Facebook response to the public consultation for the European Democracy Action Plan

Table of contents

Introduction

Facebook welcomes the opportunity to respond to the Public Consultation for the European Democracy Action Plan. We endorse the European Commission's objectives to safeguard election integrity and ensure electoral systems are free and fair; freedom of expression is supported by strengthening media freedom and media pluralism; the role of civil society; and tackling disinformation.

This response is divided into two parts. The first part - Part 1: Facebook's views on protecting European democracy - outlines our observations and viewpoints around the key themes and questions asked in this Consultation, which constitute our initial thoughts on potential regulatory updates or gaps that might work based on our experience on these matters, in Europe and beyond. It provides a perspective on the specific policy areas that, in our opinion, the European Commission should prioritize for the European Democracy Action Plan.

The second part - Part 2: Public Survey for European Democracy Action Plan (Questionnaire) - is our response to specific questions in the survey.

We want to work constructively with policymakers in shaping the rules for the internet. Our CEO, Mark Zuckerberg, has been calling for new regulation around numerous areas, but particularly election integrity.[1] In the EU, we have called for changes to strengthen political advertising laws, and we are a signatory of the EU Code of Practice on Disinformation, which we believe has helped facilitate constructive dialogue and collaboration between industry and government.

We look forward to a fruitful and effective discussion with EU policymakers and stakeholders on the European Democracy Action Plan.

Part 1: Facebook's views on protecting European democracy

In this section, we outline our views around the key themes and questions asked in this Consultation, which constitute our initial thoughts on potential regulatory updates or gaps that might work based on our experience on these matters, in Europe and beyond.

To that end, we present key elements of Facebook's own work to protect elections and the integrity of our platforms. We have invested heavily to protect the integrity of elections and combat misinformation. Part 1 sets out some of the key efforts on this front, including:
- Preventing interference
- Removing harmful content
- Partnering with independent third party fact-checkers to reduce the spread of misinformation
- Increasing transparency
- Connecting people with accurate and authoritative information
- Combatting coordinated inauthentic behaviour and influence operations
- Working with government authorities, law enforcement, security experts, civil society and other tech companies to stop emerging threats
- Supporting news organisations and journalists

---

[1] M Zuckerberg, 'The Internet needs new rules. Let's start in these four areas', *Washington Post*, 31 March 2019, https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html; M Zuckerberg, 'Big Tech needs more regulation', *Financial Times*, 17 February 2020, https://www.ft.com/content/602ec7ec-4f18-11ea-95a0-43d18ec715f5

1. Election integrity and political advertising

A. Protecting the integrity of elections

Protecting the integrity of elections while preserving freedom of expression is a top priority for Facebook. Using lessons from the past and input from experts and policymakers across the political spectrum, we've made substantial investments in teams and technologies to better secure elections and are deploying them where they will have the greatest impact.

We now have more than 35,000 people around the world working on safety and security. Their job is to monitor for suspicious activity, quickly identify content and behavior that violates our policies, remove it, and prevent it from being used again. We have 40 teams involved in this work – with more than 500 people tasked solely to elections.

Our strategy to protect elections not only applies during critical times, but year-round, and is centered around three areas:

1. Preventing interference;
2. Removing harmful content and reducing misinformation; and
3. Increasing transparency

i. Preventing interference

A key part of our strategy to prevent interference is working with government authorities, law enforcement, security experts, civil society and other tech companies to stop emerging threats by establishing a direct line of communication, sharing knowledge and identifying opportunities for collaboration.

We have advanced our security operations to take down manipulation campaigns and identify emerging threats. Our teams of expert investigators actively look for and take down coordinated networks of inauthentic accounts, Pages and Groups that seek to manipulate public debate. We have removed tens of thousands of pages, groups and accounts involved in coordinated inauthentic behavior – more than 50 networks in 2019 alone – and block millions of fake accounts every day so they can't spread misinformation.

We updated our inauthentic behavior policy to further improve our ability to counter new tactics and more quickly act against the spectrum of deceptive practices we see on our platforms - whether foreign or domestic, state or non-state.

For more information on our thinking and approach to tackling disinformation, see section 3 below on Tackling disinformation.

ii. Removing harmful content and reducing misinformation

We apply a three-part strategy - remove, reduce, and inform - to manage problematic content across the Facebook family of apps. This involves removing content that violates our policies, reducing the spread of problematic content that does not violate our policies but still undermines the authenticity of the platform, and informing people with additional information so they can choose what to click, read or share.

- **Remove:** We remove content that violates our Community Standards, including fake accounts and accounts engaged in inauthentic behavior, misinformation that may contribute to the risk of imminent violence or harm, voter fraud or interference, hate speech, bullying and harassment. We also remove ads that violate our Advertising Policies, including ads with debunked claims by third-party fact-checkers or, in certain circumstances, by authoritative bodies, as well as our Community Standards.

- **Reduce:** Problematic content that does not meet the standards for removal under our Community Standards but still undermines the authenticity of the platform, such as clickbait and content debunked by our third-party fact- checkers, are demoted in the News Feed. This significantly reduces the number of people on Facebook and Instagram who see that content.

- **Inform:** We help prevent the spread of misinformation by providing additional context and connecting them with accurate information so people can make informed decisions. Here are some examples:

  - **Misinformation labels:** Content across Facebook and Instagram that has been rated false or partly false by our fact-checkers are prominently labeled so people can better decide for themselves what to read, trust, and share.

  - **Connecting people to accurate and authoritative information**: We launch products, such as Voter Registration and Election Day Reminders, to connect people with accurate information about when and how to vote. In the US, we are testing a Voting Information Center on Facebook and Instagram, which serves as a one-stop-shop to give US voters the tools and information they need to make their voices heard at the ballot box.

  - **Additional context about content people share:** We recently introduced a new notification screen that lets people know when news articles they are about to share are more than 90 days old.

  - **Media & digital literacy:** We are also investing in media and digital literacy initiatives to raise awareness and help people be more critical about the information they see. Section 4 below outlines our thinking around digital education.

iii. Increasing Transparency

We believe increased transparency leads to increased accountability. We provide an industry-leading level of transparency around political advertising and pages so people can see who is trying to influence them. This includes:

- **Verifying Political Advertisers:** To run a political or social issue ad, advertisers must go through our authorization process, which includes proving who they are and where they live.

- **Political and Issue Ads:** Ads about social issues, elections or politics include "Paid for by" disclaimers to show who's behind the ad. These ads are then housed in a public searchable Ad Library.

- **Page Transparency:** On Facebook, we show information about a Page, such as when it was created, name changes, and the location(s) of the Page admins. We will also start labeling media outlets that we believe are wholly or partially under the editorial control of their government as state-controlled media.

- **News Feed Ranking:** People can click on "Why Am I Seeing This" in posts and ads to understand why they are seeing them and control what they see from friends, Pages and Groups in the News Feed. This is the first time that we've built information on how ranking works directly into the app.

B. Transparency in political advertising

Internet platforms have lowered traditional barriers to political engagement, connected new participants to the political system, and expanded opportunities for the expression of political

views. However, the same tools that enable this expanded engagement and access to information have opened new vulnerabilities during electoral cycles. Facebook and other internet platforms have a responsibility to help defend the integrity of the democratic process.

In the absence of widely agreed upon norms or laws that set out how digital platforms should defend elections, platforms like ours have sought to answer some of the most pressing questions around issues like the opacity of political advertising and foreign interference in domestic civic events. At present, there is no industry-wide best practice or a common regulatory framework that provides clear rules and definitions in this area, across all EU member states, and we welcome the development of EU-wide rules and standards.

One of our goals is to ensure that our services contribute to a healthy civic life. We believe that regulations that create clear, industry-wide standards for political advertisers are key to creating a fairer and more transparent environment across online platforms during elections. Regulatory guidance on requirements in this space would ensure a level playing field, and enable voters to understand who is running campaigns and who is seeing those campaigns.

Facebook has taken an industry-leading position on political ad transparency, introducing new tools that go beyond what is currently required of us by law in many countries and go further than any other platforms that allow political advertising. But we do not think that it should be the responsibility of online platforms to set the standards for political advertising and we encourage the EU to consider what more can be done to ensure fairness and transparency in elections in the EU.

i. Greater clarity in definitions and requirements

Because political expression, particularly around elections, is a fundamental feature of the democratic process, we believe that governments - rather than private platforms - should define:

1) Which entities are eligible to engage in political advertising online;
2) What steps such entities must take when purchasing online political advertising; and
3) What constitutes a political advertisement online.

In the EU, we also believe a common regulatory framework across all member states is needed. The current patchwork of definitions for political advertising across the EU makes consistency across platforms and across countries a challenge.

Regulation should set forth which entities are eligible to engage in political advertising online and how disclosures will reveal the identity of the person or entity behind an ad, creating common criteria for how to verify an entity that purchases online advertisements.

Regulation should specify clearly what an eligible entity that wants to engage in political advertising must do in order to do so legally.

Regulation should also provide clear definitions of what constitutes a political advertisement online. Is a political ad just when an advertisement mentions or features a candidate or a ballot measure? Does it matter who paid for the ad? What about social issues? How would the list of issues be defined?

Deciding whether an ad is political isn't always straightforward, and Facebook's approach is guided by the principle that Facebook should not act as the arbiter of truth. Our systems would be more effective if regulation created common standards across the EU that help define what constitutes a political advertisement.

Which definition a government regulator prefers may depend on the outcome they are trying

to achieve. For example, if a government chose to implement a blackout period that would forbid any "political ads" for a certain period of time ahead of an election, it may opt for a narrow definition, to avoid banning ads dealing with advocacy on social issues. Other governments may prefer a broader definition to ensure the transparency of any paid content that might be relevant to an electoral outcome.

When deciding on the definition, it is also important to decide when regulation should apply. Facebook believes that the regulated period should not be limited to election periods. This means that outside of an election period, political campaigns can build audiences and influence public debate with very little transparency.

Currently at Facebook, we have taken a broad definition for political advertising and adopted a policy that applies to all "ads about social issues, elections or politics" so that transparency obligations and other requirements can be imposed on a wide category of ads that could influence political discourse. Any advertiser - both political and non-political - who wants to run ads targeting countries in the EU that are about a candidate for public office, a political figure, political parties, elections (including "get out the vote" campaigns) or social issues (civil and social rights, crime, economy, environmental politics, immigration, health, political values and governance, and security and foreign policy) will be required to confirm their identity by submitting identification document(s) issued by the country where they want to run the ad. We also require political advertisers to insert a "paid for by" disclaimer either on or alongside each advertisement so that anyone who views it can see the sponsor of the ad. The disclaimer may include more information about the "paid for by" entity, such as the organization's email address, website, phone number and physical address. In all cases, however, it is up to the advertiser to comply with any applicable electoral or advertising laws and regulations in the country they want to run issue, electoral or political ads in.

Political ads are then archived in the Ad Library for 7 years. This archive offers a range of additional information that shows what other ads political campaigns are running, including who paid for them, where they ran, and information on who the ads have reached. (For more information on Ad Library and political advertising policy, see [here](#).)

Given the integral role of journalism in the democratic process, we have exempted qualified news publishers in certain EU markets from our political advertising policies. In doing so, we are acknowledging the crucial difference between news reporting about social issues and campaigning materials from politicians, lobbyists and advocacy groups. News publishers [registered in the news Page index](#), who meet additional criteria, are exempt from the authorization and disclaimer process for ads about social issues, elections or politics. However, ads with opinion-based content about social issues, elections or politics are required to be authorised and have a "Paid for by" disclaimer. Regulation for political advertising should consider whether specific types of actors, such as news organisations, should be exempted from the rules.

We also believe it is important to consider carefully how responsibilities should be allocated in any updated regulatory framework. The primary responsibility for the legality of political campaigns should lie with those who run those campaigns. While platforms can build systems that allow for accurate disclosure of required information, the primary onus for providing accurate information should be on advertisers given the scale and volume of online political advertising and platforms' limited ability to verify off-platform and offline information. Platforms like Facebook can restrict the ability of an individual that we catch providing a false ID from using our services. But this is minor compared to the types of sanctions only governments can do, like disqualify someone from an election or impose criminal or civil penalties.

ii. Establishing a common EU regulatory framework
One of the key issues identified during the European elections in 2019 was the need for a

common regulatory framework across the EU to address cross-border political advertising. To hold advertisers accountable across the EU is a highly complex task, given the variety of political systems, national electoral regulations and the number of local, regional, and national elections (each with its own complexity) that are taking place in different EU countries throughout the year. Adding to this complexity is the fact that European elections run across all EU member states every five years.

Electoral laws in the EU are determined and enforced at the national level, for both the European and national elections. Election regulators typically have little or no ability to enforce against anyone who is outside their jurisdiction. If people are allowed in other countries to run political ads, then there may not be an effective way for the local election regulator in any particular country to enforce against these campaigns, especially within the short time frame of the election period.

Taking into account local regulatory frameworks, we designed our ad transparency policies to mitigate the risk of foreign interference, by requiring advertisers to fulfill specific identity confirmation and disclaimer requirements for each country they would like to target. Therefore, an organization that would like to advertise in multiple EU countries would need to have a local representative complete the ad authorisation requirements for each of those countries. During the European elections, this process frustrated advertisers who wanted to run pan-EU political ad campaigns but did not have the structure in place to meet our single-country ad targeting requirements.

The question about "foreign" actors also needs to be considered in this respect. In the EU, some countries have electoral rules that make distinctions between citizens and foreign actors, where the rights of a foreign individual to engage in the political debate are reduced, which may include rules banning foreign donations (including in-kind donations such as funding of ad campaigns) to political parties and candidates. If foreign actors have fewer rights to engage in the political debate of another country, how would "foreign" be measured, given the supra-national nature of the EU? Would people or governments from one EU country campaigning in another EU country's election be considered "foreign"? Would it be considered interference if a citizen, organization or government of one member state runs ad campaigns to influence the outcome of an election in another EU country?

These questions and challenges point to a need for a common EU regulatory framework. The current patchwork of regulation across the EU not only makes consistency across platforms and across countries a challenge, but also ignores the cross-border nature of political communication in a digital age. Having different obligations and uncoordinated enforcement measures imposed by different Member States is inefficient and counter-intuitive.

Moreover, variation in the strictness of election campaign regulation between EU countries potentially exposes the entire EU bloc to certain vulnerabilities. Campaigners may choose to run ads in countries with less strict or poorly regulated electoral systems, and influence public discourse across the EU. Also, restrictions on foreign funding of political campaigns vary across the EU. Countries like Belgium have no restrictions, while Germany has partial restrictions and Poland fully bans foreign donations. This means that foreign money can flow unimpeded into campaigns in a number of member states.[2]

iii. Targeting of ads
We believe that the answer to the challenges we face is not to suppress political speech, but to protect against abuse by those who would seek to interfere in elections, and to increase transparency so that it is clear who is trying to influence people's vote.

---

[2] https://www.gmfus.org/blog/2018/10/09/foreign-funding-threats-eus-2019-elections

Digital political ads, due to their low cost and ability to reach relevant audiences, have leveled the playing field between big and small political actors and expanded the accessibility of paid political speech. Targeted online advertising has created opportunities for advertisers who do not have the resources to invest in broadcast media, such as television and print. These traditional forms of advertising tend to advantage incumbents, as well as well-resourced candidates and campaigns.[3]

Targeting tools benefit local candidates, grassroots campaigners, and insurgent candidates, who are often taking on incumbents with well-established funding sources. It allows smaller campaigns to spend money advertising to relevant audiences that will likely vote for them. It also allows political advertisers to reach groups of voters that may not be accessible through other media.

Our advertising enables smaller advertisers, first-time candidates and non-profits to play a bigger role in political discourse. For example, a local group called EmpowerLA used Facebook to recruit local volunteer candidates for their neighborhood councils. Using our targeting tools they were able to drive over 17,000 potential voters to the city clerk's election registration portal. This would not have been possible without targeting tools.

In the Netherlands, the Pirate Party has stated that targeting is necessary because they would not have enough budget for larger-scale campaigns. "If we were to focus on the whole of Utrecht, we would not get a response," said a party spokesperson.[4]

In a recent academic study published in the [American Political Science Review,](#)[5] it was noted that "Social media lowers barriers to entry and thereby exposes voters to information about a broader set of candidates and offices... Voters see proportionately more Facebook ads from challengers and down-ballot candidates relative to television… [and] appears to foster more intense electoral competition… These are largely positive developments for American democracy."[6]

For larger political advertisers that require broader reach, targeting smaller groups won't always help them achieve their goals. For example, in January 2020 at the height of the US primary season, over 85% of spend by U.S. presidential candidates on Facebook is for ad campaigns targeted to audiences estimated to be greater than 250,000.

And although an important tool for political campaigning, how much a campaign spends on targeted ads alone does not guarantee victory or defeat in an election. In the 2019 UK general election, for example, the Conservatives spent significantly less than Labour or the Liberal Democrats on targeted ads on Facebook, yet won the election.[7] In the Irish general election this year, Sinn Féin spent far less money on their Facebook ads than their primary political opponents - Fine Gael and Fianna Fáil - yet won the most first-preference votes and achieved the largest increase in seats of any party.[8]

It is important to note that we already removed thousands of categories from targeting related to protected classes such as race, ethnicity, sexual orientation and religion. Strict data privacy rules in the EU also place certain targeting restrictions, such as on personal data regarding people's 'political opinions'.

Rather than limiting targeting, we believe that a better approach is increasing advertising transparency by providing important information about social issue, electoral or political ads, including:

---

[3] https://www.marketplace.org/2020/03/11/social-media-political-advertisements/
[4] https://nos.nl/artikel/2223364-vvd-in-je-tijdlijn-omdat-je-tennist-partijen-storten-zich-op-slimme-targeting.html
[5] https://doi.org/10.1017/S0003055420000696
[6] https://doi.org/10.1017/S0003055420000696
[7] https://www.bbc.com/news/election-2019-50785051
[8] https://www.euronews.com/2020/02/10/ireland-election-how-sinn-fein-dominated-the-social-media-campaign

- The entity responsible for the ad;
- Total political ad spend by advertiser;
- Basic demographic information about who saw the political ad, including age range and gender; and
- Range in ad spend and impressions for each political ad, as well as its potential reach

Last year, we updated the Ad Library to include Potential Reach, which provides the public with information on how big of an audience the advertiser aimed to reach with the ad. This increased transparency enables everyone to see and assess the use of our ad tools. We believe the information about who is running the ad and who actually sees the ad best aligns with effective platform transparency.

In addition to transparency, we believe it is important to give people more control over the ads they see, which is why we introduced tools like "Why am I seeing this ad?" and Ad Preferences more than five years ago. These tools provide different options for people to control how data can and can't be used to show ads.

Earlier this year, we rolled out a control to let people choose how an advertiser can reach them via Custom Audience lists. People have always been able to hide all ads from a specific advertiser in their Ad Preferences or directly in an ad. But now they are able to stop seeing ads based on an advertiser's Custom Audience list — or make themselves eligible to see ads if an advertiser used a list to exclude them.

For political and social issue ads, we recently introduced controls for people to see fewer of these types of ads on Facebook and Instagram. Through the Ad Preferences tool, people are able to turn off all social issue, electoral or political ads from candidates, Super PACs or other organizations that have the "Paid for by" political disclaimer on them. We've launched this option in the US to start, and we aim to make it available in countries where we have enforcement on ads about social issues, elections and politics later this fall.

Finally, just as imposing restrictions around the content of political ads implicates core speech rights, so too does limiting targeting. Some have argued that, "microtargeting is a form of political communication, and thus is an exercise of the right to freedom of expression, which is guaranteed by both Article 11 of the EU Charter of Fundamental Rights, and Article 10 of the European Convention on Human Rights (ECHR)."[9] This is not to say that regulating targeting is necessarily inconsistent with the right to freedom of expression; but, as with other restrictions on speech, policymakers should consider whether there are narrowly tailored options that preserve free speech while also addressing concerns about targeting.

Ultimately, we support and welcome engagement in a robust conversation about targeting, but we believe that conversation should weigh both the costs and benefits of the practice.

iv. Offline versus online political advertising rules

Retrofitting the rules that regulate offline advertising for the online world may be appropriate in some instances, but may not be possible in others.

A number of countries limit overall political expenditures by candidates, or, alternatively, require political organizations to report advertising expenditures. Facebook believes the decision on whether to limit political advertising expenditures should remain within the purview of democratic governments.

---

[9] https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe

There is also the concept of "airtime", which would be an exceptionally challenging one to translate into the online space. Even if regulation placed limits on - for example - the number of people a political advertiser would be permitted to target with an ad, the ad could be further disseminated through organic (unpaid) sharing.

At the same time, Facebook supports transparency measures that allow users to understand which political content is paid for, by whom, and for what purpose. A regulatory focus on transparency, if implemented correctly, can increase public accountability and improve governance. For example, requiring "paid for by" disclaimers on political ads would allow journalists, watchdogs, civil society and people in general to better scrutinize the funding entity behind the ads.

v. Meaningful accountability

Our Ad Library provides a public, searchable ad database that allows journalists, regulators, watchdog groups, researchers, academics and people in general to hold advertisers accountable. To help people scrutinize the ads in the advertising ecosystem, the Ad Library provides a comprehensive, searchable collection of all currently active ads (political and non-political) running across Facebook apps and services; an archive of political ads that remain in the library for 7 years; and aggregated insights. We have made several updates to these tools since they were first launched. As we continue to receive feedback about these tools, we will make improvements to make it more insightful to people.

We believe meaningful accountability comes from a holistic look at a platform's overall content moderation system. In order to meaningfully audit platforms' systems, widely agreed global standards against which platforms can be evaluated are needed. Currently, none exist, so a first step would be to formulate such standards. These standards should ideally be formulated based on industry expertise, but with broad buy-in from global regulators, academics, and civil society to minimize fragmentation of oversight and multiple conflicting standards.

Whilst we understand the desire for a broader range of competent authorities, social science researchers and civil society to have access to more information, there are a number of potential concerns with such access and it would be desirable to have this coordinated through a voluntary cooperation scheme. It is important that such requests should have a defined and reasoned base or outcome, underpinned by the need for good regulatory outcomes. Of particular concern is the risk of bad actors gaming the platforms once the information from researchers and civil society becomes available. Additionally, there are potential business confidentiality, security, user privacy and competition concerns with interrogation of systems by third parties. There are specific data security risks that are involved with sharing datasets with third parties - not just GDPR and the security risks that may arise from sharing business data, but also information such as how our AI algorithms work, which could be used by bad actors to learn how to circumvent our integrity measures.

2. Strengthening media freedom and media pluralism

Facebook is committed to supporting journalism and we want to help news organizations as they adapt to the changing digital world. We support regulation that will help the relationships between technology companies and news organizations. Meaningful collaboration allows us to jointly build innovative and sustainable solutions to support journalism. We support this idea because journalism is important to society and a healthy democracy.

A. Investing in tools and programs to support the news business

Working with publishers globally, we're investing in tools and programs that help news

businesses adapt to the changing digital landscape. We want to collaborate with more news partners worldwide. We want to see quality journalism thrive online and off.

Our support for news publishers comprises: free organic distribution of news on our platforms that grows the audience for news publishers; customised tools and products to help news publishers monetise their content; initiatives to assist publishers to innovate with online news content; direct investments by commissioning news content that can appear on online services, including Facebook; and the indirect value to publishers such as brand awareness and community-building.

By providing publishers a wider audience through free distribution, and investing in free tools and programs specifically designed to drive readership, Facebook can encourage and support sustainable business models. The following are some of the projects we're currently working on:

Expanding Facebook News: We are accelerating our plans to expand Facebook News internationally. We are considering the UK, Germany, France, India and Brazil for launching within the next six months to a year. Wherever we decide to launch next, we aim to have commercial deals with high quality news publishers to ensure their content is available in the new product. Helping publishers reach new audiences has been one of our most important goals - in the US where Facebook News has first launched, we've found over 95% of the traffic Facebook News delivers to publishers is incremental to the traffic they already get from News Feed.

More tools to support the subscription business: News organizations around the world are increasingly focused on subscriptions to help drive their business. We have built a new account linking tool that provides a better experience for people on Facebook when they see and access content from publishers they subscribe to. We're collaborating with publishers around the world to test this new product.

Building enduring business value through the Global Accelerator Program: We will continue our investment in our premiere business training program, one of the most successful collaborative programs we've built with the industry. To date, the more than 120 publisher participants in the program have generated over $30 million in customer lifetime value since the program's inception in 2018.

Supporting entrepreneurship in journalism around the world: A thriving future for news requires more entrepreneurs to start tomorrow's great journalism companies. To that end, we have made a substantial investment in a new online certificate program for niche media entrepreneurs at the Craig Newmark Graduate School of Journalism. This program will train dozens of journalistic entrepreneurs from around the world over the next several years.

COVID-19 relief: The news industry is working under extraordinary conditions to keep people informed during the COVID-19 pandemic. At a time when journalism is needed more than ever, ad revenues are declining due to the economic impact of the virus. Local journalists are being hit especially hard, even as people turn to them for critical information to keep their friends, families and communities safe. As part of Facebook's work to keep people safe and informed about the coronavirus, we committed $100 million in COVID-19 relief support for the news industry. Publishers are sharing ways funds have been used to finance critical reporting and cover investment in sustainable business transformation.

Supporting fact-checking organizations and combating COVID misinformation: Fighting the spread of misinformation on our platform is one of our biggest focus areas. We have partnered with over 70 third-party fact-checking organizations worldwide who are certified through the non-partisan International Fact-Checking Network (IFCN) to identify, review and take action on this content. In response to COVID-19, we've been focused on supporting our fact-checkers abilities to combat the spread of health misinformation. We launched a $1M grant program to help organizations maintain or increase their capacity during this time. Most recently, we launched a global health fellowship, enabling 10 organizations in Africa, Asia, Europe, India, Latin America and the Middle East to bring on new team members to help them approach this complex and important topic.

B. Safety of journalists

We believe in press freedom and strongly support the right of journalists to work without fear for their personal safety or other repercussions. This is why it is important for companies like Facebook to help journalists stay vigilant about their safety on our platform.

One of the pillars for the Facebook Journalism Project is to provide tools and training for journalists. We've worked in consultation with the European Journalism Centre, the Committee to Protect Journalists, ConnectSafely, the Inter American Press Association (IAPA), the International News Safety Institute, and the James W. Foley Legacy Foundation to create resources designed specifically for journalists to help them protect their accounts and themselves on Facebook.

We offer our Safety Tips for journalists which we have also made available as a free eLearning course. This course shows journalists how to keep their accounts secure to help them stay safe online and protect their sources and contacts.

We also started to further protect personal Facebook profiles of journalists against online abuse in the US, Brazil, Mexico and the Philippines, and we plan to expand this to other countries. These protections for journalists include: additional account protections; security features that further protect information and online presence on Facebook; account security monitoring; additional support to help trouble-shoot potential harassment or bullying against accounts; updates on special features; and new tools and features built with journalists in mind.

C. Providing people with additional context and more transparency

People want to see information that is timely and credible. This is why we have prioritized providing more information about the news content people see, so they can decide for themselves what to read, trust and share. We are continuously introducing new features that will provide more context and transparency. Here are few examples of tools and features we have implemented:

Article context button: Articles posted by a news publisher on Facebook, for example, features a "context button" (that looks like *i*), which provides information about the source of the article, such the publisher's Wikipedia entry, related articles on the same topic, information about how many times the article has been shared on Facebook, where it is has been shared, as well as an option to follow the publisher's page.

Labelling state-controlled media: We have started labeling media outlets that we believe, based on our own research and assessment against a developed set of criteria, may be wholly or partially under the editorial control of their government as [state-controlled media](). To ensure we are transparent when it comes to paid content from these publishers, we also plan to begin labeling ads from state-controlled publishers later this year. We're providing greater transparency into these publishers because we believe they combine the opinion-making influence of a media organization, with the strategic backing of a state, and we believe people should know if the news they read is coming from a publication that may be wholly or partially under the influence of a government. The labels appear globally in the Ad Library Page view, on Pages, and in the Page Transparency section.

Articles more than 90 days old: We recently introduced a new [notification screen]() that lets people know when news articles they are about to share are more than 90 days old. To ensure people have the context they need to make informed decisions about what to share on Facebook, the notification screen will appear when people click the share button on articles older than 90 days, but will allow people to continue sharing if they decide an article is still relevant.

Prioritize original news reporting: We are updating the way news stories are ranked in News Feed to prioritize original reporting and stories with [transparent authorship](). Original reporting plays an important role in informing people around the world, from breaking a news story, to creating an in-depth investigative report, uncovering new facts and data, sharing critical updates in times of crisis, or broadcasting eyewitness reports. This important journalism takes time and expertise, and we want to ensure that it's prioritized on Facebook.

Demoting news content that does not have transparent authorship: We are starting to demote news content that does not have transparent information about the publisher's editorial staff. We will review news articles for bylines or a staff page on the publisher's website that lists the first and last names of reporters or other editorial staff. We've found that publishers who do not include this information often lack credibility to readers and produce content with clickbait or ad farms, all content people tell us they don't want to see on Facebook.

3. Tackling disinformation

As noted in this Consultation, "disinformation undermines the ability of citizens to form informed opinions" and can be "a tool for manipulative interference by external actors". It can amplify distrust and undermine the integrity of elections, governance and civic discourse. Tackling disinformation is a critical, continuous challenge for governments, industry, media, civil society and academia, and cross-sector cooperation is essential to combat sophisticated threat actors and preserve the community's trust in democracy.

Disinformation can manifest on social media, and Facebook has steadily increased our investments in tools, technology and infrastructure to enforce our policies and promote authentic communications via our services.

A. Greater clarity in definitions

In the debate about disinformation, there is much conflation and confusion between concepts such as disinformation, misinformation, foreign interference, influence/information operations, and even election integrity. In order to address the issues, the methodology in how it is addressed by various entities in different operational environments needs to be understood in more granularity. As disinformation applies and is used in a multitude of different operational environments and across multiple platforms and media surfaces, no one size fits all methodology to combatting it can be implemented.

Pertaining to one of the questions in this Consultation, we do not think the definition of "disinformation" needs to be broadened or complemented. Rather, we believe more clear and nuanced terminologies are needed to differentiate between the different components of the problem and to better align democratic concerns with security concerns. As noted in a paper[10] by the the Carnegie Endowment for International Peace:

> "The EU should first revise the terminology used to support disinformation policy and analysis to make it easier to distinguish between different aspects of the problem. Disinformation is currently used as a catchall term that does not help the EU institutions define different areas of problematic behavior. It muddles the actions of individuals inadvertently sharing incorrect information [i.e. misinformation] with the hybrid influence campaigns of hostile states."

At Facebook, instead of referencing "disinformation", we use the term **influence operations (IO)** to describe coordinated efforts that aim to manipulate or corrupt public debate for a strategic goal. Two key markers for influence operations are **inauthenticity** and **coordination.** To combat this threat, we have developed an inauthentic behaviour policy that targets coordinated efforts to manipulate public debate for a strategic goal, where fake accounts are central to the operation, and allows us to take down networks of accounts, pages and groups based on behavioral signals. There are two tiers of these activities that we work to stop: 1) coordinated inauthentic behavior in the context of domestic, non-government campaigns (CIB) and 2) coordinated inauthentic behavior on behalf of a foreign or government actor (FGI).

When we look at misinformation and influence operations, we differentiate between the two on the basis of behavior and content. When we look at influence operations, we focus on the **behaviour**, while with misinformation we focus on **content**. Misinformation refers to claims that are misleading or false, and it is necessary to identify misinformation through analysis of the content. Conversely, actors engaged in influence operations need not necessarily use misinformation; most of the content shared by IO campaigns are not provably false, and would in fact be acceptable political discourse if it was shared by authentic actors. The real issue is that the actors behind these campaigns are using deceptive behaviors to conceal the identity of the organisation behind a campaign, make the organisation or its activity appear more popular or trustworthy than it is, or evade enforcement efforts.

---

[10] https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286

While there may be some overlap (actors engaged in IO may also utilise misinformation), disinformation and misinformation are not the same. This is the view of numerous experts in this space, such as Camille Francois at Harvard University[11] and First Draft[12].

The distinctions between disinformation and misinformation is important, because the policy concerns underlying each differ, and the most appropriate response from platforms like Facebook will also be different. For example, we believe the appropriate role we should play in relation to disinformation is different in relation to misinformation. The next section on Actor, Behavior, Content-Based Enforcement explains in more detail why it is important to have clear delineations between disinformation and misinformation.

As policymakers decide on the appropriate measures to tackle disinformation, it is important that the terms and definitions are clear and precise, in order to educate the broader community and to ensure rules and regulations, as well as enforcement measures to hold relevant actors accountable (such as transparency reporting metrics), put in place are fit-for-purpose.

B. Actor, behavior, content-based enforcement

Facebook enforces against a broad range of violating activity across three specific areas:
1) Actor-based enforcement, which involves the removal of accounts or organizations because of the totality of their activity on the platform;
2) Behavior-based enforcement, which is predicated on specific violating behaviors exhibited by violating actors; and
3) Content-based enforcement, which predicates enforcement on specific violations of our Community Standards.

Dealing with integrity issues online is a complex problem. The public debate often treats this as a single problem, but the truth is that a variety of different problems rolled together. When we blur issues together as one problem set, it becomes very hard to develop a strategy to solve any one part. In accordance with other cross-sector approaches used across the influence operations environment, we intentionally break this problem out along these three dimensions - actors, behaviors, and content. For example, any potential violation could be conducted by a problematic actor (for example, a foreign government); using problematic behavior (for example, networks of fake accounts); or could distribute problematic content (e.g., misinfo or hate speech). We have specific policies that work along each dimension, and tailor our response to the nature of the violation. This gives us a range of tools to respond with. By combining all three dimensions, we have a network of enforcement operations. It's important to remember that there's no silver bullet, and all of them have to work together.

---

[11] C Francois, *Actors, Behavior, Content: A Disinformation ABC*, 20 September 2019, https://science.house.gov/imo/media/doc/Francois%20Addendum%20to%20Testimony%20-%20ABC_Framework_2019_Sept_2019.pdf
[12] H Derakhshan & C Wardle, 'Information Disorder: Definitions', *Understanding and Addressing the Disinformation Ecosystem*, December 2017, https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v4.pdf?x42643

C. Combatting coordinated inauthentic behaviour and influence operations

In the social media landscape and beyond, influence operations (IO) rely on **inauthenticity** -- where users misrepresent themselves, through fake profiles or non-transparent **behaviors**, for the purpose of manipulating or corrupting public debate -- and **coordination**. IO manifests in different ways on different platforms and in different fora.

Governments around the world have begun to propose and implement legislation and regulatory efforts to address this societal concern, creating a fragmented approach to a very global threat that has known commonalities, regardless of geography.

The below IO legislative principles consolidate approaches that we have seen work worldwide, in multiple governance structures, to foster cross-sector and collaborative ways to mitigate this threat within a consistent and cohesive global regulatory framework. We believe that approaching legislation or regulation in the IO space should be "pursued but accompanied by a regulatory package fixing overarching principles applicable to all information society services and establishing more detailed rules for dealing with disinformation under such general principles."

At a high level, IO legislation should, in collaboration with industry and civil society, promote:
1) Definitions of bad behavior and promote transparency best practices around private and public sector enforcement against those definitions;
2) Impose costs on the threat actors behind IO campaigns; and
3) Enable greater cross-sector information sharing on signals and collaboration to detect and deter threats.

It should strike a balance between effectively combating IO threats, while also protecting speech and the privacy of users. These would include:

● **Transparency in ads.** Require much greater transparency for contributions or expenditures for political advertising;

● **Reporting on inauthentic behavior.** Work with industry and civil society experts to provide minimum disclosure frameworks, collaborative development of transparency best practices, and the sharing of lessons learned, so there are parameters on what to report publicly on the impact of inauthentic behavior across social media and elsewhere to help governments, researchers and the public assess current risk.

● **Broad applicability.** Be crafted to cover IO broadly, as opposed to specific tactics of IO (e.g., the use of fake accounts), because IO manifests differently on different platforms and in traditional media, and narrow definitions will likely leave loopholes that attackers can exploit;

● **Increased information sharing.** Enable greater information sharing of IO threat signals among industry and between industry, civil society, and government, while protecting the privacy of innocent users who may be swept up in these campaigns;

● **Deterring violators.** Impose economic, diplomatic, and/or criminal penalties on the threat actors behind serious IO campaigns, understanding that different penalties and mitigations apply in foreign and domestic contexts;

- **Supporting technical research.** Support private and public innovation and collaboration on technical detection of adversarial threats such as manipulated media and deep-fakes.

- **Supporting media and digital literacy.** Support media and digital literacy to educate users and promote and strengthen societal resilience. (see section 4.A on Digital citizenship)

D. Misinformation

When it comes to misinformation, there is an inherently fraught definitional challenge - governments, policymakers, civil society, academics, and people in general do not agree on what misinformation is. Moreover, there is an important difference between **misinformation shared unintentionally** and misinformation shared intentionally to deceive - commonly referred to as "disinformation" (as described above).

Defining what constitutes misinformation (the unintentional form) is very challenging. Adding to the challenge is determining who decides if something is untruthful; who or what is the source of truth; and what should the penalties be. Any regulation attempting to address these questions risks capricious restrictions on legitimate speech. Some governments are looking at mis/disinformation as a category of harm. In the UK, for example, addressing mis/disinformation as **harmful content** "will ensure the focus is on protecting users from harm, not judging what is true or not."[13] However, deciding on what is harm can still be highly contextual, difficult to define, often culturally subjective, and legally ambiguous. Therefore, any regulation for harmful content would still need to recognise the need to balance the removal of harmful content with the protection of freedom of expression and other fundamental rights. For these reasons, many governments have explicitly opted not to engage in the arena of misinformation.

Our approach to misinformation is guided by the principle that we should provide people with accurate and informative content, while balancing free expression. Our users want to see high quality content on our platform, and so do we, which is why our strategy to combat misinformation has three parts: remove, reduce, and inform (as noted above in section 1.A - Removing harmful content and reducing misinformation).

We remove content that violates our Community Standards, which includes extreme forms of misinformation, including voter suppression, misleading manipulated videos and misinformation that contributes to imminent physical harm. For misinformation that doesn't violate our Community Standards, but nevertheless undermines the authenticity and integrity of our platform, our approach is to work with our network of independent third party fact-checking partners to reduce the distribution of misinformation, show strong warning labels and notify people who come across it, try to share it or already have. Based on one fact-check, we're able to kick off similarity detection methods that identify duplicates of debunked stories, applying the same enforcement penalties of reducing the distribution, showing warning labels, and notifying people.

We continue to find new ways to connect people with accurate, reliable and authoritative information. This is a core component of our strategy to combat misinformation because we want to be able to provide our users with the means to decide what to read, trust and share. Based on lessons from the COVID-19 pandemic, where having access to accurate information can mean the difference between life or death, we have launched a number of products, such as the COVID-19 Information Center. The Covid-19 Information center

---

13

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf#page=34

directs people to authoritative sources of information such as up to date information from international and local health authorities, resources and tips to stay healthy and safe and with the latest, localized, news sources. For elections, we provide Voter Registration and Election Day Reminders that direct people to official websites about when and how to register or vote.

Since 2019, we have taken a similar approach to misinformation about vaccines - in addition to removing widely debunked vaccine hoaxes from search results and group recommendations, we connect people with accurate information from health authorities such as the WHO on Groups and Pages that discuss vaccines, and when people try to search for this content on Facebook or Instagram.

Furthermore, informing people with accurate and authoritative information, as well as more context, is an approach that can be more impactful than the alternative of just removing content. If we simply removed all posts flagged by fact-checkers as false, the content would still be available elsewhere on the internet, other social media platforms, or even around the dinner table. By leaving this content up and surfacing research from fact-checkers or pointing people to authoritative information, we're providing people with important information and context.

The goal of our strategy around authoritative information is to launch features (such as the COVID-19 information Center) when communities or countries are facing certain threats, such as the COVID-19 health crisis, where the risk for widespread misinformation and user confusion about that threat is high, and there are widely agreed-upon authoritative sources and information that can be referenced. Our goal is to change people's behavior, attitudes or knowledge about those threats by making authoritative information more visible and accessible. By connecting people with clear, accurate and authoritative information, we aim to reduce the spread of misinformation and the efficacy of malicious networks that might try to take advantage of uncertainty and manipulate public discourse.

As noted by an [international group](#) of human rights experts (in relation to COVID-19): "it is essential that governments and internet companies address disinformation in the first instance by themselves providing reliable information… Resorting to other measures, such as content take-downs and censorship, may result in limiting access to important information for public health and should only be undertaken where they meet the standards of necessity and proportionality."[14]

4. Supporting civil society and active citizenship

The role of civil society and citizens is extremely important in developing policies to protect the integrity of democratic debate. Across Europe, we partner with many organizations that are working to strengthen democracy, good governance and election integrity. We also work with these organizations to help uncover and combat threats that we see to the integrity of elections and civic debate. These organizations include a wide variety of international and local NGOs that work with European-based research organizations, civil society and government oversight bodies to aid in that mission. This work is tailored across the bloc to support day-of and post-electoral environments based on the needs and challenges facing each country.

Supporting rule of law initiatives in transitioning democracies: Through our partnership with the International Foundation for Electoral Systems (IFES) and Stockholm-based International Institute for Democracy and Electoral Assistance (IDEA), we've supported and

---

[14] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729

trained civil society, election commissions and oversight bodies in the Western Balkans on how to use our tools like the Ad Library to conduct oversight as well as our other products on Instagram and Facebook to reach their constituents.

Strengthening civil society ahead of elections - Through our partnerships with the National Democratic Institute (NDI), International Republican Institute (IRI), Internews and Freedom House, we have designed our partnerships to support their networks with not only resources, but also trainings on how to best use our platforms for advocacy, outreach and oversight. We've trained civil society across the EU as well as the Western Balkans and Ukraine.

Supporting thought leadership in democracy - Facebook is a core sponsor and active partner for EU-based think tanks such as the Athens Democracy Forum, Munich Security Conference and the Copenhagen-based Alliance for Democracy. These organizations promote positive Trans-Atlanticism, democratic systems and open societies.

A. Digital citizenship

At Facebook, we are committed to help build safe, healthy and supportive digital communities. In order to do this, we need to think about the skills and support that people need to discern fact from fiction, build healthy relationships, stay safe, find greater well-being, build resilience, lead with empathy, communicate across diverse cultures, respect other perspectives, think critically about how they contribute to society and work together to make positive progress, online and off.

i. From digital literacy to digital citizenship

Given the multitude of online threats that a person may encounter, a broad set of skills and competencies are needed to safely and intelligently navigate the digital landscape - that goes beyond digital and media literacy. A holistic approach is necessary to equip people with the skills they need, where they are not only taught critical thinking or media literacy but also how to participate in digital society safely, respectfully and responsibly.

Digital citizenship is how we navigate our privileges and obligations in this new space. It is how we decipher and share information we have access to, and most importantly, how we interact with other people. We all play a part in creating responsible digital citizens and building a brighter digital future.

To build a resilient digital society and tackle some of the challenges democracies face, we need to look beyond digital literacy to digital citizenship. This is why we have expanded our efforts to tackle the problem more holistically. Here are some examples of how we are helping to develop digital citizenship:

- **Get Digital:** We recently launched a program, Get Digital, to provide lessons and resources to help young people stay safe online and protect their personal information; navigate content and information and evaluate the trustworthiness of a source; build positive and inclusive communities online by being kind and respectful; and develop healthy habits for when to use technology. There are also lessons that help develop digital skills, such as understanding algorithms, programming, as well as help prepare them for future careers in technology. It also helps them discover how technology can be used for civic and political engagement. These resources are

designed to be used by educators and families both in the classroom and at home, but they've become even more important as young people spend more time on their devices while at home during the COVID-19 outbreak. The Get Digital website is currently available in English, but will be expanding into other languages, including French, German, Portuguese, Italian, and Spanish, in the coming months.

● **Digital Literacy Library:** The Digital Literacy Library is available in 45 languages and is a collection of ready-to-use lessons for parents and educators looking to address digital literacy and helping young people build the skills they need to safely enjoy digital technology. The lessons were developed by the Youth and Media team at the Berkman Klein Center for Internet & Society at Harvard University, and aims to help young people between the ages of 11-18 to think critically and share thoughtfully online. The lessons address thematic areas such as privacy and reputation, identity exploration, security, safety and wellbeing, and more.

● **Media literacy campaign to stamp out false news:** We want to give people the tools to make informed decisions about the information they see online and where it comes from. To support this effort, a campaign was rolled out in countries across the EU to educate and inform people about how to detect potential false news. In consultation with some of our fact-checking partners, we developed 'Three questions to help stamp out false news', which appeared on Facebook adverts throughout July and August, directing people to a full set of tips on www.stampoutfalsenews.com. These adverts ask people to challenge the information they see on posts by asking themselves the following:
  1. Where's it from? If there's no source, search for one.
  2. What's missing? Get the whole story, not just the headline.
  3. How does it make you feel? People who make false news try to manipulate feelings.

ii. Multi-stakeholder collaboration

Fostering digital citizenship is a whole-of-society responsibility and cannot be achieved by any one stakeholder. It requires a multi-disciplinary strategy involving the full range of stakeholders, from government to industry to civil society, educators and citizens themselves. We believe the European Commission can play a role in facilitating more regular dialogue and collaboration between the range of relevant stakeholders by establishing a cooperation framework - this can be built on the work of the media literacy expert group, which Facebook has participated in.

At Facebook, working in partnership with experts, educators, civic society and governments around the world is central to our digital citizenship efforts. We have developed a series of tools and resources - such as online tutorials, lesson plans for educators, tips for spotting false news, and awareness-raising ad campaigns - to educate and equip people with the necessary skills for navigating the digital world. Our partners bring valuable subject matter expertise and are also important channels for distributing these tools and resources to a broader audience. Partners we work with include various government bodies (such as ministries of education and media regulators), our global network of third-party fact-checkers, parent-teacher associations, the European Association for Viewers Interests (EAVI), the UNESCO Institute for Information Technologies in Education (UNESCO IITE), Yale University, Harvard University, and Micro:bit Educational Foundation, and many more.

iii. Institutional support

Building on existing initiatives, such as the literacy provisions in the Audiovisual Media Services Directive (AVMSD) or the Digital Education Action Plan, we believe more institutional support in the form of funding and incentives are needed from the European Commission to promote the concept of digital citizenship. This should be part of a long-term strategy and education programme across the Member States that would not only apply to formal education, but also in non-formal education settings and through life-long learning opportunities, as referenced by the European Commission on past occasions. Facebook stands ready to collaborate and support, as far as digital platforms can, in these digital education efforts.

We welcome further discussions with EU policymakers and stakeholders on the role of digital platforms in supporting civil society and active citizenship, and more broadly on the European Democracy Action plan.

For more information about Facebook's submission, please contact:

Aura Salla, Managing Director EU Affairs
aurasalla@fb.com

Part 2: Public Survey for European Democracy Action Plan (Questionnaire)

Questions on election integrity and political advertising

(i) Transparency of political advertising

Q5. Online targeted political content may make use of micro-targeting techniques allowing advertisers to target with high precision people living in a specific location, of a certain age, ethnicity, sexual orientation or with very specific interests. Do you think that:

	Fully agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Fully disagree	I don't know/No reply
1. Micro-targeting is acceptable for online political content and it should not be limited	Fully agree, but with the exception of sensitive categories as identified by data privacy rules (see iii. Targeting of Ads)					
2. Criteria for micro- targeting of political content should be publicly disclosed in a clear and transparent way for every ad		Somewhat agree, see iii. Targeting of Ads				
3. Micro-targeting criteria should be strictly limited				Somewhat disagree, see iii. Targeting of Ads		
4. Micro-targeting criteria should be banned					Fully disagree, see iii. Targeting of Ads	

Please explain:

> See iii. Targeting of Ads

Q6. EU countries regulate offline political advertising on traditional media (e.g. press, television) in the context of local, national or EU elections. These rules limit the amount of airtime or maximum expenditure permitted for political advertising on broadcast TV or print media. Do you think similar rules should also apply to online targeted political content?

☐ Yes

☒ **No**

☐ I don't know

Please explain.

> See [iv. Offline versus Online Political Advertising Rules](#)

(ii) Threats to electoral integrity

Q1. Do you believe the following are real and existing threats to the electoral process in the EU and its Member States?

	Yes	No	Don't know
1. Intimidation of minorities	See [Protecting People from Bullying and Harassment](#)		
2. Intimidation of political opposition	See [Protecting People from Bullying and Harassment](#)		
3. Micro-targeting of political messages, that is messages targeted to you or a narrowly defined group		See [iii. Targeting of Ads](#)	
5. Disinformation or fake accounts run by governments, including foreign governments	See [How We Respond to Inauthentic Behavior on Our Platforms](#)		
6. Divisive content, that is content created to divide society on an issue	See [Investments to Fight Polarization](#)		
7. The amplification of content that makes it difficult for you to encounter differing voices	See [iii. Targeting of Ads](#)		
8. Intimidation of women candidates	See [Protecting People from Bullying and Harassment](#)		
9. I or someone I know has been targeted based on sensitive criteria such as gender, ethnicity or sexual orientation			
10. Content where I could not easily determine whether it was an advertisement or a news post			
11. Other	See [1.A Protecting the Integrity of Elections](#)		

[IF Q1=11: Please define]

> See section [1.A Protecting the Integrity of Elections](#).

(iv) European Elections

Q1. In your opinion, what initiatives at national level could strengthen monitoring and enforcement of electoral rules and support the integrity of European elections (multiple selections possible)?

☒ Strengthened sharing of information and monitoring activity across borders and between authorities

☒ Technical interfaces to display all political advertisements as defined by online service providers

☒ Technical interfaces to display all advertisements (political or not)

☒ Clear rules for delivery of political ads online in electoral periods, similarly to those that exist in traditional media (TV, radio and press)

☐ Independent oversight bodies with powers to investigate reported irregularities

☐ Enhanced reporting obligations (e.g. to national electoral management bodies) on advertisers in a campaign period

☐ Enhanced transparency of measures taken by online platforms in the context of elections, as well as meaningful transparency of algorithmic systems involved in the recommendation of content

☐ Privacy-compliant access to platform data for researchers to better understand the impact of the online advertisement ecosystem on the integrity of democratic processes

☒ Greater convergence of certain national provisions during European elections

☒ Stronger protection against cyber attacks

☒ Higher sanctions for breaches of the electoral rules

☐ Other – please specify

Q2. In your opinion what initiatives at European level could strengthen monitoring and enforcement of rules relevant to the electoral context?

☒ Strengthened sharing of information and monitoring activity across borders and between authorities

☒ European-level obligations on political advertising service providers

☐ European-level shared online monitoring and analysis capability being made appropriately available to national authorities

☒ Cross border recognition of certain national provisions

☐ Other

Questions on strengthening media freedom and media pluralism

(i) Safety of journalists / conditions for journalistic activities

Q1. Are you aware of issues regarding safety of journalists and other media actors or conditions for journalistic activities in your country?

☒ Yes (please justify)

☐ No (please justify)

☐ I do not know

Q1.1 If yes, what kind of issue?

☐ Lack of proper sanction applied to perpetrators of attacks against journalists–
Yes/No

☐ Abuse of defamation laws or other laws aiming at silencing journalists and news media –
Yes/No

☐ Lack of legal safeguards for journalistic activities – Yes/No

☐ Lack of institutions to protect journalists – Yes/No

☒ Online hate speech – Yes

☒ Cyberbullying – Yes

☐ Physical threats – Yes/No

☒ Other – please specify

Please explain

> See section 2.B Safety of journalists

(ii) Media independence and transparency

Q2. How important is the support for independent journalism (including free lance journalists and bloggers/web journalists) and the protection of the safety of independent journalists to supporting democracy in the EU and internationally?

☒ Very important

☐ Important

☐ Not important

☐ Don't know

Please explain

> See section 2 Strengthening media freedom and media pluralism

Q4. Should it be mandatory for all media outlets and companies to publish detailed information about their ownership on their website?

☒ Yes (please explain)

☐ No (please explain)

☐ I do not know

Please explain

> We think it is important to provide more background and information on the publishers and links that appear in News Feed so people can decide for themselves what to read, trust and share. We have launched a context button that appears alongside links to articles shared in News Feed. When clicked, the button opens a card showing the publisher's Wikipedia entry (if available), related links, information about how many times the link has been shared on Facebook and where it has been shared, if available.

Q5. Should content by state-controlled media, where governments have direct control over editorial lines and funding, carry specific labels for citizens?

☒ Yes (please explain)

☐ No (please explain)

☐ I do not know

Please explain

> We have also started labeling media outlets that we believe, based on our own research and assessment against a developed set of criteria, may be wholly or partially under the editorial control of their government as state-controlled media. To ensure we are transparent when it comes to paid content from these publishers, we also plan to begin labeling ads from state-controlled publishers later this year. We're providing greater transparency into these publishers because we believe they combine the opinion-making influence of a media organization, with the strategic backing of a state, and we believe people should know if the news they read is coming from a publication that may be wholly or partially under the influence of a government. The labels appear globally in the Ad Library Page view, on Pages, and in the Page Transparency section.

Q6. Do you think information from independent media and trustworthy sources should be promoted on online intermediary services (such as search engines, social media, and aggregators)?

☒ Yes (please explain)

☒ If yes, please give examples of how it could be achieved and how to distinguish sources to be promoted?

☐ No (please explain)

☐ I do not know

Please explain

> See C. Providing people with additional context and more transparency
>
> Content on Facebook is ranked based on a set of News Feed Publisher Principles:
> - People on Facebook value meaningful, informative stories
> - People on Facebook value accurate, authentic content
> - People on Facebook value standards for safe, respectful behavior
>
> These principles guide News Feed's ranking of the thousands of stories on average that vie for attention each day in a person's feed.
>
> People want to see reliable and credible information on Facebook. People tell us that authentic stories are the ones that resonate most, so we work hard to understand what type of posts people consider genuine so that we can rank them higher in News Feed. We work to understand what kinds of stories people find misleading, sensational and spammy, to make sure people see those less.

Q7. Do you think further laws or institutions should be put in place in your country to strengthen media independence and transparency in any of the following areas?

☒ Transparency of state advertising and state support to news media / journalism – Yes

☒ Transparency of media ownership – Yes

☐ Promotion of information from independent media and trustworthy sources– Yes/No

☐ Ownership limitations of commercial actors – Yes/No

☐ Ownership limitations of political actors – Yes/No

☐ Rules to prevent foreign (extra-EU) based manipulative and hate- spreading websites from operating in the EU - Yes/No

☐ Other – please specify

☐ No, what is in place is sufficient

☐ No

☐. I do not know

Please explain your answer

> See section 2 Strengthening media freedom and media pluralism

Q8. Do you think that the EU should act to strengthen media independence and transparency in any of the following areas? (Multiple answers possible)

☒ Transparency of state advertising and state support to news media / journalism – Yes

☒ Transparency of media ownership – Yes

☐ Promotion of information from independent media and trustworthy sources– Yes/No

☐ Ownership limitations of commercial actors – Yes/No

☐ Ownership limitations of political actors – Yes/No

☐ Other – please specify

☐ No
☐ I don't know

Please explain

> See section 2 Strengthening media freedom and media pluralism

Q9. If you answered yes to some of the options of the previous question, how should the EU act in these areas?
☐ By issuing guidance – Yes/No
☐ By setting up dedicated structured dialogue with Member States – Yes/No
☐ By providing financial support – Yes/No
☐ By adopting legislation – Yes/No
☒ Other – please specify

Please explain

> See section 2 Strengthening media freedom and media pluralism

Questions on tackling disinformation

(i) Scope

Q1. The April 2018 Commission Communication on Tackling online disinformation: a European Approach defines disinformation as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.[4]
Do you think this definition should be broadened and complemented to distinguish between different aspects of the problem?

[4] Public harm includes threats to democratic processes as well as to public goods such as Union citizens' health, environment or security. Disinformation does not include inadvertent errors, satire and parody, or clearly identified partisan news and commentary.

☐ Yes (please specify)

☒ No (please specify)

☐ Don't know

Please explain.

> We do not think the definition of "disinformation" needs to be broadened or complemented. Rather, we believe more clear and nuanced terminologies are needed to differentiate between the different components of the problem and to better align democratic concerns with security concerns. As noted in a paper[15] by the the Carnegie Endowment for International Peace:
>
> > "The EU should first revise the terminology used to support disinformation policy and analysis to make it easier to distinguish between different aspects of the problem. Disinformation is currently used as a catchall term that does not help the EU institutions define different areas of problematic behavior. It muddles the actions of individuals inadvertently sharing incorrect information with the hybrid influence campaigns of hostile states."

---

[15] https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286

In order to address the issues related to misinformation and disinformation, the methodology in how it is addressed by various entities in different operational environments needs to be understood in more granularity. As disinformation applies and is used in a multitude of different operational environments and across multiple platforms and media surfaces, no one size fits all methodology to combating it can be implemented.

For this reason, Facebook enforces against a broad range of violating activity across three specific areas: actor-based enforcement, which involves the removal of accounts or organizations because of the totality of their activity on the platform; behavior-based enforcement, which is predicated on specific violating behaviors exhibited by violating actors; and content-based enforcement, which predicates enforcement on specific violations of our Community Standards.

Dealing with integrity issues online is a complex problem. The public debate often treats this as a single problem, but the truth is that it's many different problems rolled together. When we blur issues together as one problem set, it becomes very hard to develop a strategy to solve any one part. In accordance with other cross sector approaches used across the influence operations environment, we intentionally break this problem out along the three dimensions - actors, behaviors, and content. For example, any potential violation could be conducted by a problematic actor (for example, a foreign government); using problematic behavior (for example, networks of fake accounts); or could distribute problematic content (e.g., misinformation or hate speech). We have specific policies that work along each dimension, and tailor our response to the nature of the violation. This gives us a range of tools to respond with. By combining all three dimensions, we have a network of enforcement operations. It's important to remember that there's no silver bullet, and all of them have to work together.

See also section 3 below on Tackling disinformation.

Q2. So far, the European Commission has addressed the spread of disinformation through a self-regulatory approach, which has resulted in a Code of Practice on Disinformation being subscribed by major online platforms and trade associations representing the advertising industry. Do you think that this approach should be:
[5] This question complements the questionnaire for the public consultation on the Digital Services Act, which focuses on illegal content
☒ Continued as it is currently pursued (status quo)
☐ Pursued but enlarged to a wider range of signatories
☐ Pursued but combined with a permanent monitoring and reporting programme
☐ Pursued but on the basis of a substantially reviewed Code of Practice
☐ Pursued but accompanied by a regulatory framework fixing basic requirements for content moderation, data access and transparency, as well as respective oversight mechanisms
☒ Pursued but accompanied by a regulatory package fixing overarching principles applicable to all information society services and establishing more detail rules for dealing with disinformation under such general principles
☐ Replaced by special regulation on disinformation
☐ Abandoned altogether, as all forms of restriction or control on content posted online by internet users and which is not illegal in nature (e.g. illegal hate speech, incitement to terrorism) could endanger freedom of speech
☒ Other (please explain)

Please explain.

See section 3 Tackling disinformation.

Q3. Have you ever encountered the following measures to reduce the spread of disinformation on social media platforms?

	Yes	No	Don't know
1. Alerts when attempting to share or publish content that has failed a fact- check by journalists or a fact-checking organisation	See Facebook's Approach to Fact-Checking: How It Works		
2. Notifications to users who have previously engaged with content or sites that have failed a fact-check by journalists or a fact-checking organisation	See Facebook's Approach to Fact-Checking: How It Works		
3. Clear labels above content or sites that have failed a fact-check by journalists or a fact-checking organisation	See Facebook's Approach to Fact-Checking: How It Works		
4. Mechanisms allowing you to report disinformation	See How to report a post as false news?		

Q3.1 If yes, on which platforms have you encountered this?
☐ Google
☒ Facebook
☐ Twitter
☐ YouTube
☐ WhatsApp
☐ Other (Please specify)

(ii) Disrupting the economic drivers for disinformation

Q1. What type of measures should online platforms and advertising networks operators take in order to demonetise websites that create, present or disseminate disinformation?[6]

[6] Please note that this question refers to monetisation of websites that systematically publish false or misleading information, which is not illegal in nature. Monetisation via advertisement placements of web sites publishing illegal content is addressed within the context of a separate questionnaire for the public consultation on the Digital Services Act.

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/No reply
1. Establish and regularly update lists of websites identified by fact-checkers as systematic sources of disinformation (black list approach) and publish them			See Enforcing on repeat offenders			
2. Establish and regularly update lists of websites identified by fact-checkers as systematic sources of disinformation (black list approach) and remove the ad accounts concerned			See Enforcing on repeat offenders			
3. Establish and regularly update lists of websites identified by fact-checkers as systematic sources of disinformation (black list approach) and temporarily suspend the ad accounts concerned			See Enforcing on repeat offenders			
4. Establish and regularly update lists of websites identified by fact-checkers			See Enforcing on repeat			

as occasional sources of disinformation (grey list approach) and give the advertisers the possibility to selectively exclude such websites			offenders			
5. Block ad accounts only for those websites that engage in deceptive behaviour (e.g. spamming, misrepresentation of identity, scraping content from other sources, containing insufficient original content, etc.)			See Disabled Ad Account			
6. Ensure a systematic scrutiny of websites providing advertisement space and limit ad placements only on those websites that are considered trustworthy by reputable indexes (white list approach)						
7. Ensure transparency of platforms vis-à-vis advertisers and provide for third-party verification (e.g. position of the ads, the content the ads are run next to, metrics)						
8. Other						

Q2. Paid-for content on issues of public interest is promoted on social media platforms both during and outside electoral periods. Due to the special prominence given to such paid-for content in news-feeds and other systems for displaying content online, users may be misled as to its credibility or trustworthiness, irrespective of the veracity of the content. Do you think that issue-based advertising / sponsored content of political context:

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/No reply
1. Should be systematically labelled	See policy for Ads about social issues, elections or politics					
2. Should be systematically labelled and collected in public, searchable repositories	See Ad Library					
3. Should be subject to the same rules as on political advertising (see above section)	See policy for Ads about social issues, elections or politics					
4. Should not be regulated					See 1.B Transparency in Political Advertising	

(iii) Integrity of platforms' services

Q1. Do you think there should be targeted regulation at EU or national level to prohibit deceptive techniques such as the use of spam accounts and fake engagement to boost posts or products?

☐ Yes
☐ No
☐ Don't know
☒ Other - See section 3 Tackling disinformation.

Q1.1 If you replied yes to the previous question, what do you think should be the most appropriate measures to tackle the above-mentioned manipulative techniques and tactics?

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/No reply
1. Label the content as artificially promoted						
2. Demote the content to decrease its visibility						
3. Suspend or remove the content because the use of manipulative techniques is contrary to platforms' terms of service						
4. Suspend or remove the accounts engaging in manipulative techniques						
5. Invest in internal intelligence systems to detect manipulative techniques						
6. Invest in artificial intelligence to detect manipulative techniques						
7. Other	See section 1.B Transparency in Political Advertising and section 3 Tackling disinformation					

(iv) Enhancing users' awareness

Q1. Do you agree that the following kinds of measures would help enhance user's awareness about how platforms operate and prioritise what users see first?

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree
1. Promoting content from trustworthy sources	See Helping Ensure News on Facebook Is From Trusted Sources and Prioritizing Original News Reporting on Facebook				

2. Promoting factual content from public authorities (e.g. on COVID-19)	See Keeping People Safe and Informed About the Coronavirus					
3. Providing tools to users to flag false or misleading content	See How to report a post as false news?					
4. Demoting content fact-checked as false or misleading	See Facebook's Approach to Fact-Checking: How It Works					
5. Labelling content fact- checked as false or misleading without demoting	See Facebook's Approach to Fact-Checking: How It Works					
6. Platforms should inform users that have been exposed to fact-checked content	See Facebook's Approach to Fact-Checking: How It Works					
7. Removing content which is found false or misleading and contrary to terms of service (e.g. threatening health or public safety)	We remove misinformation that could contribute to imminent physical harm.					

Which sources do you consider as trustworthy?

> We prioritize news from publications that the community rates as trustworthy. These trusted sources were determined by surveying a diverse and representative sample of people using Facebook to gauge their familiarity with, and trust in, various different sources of news. This data informs ranking in News Feed.
>
> We also promote accurate and authoritative information from commonly recognized authorities, such as an election commission or public health organisation.

Q2. In your opinion, to what extent, if at all, can the following measures reduce the spread of disinformation?

	No contribution	Minor contribution	Little contribution	Major contribution	Don't know
1. Demotion of posts or messages that have failed a fact-check by journalists or a fact-checking organisation in the newsfeed				See Facebook's Approach to Fact-Checking: How It Works	
2. Alerts if attempting to share content that has failed a fact-check by journalists or a fact-checking organisation				See Facebook's Approach to Fact-Checking: How It Works	
3. Notifications to users who have previously engaged with content that has failed a fact-check by journalists or a fact-checking organisation				See Facebook's Approach to Fact-Checking: How It Works	
4. Clear labels above content that has failed a fact-check by journalists or a fact-checking organisation				See Facebook's Approach to Fact-Checking: How It Works	
5. Mechanisms enabling readers to flag content that is misleading				See How to report a post as false news?	

6. Mechanisms to block sponsored content from accounts that regularly post disinformation				See Enforcing on repeat offenders	
7. Closing of fake accounts and removal of automated social media accounts like bots				See How Does Facebook Measure Fake Accounts?	
8. Closing of accounts that continuously spread content that has failed a fact-check by journalists or a fact-checking organisation				See Enforcing on repeat offenders	
9. Allowing more diversity in suggestion algorithms designed to find videos, posts or sites that you might be interested in					
10. Other					

Q2.1. IF your answer=10, Please specify:

See section 3 Tackling disinformation.

Q3. To what extent, if at all, do you support the following measures to reduce the spread of disinformation?

	Do not support at all	Do not support	Neither support nor discourage	Support	Support fully	Don't know
1. Demotion of posts or messages that have failed a fact- check by journalists or a fact-checking organisation in the newsfeed					See Facebook's Approach to Fact-Checking: How It Works	
2. Alerts if attempting to share content that has failed a fact- check by journalists or a fact-checking organisation					See Facebook's Approach to Fact-Checking: How It Works	
3. Notifications to users who have previously engaged with content that has failed a fact-check by journalists or a fact-checking organisation					See Facebook's Approach to Fact-Checking: How It Works	
4. Clear labels above content that has failed a fact-check by journalists or a fact-checking organisation					See Facebook's Approach to Fact-Checking: How It Works	
5. Mechanisms enabling readers to flag content that is misleading					See How to report a post as false	

					news?	
6. Mechanisms to block sponsored content from accounts that regularly post disinformation					See Enforcing on repeat offenders	
7. Closing of fake accounts and removal of automated social media accounts like bots					See How Does Facebook Measure Fake Accounts?	
8. Closing of accounts that continuously spread content that has failed a fact-check by journalists or a fact-checking organisation					See Enforcing on repeat offenders	
9. Allowing more diversity in suggestion algorithms designed to find videos, posts or sites that you might be interested in						
10. Other						

Q3.1 IF your answer=10, Please specify:

> See section 3 Tackling disinformation.

What safeguards and redress mechanisms do you consider appropriate and necessary to avoid errors and protect users' rights?

> Publishers are able to dispute a fact-check rating issued by a third party fact checker on content they created if they believe it is inaccurate. They can do this by reaching out directly to the third-party fact-checking organization. Fact-checkers are responsible for evaluating the validity of each correction. If a fact-checking partner decides to change a rating based on a dispute, the demotion on the content will be lifted, associated ad disapprovals may be lifted, and the strike toward the Page or domain becoming a repeat offender will be removed.
>
> Pages and profiles are not able to dispute fact checks on content they did not create themselves. However, if the publisher that wrote the original content successfully issues a correction or disputes the rating, the enforcement on the Page will be lifted.

Q6. End-to-end encrypted messaging services (such as WhatsApp, Telegram or Signal) can be used to spread false and harmful content. In your view, should such platforms introduce measures to limit the spread of disinformation, with full respect of encryption and data protection law (more than one reply is possible)?

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/No reply
1. Introduce easy-to- find reporting or flagging system for users	See Report issues to WhatsApp					
2. Limit the possibility to forward the same content to many users	See Keeping WhatsApp Personal and Private					

3. Limit the amount of people in a discussion group		See [WhatsApp Group Participants](#)				
4. In exceptional cases, proactively contact users about potential disinformation wave or promote authoritative content (e.g. in cases like Covid-19 pandemic)		See [Fact Checking Organizations on WhatsApp](#); [WHO Health Alert brings COVID-19 facts to billions via WhatsApp](#)				
5. Other (please elaborate)			See [Stopping Abuse: How WhatsApp Fights Bulk Messaging and Automated Behavior](#)			

Other: please explain

Private messaging services differ in key ways from public social media platforms, and the disinformation challenge plays out differently on these services as a result. The approach to tackling disinformation on these services should reflect these differences, as well as those between messaging services. While efforts to address the challenge will be most effective if they are tailored to each service, we believe they should fall into three broad categories: tackling abuse at the account level based on behavioural signals and other available information, not content; integrity features in the product; and connecting people with authoritative sources and advice.

WhatsApp, for example, is designed to help people communicate directly with their friends and loved ones. Approximately 90 percent of the messages sent on WhatsApp are one-to-one, the maximum group size is 256 and the majority of group chats include fewer than ten people. There are no algorithms to promote content, and users do not build audiences or discover new people as they would on social media. Preventing unsolicited communication is built into the design of the service. A user must have someone's phone number to contact them on WhatsApp, and when a WhatsApp user receives a message from an unknown number, we immediately ask them if they want to allow messages from, block or report the sender of the message. Further, WhatsApp is designed to limit spam and virality through product features like forward limits and through measures to detect and ban accounts engaging in bulk messaging or automated behavior. WhatsApp messages and calls are protected by end-to-end encryption, which means no one except the sender and recipient can see the content, not even us. End-to-end encryption is essential to protect people's private conversations and keep them safe from criminals and hackers.

In light of WhatsApp's nature and purpose, its approach to tackling disinformation focuses on three key areas: tackling [abuse at the account level](#) based on behaviour-based signals and other available information not message content; introducing features in the product to [limit virality](#) and [empower users](#); and connecting people with [authoritative sources of information](#), education and tips. To this final point, we don't believe private messaging services should proactively notify users of potential disinformation because doing so could counterproductively raise awareness of rumours or disinformation and would violate users' expectations of

privacy. Instead, private messaging services should work with partners and use other channels to raise awareness and to make it easier for people to find authoritative sources of information should they wish to do so. We believe this three pronged approach is the most effective way to help address the disinformation challenge while protecting people's ability to communicate freely, privately and securely on messaging services.

Q10. Do you think it should be mandatory for online platforms to offer oversight bodies that enable users to seek recourse in case their account has been locked or content they have posted has been deleted?

☐ Yes
☐ No
☐ Don't know

Please explain

Every day, platforms like Facebook make difficult decisions about what content should stay up and what should come down. As our community has grown to more than 2 billion people, we have come to believe that Facebook should not make so many of those decisions on its own — that people should be able to request an appeal of our content decisions to an independent body.

To do that, we have established an external oversight board that is a body of independent experts, coming from a diverse set of disciplines and backgrounds, who will review Facebook's most challenging content decisions - focusing on important and disputed cases. It will share its decisions transparently and give reasons for them. The board will be able to reverse Facebook's decisions about whether to allow or remove certain posts on the platform. Facebook will accept and implement the board's decisions. The purpose of the board is to provide oversight of how we exercise that responsibility and to make Facebook more accountable.

Aside from the oversight board, Facebook users may also request a review if they disagree with content that has been taken down or an account that has been disabled.

Q11. Do you think it should be mandatory for online platforms to provide points of contact for each Member State in their language?

☐ Yes
☒ No
☐ Don't know

Q13. How should the EU respond to foreign state and non-state actors who interfere in our democratic systems by means of disinformation (multiple answers possible)?

	Yes	No	Don't know
1. Analyse and expose state-backed disinformation campaigns	See Coordinated Inauthentic Behavior Reports		
2. Conduct public awareness-raising campaigns	See section 4 below on Supporting civil society and active citizenship		
3. Support independent media and civil society in third countries			
4. Impose costs on state who conduct organised disinformation campaigns			

5. Develop more effective public outreach and digital communication strategies			
6. Other, (please specify)	See section [3 Tackling disinformation](#)		

Q14. In your opinion, should content by state-controlled media outlets be labelled on social media?

☒ Yes - see [Labeling State-Controlled Media On Facebook](#)
☐ No
☐ Don't know

For more information about Facebook's submission, please contact:

Aura Salla, Managing Director EU Affairs
aurasalla@fb.com