.

Google launched our Grow with Google digital skills training programs in 2015 with the aim of supporting European businesses and entrepreneurs to grow their own skills, make more use of the digital economy and support the growth of the Digital Single Market. We have made a number of commitments through the Commission's Digital Skills Coalition in support of the joint goal of supporting growth within the Single Market.

Consistent with our work on digital growth, and as we detail above, since the outbreak of COVID-19, teams across Google have launched over 200 new products, features and initiatives and are contributing over $1 billion in resources to help our users, clients, partners, and governments through this unprecedented time. Our major efforts are focused around: providing trusted information to our users, contributing to recovery efforts across the globe, and helping people adapt to a changing world—including by providing tools and resources to help businesses and organisations continue to

function through lockdowns, and investing in people and their skills to achieve a sustainable, inclusive economic recovery.

We launched Grow with Google with the goal of training one million Europeans in digital skills. We have also made changes to tools like Search and Maps so that businesses could more easily update their customers about changes to their opening hours and other information, as well as making it easier to receive donations, sell gift cards and take orders online. Now we are investing further to help businesses digitise faster, including enabling access to free tools and capital for underserved businesses. Where they are not already online, we are helping them build a digital presence. Then, with tools like Grow my Store and Google my Business - now updated with COVID-related information and insight - we are helping them find new customers online and we've added over 10 features to support businesses affected by COVID-19 since February.

The following questions are targeted at all respondents.

Governance of digital services and aspects of enforcement

The 'country of origin' principle is the cornerstone of the Single Market for digital services. It ensures that digital innovators, including start-ups and SMEs, have one set of rules to follow (that of their home country), rather than 27 different rules.

This is an important precondition for services to be able to scale up quickly and offer their services across borders. In the aftermath of the COVID-19 outbreak and effective recovery strategy, more than ever, a strong Single Market is needed to boost the European economy and to restart economic activities in the EU.

At the same time, enforcement of rules is key; the protection of all EU citizens regardless of their place of residence, will be in the center of the Digital Services Act.

The current system of cooperation between Member States foresees that the Member State where a provider of a digital service is established has the duty to supervise the services provided and to ensure that all EU citizens are protected. A cooperation mechanism for cross-border cases is established in the ECommerce Directive.

1. Based on your own experience, how would you assess the cooperation in the Single Market between authorities entrusted to supervise digital services?
5000 character(s) maximum

Competition Law
As a preliminary remark, we believe that a participative approach that entails cooperation between governments, competition agencies, and industry can lead to a better understanding of the digital sector. We consider that the European Competition Network is an effective mechanism to promote the consistent application of competition law. We support transparent cooperation between national competition authorities (including sectoral regulators) within member states and joint efforts to strengthen capacity as regards digital services. We welcome initiatives to better resource national competition authorities and to develop or strengthen in-house expertise on digital markets.

Consumer Law

We welcome the cooperation mechanisms provided for in the consumer law framework, and support how these have been used by local authorities and the Commission—these mechanisms have allowed prompt action, and provided greater legal certainty for businesses by addressing fragmentation.

Our experience of the Consumer Protection Cooperation (CPC) Regulation since January 2020 is that the mechanisms to investigate and tackle cross-EU infringements are now more effective, allowing prompt cooperation on infringements with centralised help from the European Commission. We welcome the prompt response to COVID-19 consumer scams by the EU Commission and the CPC Network—in our view this is a good example of using the cooperation mechanisms to provide effective and coherent cross-border oversight.

For us, cooperation mechanisms such as the CPC Network Common Position and coordinated action are important in the context of a framework based on country-of-origin: they allow companies to make decisions to protect users based on consistent interpretation of the relevant laws, allowing more coherent solutions, and may reduce the need for lengthy enforcement procedures through multiple instances.

GDPR
Although the GDPR provides a number of tools for cooperation between DPAs, we consider that their potential to reduce fragmentation is not yet fully realised.

The consistency mechanism is an important part of ensuring a consistent approach to enforcement across Europe, bolstering the One-Stop-Shop (OSS) mechanism. We would therefore support greater use of European Data Protection Board (EDPB) opinions. When enforcing the GDPR, DPAs are not obliged to involve the EDPB or start a coherency procedure, even if the matter is of general importance or has implications in more than one Member State. For matters of general importance with implications across several Member States, we would recommend that the EDPB should be consulted.

We welcome the provision in the GDPR for certification mechanisms and codes of conduct, and make the following suggestions aimed at reducing the potential for fragmentation.

- Codes of conduct serve as rigorous accountability mechanisms and increase transparency, but the current approval process is slow and leads to fragmentation. The guidelines and accreditation process of Monitoring Bodies of the EDPB require each Member State to submit its individual accreditation requirements to the EDPB for its opinion. Fragmentation would be reduced if the accreditation criteria of all Member States were assessed together, leading to an EU-wide applicable accreditation requirement.
- Given the flexibility available for creating GDPR certifications, this could lead to further fragmentation by Member States. We would welcome European certification mechanisms that replicate already internationally recognised and widely adopted standards: this would not only promote harmonisation, but also improve cooperation between European and international DPAs.

2. What governance arrangements would lead to an effective system for supervising and enforcing rules on online platforms in the EU in particular as regards the intermediation of third party goods, services and content (See also Chapter 1 of the consultation)?
Please rate, on a scale of 1 (not at all important) to 5 (very important), each of the following elements.

	1 (not at all important)	2	3 (neutral)	4	5 (very important)	I don't know / No answer
Clearly assigned competent national authorities or bodies as established by Member States for supervising the systems put in place by online platforms					X	
Cooperation mechanism within Member States across different competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g. consumer protection, market surveillance, data protection, media regulators, anti-discrimination agencies, equality bodies, law enforcement authorities etc.)			X			
Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States			X			
Coordination and technical assistance at EU level					X	
An EU-level authority			X			
Cooperation schemes with third parties such as civil society organisations and academics for specific inquiries and oversight			X			
Other: please specify in the text box below						

3. Please explain
5000 character(s) maximum

We are at this stage cautious in rating the oversight elements identified by the Commission above: the mix and detail of governance arrangements should be driven by the needs of the regulatory framework; there will be important interactions between the oversight elements identified; and the effectiveness of oversight arrangements may differ between frameworks for the intermediation of third party goods, services and content.

Any governance arrangements should: (i) be designed to fulfil the specific task(s) that help achieve the regulatory objectives; (ii) be based on a robust analysis of how each of the elements interacts; and (iii) promote legal clarity for users and industry, so as to enable the next wave of innovation and economic growth.

Regulatory objectives

In our view, regulatory functions should be centered around: timely and systemic efforts to protect users from illegal content; growth, providing legal certainty across the ecosystem; and innovation, supporting user choice and accommodating new technologies. These objectives should be provided for in the regulatory framework.

The regulatory toolkit should therefore have a systemic focus, with transparency at the center. It could include: compiling transparency reports; developing and reporting on common performance indicators (CPIs); and encouraging reporting on joint work between industry and civil society. The toolkit could also empower regulators to work with industry to support platforms of all sizes as they identify and develop holistic solutions to emerging issues, e.g. through: product and service certifications; guidance on process standards; or sandboxing for compliance tools.

Where systemic failures are suspected, information or enforcement notices should privately be given to a service provider, affording it a reasonable opportunity to investigate and, if necessary, take appropriate action. Sanctions should be reserved for cases of non-compliance with reporting obligations or a failure to address a systemic issue.

National regulators
As we set out above, the eCD's country-of-origin principle has been fundamental in supporting innovation and growth in digital services. It should be retained and supported in any new regulatory framework for the systems platforms use to help keep users safe: it can promote certainty and growth by providing clarity to users and service providers on which body is providing oversight of those systems. On this basis, clearly assigned competent national authorities should play a leading role in supervising the systems put in place by online platforms.

Cooperation between regulators
Because the single market sees platforms offer services across the EU, and platforms offer services within many sectors and with diverse functionalities, an EU regulatory regime will likely be more effective if regulators can cooperate, whether at national or EU level.

Cooperation should be structured around clear purposes, and those purposes should reflect the specific needs of the regulatory frameworks for the intermediation of third party content, services and goods.
Indeed, and as we outline above, an important purpose for cooperation between regulators at the EU level may be to support country-of-origin and any minimum harmonisation of process rules by promoting alignment and coherence in how regulators achieve their regulatory goals.

For a framework focused on systems and transparency, EU-level cooperation towards such coherence could include:

- Sharing technical expertise or best practices around transparency reports;
- With industry, developing CPIs or technical standards for compliance systems;
- Providing recommendations that support sandboxing for compliance solutions;
- Annual reporting between regulators on holistic strategies to achieve the regulatory objectives.

A thorough consideration of second and third order consequences should inform the terms of any cooperation and the process safeguards: e.g. around the independence of regulators, limits on information sharing, or clear process timelines to ensure that decision-making is timely. Regulators should also be transparent in their cooperation. Cooperation between regulators should not reduce certainty for industry and users, and support robust regulatory decisions.

Collaboration with civil society and academia
Given the shared responsibility in tackling illegal content online, civil society has an important role to play. Google supports regulators as they convene and assist in coordinating this work.

As set out above, Google participates in a number of collaborative efforts with civil society (e.g., through the Trusted Flaggers programme), and supports industry groups that work together on enforcement strategy, knowledge sharing, training and networking.

Collaboration with third parties in regulatory decision-making must be assessed against national administrative laws; any role in oversight or enquiries should meet the same standards of independence, transparency and due process.

4. What information should competent authorities make publicly available about their supervisory and enforcement activity?
3000 character(s) maximum

As set out in Principle 2 of the 2012 OECD Council Recommendation on Regulatory Policy and Governance, we consider that countries and regulators should "adhere to principles of open government, including transparency and participation in the regulatory process to ensure that regulation serves the public interest and is informed by the legitimate needs of those interested in and affected by regulation."

We also consider that the objectives that guide the EU's principle of openness could helpfully inspire the objectives for information-sharing from competent authorities about their supervisory and enforcement activity - that is, the provision of information should be such as to promote good governance and participation in the regulatory process.

On this basis, regulators should make publicly available information that allows: citizens and users of online platforms to understand the rules that are being applied by the regulator, through communications that are accessible and can be understood by the general public; industry and stakeholders from civil society to participate in regulatory processes; and regulated entities to understand what is required of them. As the OECD also suggests in its 2012 recommendations, "key operational policies and other guidance material, covering matters such as compliance, enforcement and decision review should be publicly available." The information regulators provide may also include, as appropriate, signposting to other relevant regulators, coordinating bodies, or user interest groups. Any information made available should respect the legitimate interests of regulated entities and users, including privacy, data protection and the protection of business secrets.

To promote the accessibility and reach of publicly available information, regulators should, as appropriate, provide updates through a range of communications channels and in an appropriate mix of formats. Regulators should have websites that are easy for users to navigate and to search for information.

5. What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms?
3000 character(s) maximum

We suggest that, as in all regulatory systems, the requisite capabilities should be closely aligned to the nature and objectives of the regulatory regime.

For example, a systems-focused regime may, depending on the framework, require a balance of quantitative and qualitative skills and resources on controls, governance and processes, as well as the relevant subject-matter (i.e., content standards, consumer law, or data protection).

Competent authorities should have a robust understanding of the markets they are regulating, including the range and diversity of online platforms. To facilitate relevant regulators having a good base understanding of the markets and technologies, it may be worth exploring initiatives with industry and civil society to educate regulators and policymakers within the EU e.g., through partnerships with industry and civil society to provide market and technical education and training.

In line with good regulatory practices, the relevant competent authorities should regulate based on a strong evidence base, and conduct robust investigations within the context of the administrative system. As such, and as in other regulatory systems, competent authorities supervising online platforms should have expert legal, technical, and economic functions.

6. In your view, is there a need to ensure similar supervision of digital services established outside of the EU that provide their services to EU users?

Yes, if they intermediate a certain volume of content, goods and services provided in the EU
Yes, if they have a significant number of users in the EU
No
Other
I don't know

7. Please explain
3000 character(s) maximum

There is a need to ensure similar supervision of digital services established outside the EU that provide their services to EU users. Given the challenges associated with supervising services established outside the EU, such a framework may benefit from a de minimis threshold level, but in our view the vast majority of service providers when providing their services to EU users should be complying with EU standards and subject to supervision.

9. In your view, what governance structure could ensure that multiple national authorities, in their respective areas of competence, supervise digital services coherently and consistently across borders?
3000 character(s) maximum

Cooperation within member states will depend on the national regulatory framework, but cooperation could focus on case allocation between sectoral regulators or on holistic approaches to achieving policy goals.

10. As regards specific areas of competence, such as on consumer protection or product safety, please share your experience related to the cross-border cooperation of the competent authorities in the different Member States.

3000 character(s) maximum

We welcome the efforts to harmonise consumer laws across the EU with various consumer directives, and the CPC Network coordinated actions have in some respects helped to promote coherent enforcement.

As we set out above, we welcome the cooperation mechanisms provided for in consumer law framework, and support how these have been used by local authorities and the Commission—these mechanisms have allowed prompt action, and provided greater legal certainty for businesses by addressing fragmentation.

Our experience of the CPC Regulation since January 2020 is that the mechanisms to investigate and tackle cross-EU infringements are now more effective, allowing prompt cooperation on infringements with centralised help from the EU Commission, with new powers for local enforcement to protect services and their users from non-compliant traders. We welcome the prompt response to COVID-19 consumer scams by the European Commission and the CPC Network—in our view this is a good example of using the cooperation mechanisms to provide effective and coherent cross-border oversight.

For us, cooperation mechanisms such as the CPC Network Common Position and coordinated action are important in the context of a framework based on country-of-origin: they allow companies to make decisions to protect users based on consistent interpretation of the relevant laws, allowing more coherent solutions, and may reduce the need for lengthy enforcement procedures through multiple instances.

11. In the specific field of audiovisual, the Audiovisual Media Services Directive established a regulatory oversight and cooperation mechanism in cross border cases between media regulators, coordinated at EU level within European Regulators' Group for Audiovisual Media Services (ERGA). In your view is this sufficient to ensure that users remain protected against illegal and harmful audiovisual content (for instance if services are offered to users from a different Member State)? Please explain your answer and provide practical examples if you consider the arrangements may not suffice.

3000 character(s) maximum

We welcome the provisions of the revised AVMSD and the framework they present to support protecting users across Europe. Given that the implementation deadline is not yet past, it is too early to assess the sufficiency of ERGA's new role in cooperation mechanisms in cross border cases.

However, we welcome the possibility within ERGA for national regulators to exchange experience and best practices on the application of the regulatory framework; this provides an opportunity to promote consistency in national approaches and support the operation of country-of-origin.

The revised AVMSD recognizes the role that video sharing platforms (VSPs) play in protecting users against illegal AV content: VSPs take appropriate measures to protect users and provide tools to users who upload videos to help them comply with their own obligations (particularly where they themselves constitute a media service provider).

An important part of providing equal protection to European users is VSPs incorporating, applying, or offering the above processes and tools uniformly across borders: as VSP users consume content from, or offer content to, different countries and in different languages, they should not be presented with a wide range of varying, and potentially confusing, solutions. The revised AVMSD framework

recognizes the importance of clarity in process rules, and allows VSPs to be measured on their compliance measures through the country-of-origin principle.

The country-of-origin framework operates to allow VSPs and VSP channel owners to comply with their AVMSD obligations through the regulatory framework of their home state; we support this, but would identify this element as benefitting from cooperation that promotes consistency in national approaches. Such cooperation would be beneficial because these two types of actors (VSPs and channel owners) may be subject to varying obligations/incoherent national approaches if they are overseen by different home states.

For example, varying approaches to age-gating could mean that channel owners must rate their content in different ways for different territories, and would look to VSPs to offer age-verification measures to enable channel compliance with a divergent set of implementation rules across states. It is infeasible for VSPs to offer such tools, and would also either reduce the level of protection against harmful/illegal content due to the degradation in user experience, or at least lead to an inconsistent user experience across member states or depending on the origin of the content the user is consuming.

Consistency in transposition and enforcement will therefore be an important part of protecting users across Europe. To meet the challenges identified in the age-gating example above, cooperation within ERGA towards this end could include: guidance on the appropriate age at which age-verification measures should be applied, or best practices on tools those uploading AV content to VSPs can use to rate that content.

12. Would the current system need to be strengthened? If yes, which additional tasks [would] be useful to ensure a more effective enforcement of audiovisual content rules?
Please assess from 1 (least beneficial) – 5 (most beneficial). You can assign the same number to the same actions should you consider them as being equally important.

Coordinating the handling of cross-border cases, including jurisdiction matters	
Agreeing on guidance for consistent implementation of rules under the AVMSD	★★★★★
Ensuring consistency in cross-border application of the rules on the promotion of European works	
Facilitating coordination in the area of disinformation	
Other areas of cooperation	★★★★★

13. Other areas of cooperation - (please, indicate which ones)
3000 character(s) maximum

Open platforms such as YouTube allow users to consume and offer content across Europe, so we welcome cooperation between member states and national competent authorities aimed at protecting all European users equally from illegal content.

Any cooperation between Member States or regulators should be transparent, proportionate, and structured around clear objectives. It should also support country-of-origin, the legal certainty it provides to industry and the coherent approach it promotes to national oversight and enforcement regimes.

Promoting consistency.
As we set out above, we welcome the possibility within ERGA for national regulators to exchange experience and best practices on the application of the regulatory framework; this provides an opportunity to promote consistency in national approaches and support the operation of country-of-origin.

The Commission may wish to explore increased cooperation, including between member states in the Contact Committee or competent authorities through ERGA (as appropriate) that is aimed at reducing conflicting approaches within the framework (e.g. through the development of guidelines).

Smooth functioning of country-of-origin.
Cooperation between NCAs may also be important to aid the smooth functioning of the country-of-origin framework. There may be a need to clarify how Member States are to prepare and maintain the list of MSPs under their jurisdiction: structured cooperation and information exchange within ERGA may help avoid excessively burdensome requirements to media service providers under the jurisdiction of another member state.

Structured reporting.
We welcome the opportunity that a forum such as ERGA presents to help regulators monitor the impact of existing policies and to better understand emerging trends: this is an important part of protecting users from illegal content. To this end, future regulation could facilitate structured reporting mechanisms that will support better understanding of relevant issues across the 27 member states, e.g., regular reporting from NRAs on predetermined data points or metrics.

14. Are there other points you would like to raise?
3000 character(s) maximum

As regards compliance frameworks related to illegal content, the Commission may wish to explore mechanisms to support the development of generally accepted international standards. Today, online platforms successfully leverage an array of compliance frameworks for security, privacy, finance, trade etc. Many of these compliance frameworks are rooted in international standards like ISO, established best practice, and sector specific guidelines. The Commission may wish to explore including mechanisms in the DSA that support the development within the EU of international standards for compliance frameworks related to addressing illegal content.

[End]