ANNEX II CURRENT BEST PRACTICES FROM SIGNATORIES OF THE CODE OF PRACTICE

Current Practices from Signatories of the Code			
Subject Area	**Best Practice Principles**	**Links to Policies/Actions**	**Explanation**
Advertising Policies	Platforms endeavour to tackle disinformation by pursuing follow the money approaches to disinformation and preventing bad actors from receiving remuneration.	Facebook false news policy	Policies disrupting economic incentives for people, Pages, and domains that propagate misinformation by removing accounts and content that violate our Community Standards or ad policies; reducing the distribution of false news and inauthentic content like clickbait and by informing people by giving them more context on the posts they see.
		Facebook's ads policy	Examples of prohibited types of content (including false and misleading content) and consequences for failure to comply with local law and regulations, and Facebook's rules and standards
		Google Policy on misrepresentation	Ads policy that prohibits the placement of Google ads on pages that misrepresent, misstate, or conceal information about themselves, their content, or the primary purpose of their web properties; also prevents monetization of content about politics, social issues, or matters of public concern to users in another country if the advertiser misrepresents or conceals its country of origin or other material details.

		Google's Annual Bad Ads Report	Example of transparency currently provided on advertising policies and enforcement.
		Twitter ads policy	Ads policy highlighting the responsibility of advertisers on Twitter, covering issues such as, links within ads, as well as for transactions and sales promoted through Twitter Ads.
		Twitter ads quality policy	Transparency rules and requirements for advertisers on Twitter.
Political advertising policies	Online platforms are developing solutions to increase transparency of political advertising and enable consumers to understand why they are seeing ads. Platforms are also developing tools so that civil society can better understand the political online advertising ecosystem.	Facebook *View Ads* and *Pages Transparency* services	Controls for users to view more information about Pages and their active ads - this enables transparency about the full range of political actors' ads
		Facebook political advertising policy	Policies allowing advertisers to run political, election related and issue ads, provided they comply with all applicable laws and processes required by Facebook.
		Facebook "Why am I seeing this ad" service	Controls for users to determine what ads they see and explanations why.
		Google ad settings for consumers	Controls for consumers to determine what advertisements they see
		Google political advertising policy	Policy for political ads that includes

			restrictions on targeting to consumers
		Twitter Ads Transparency Centre	Transparency dashboard for both users and non-users providing transparency on all ads running on Twitter.
		How Twitter ads work	Information and controls for users on how Twitter Ads work, why you see certain ads, your privacy settings and other options.
		Twitter Political Campaigning Policy	Policy around political campaigning advertising on Twitter, including country specific restrictions.
Service integrity policies	Platforms endeavour to tackle disinformation by applying policies which limit the abuse of the platform by inauthentic users.	Facebook misrepresentation policy	Authenticity policies restricting impersonation and misrepresentation, and holding users and Pages accountable.
		Facebook spam policy	Policies restricting commercial spam, and the use of misleading or inaccurate information to collect likes, followers, or shares.
		Facebook transparency report (about fake accounts)	Report on enforcement of Community Standards including reporting on the removal of fake accounts.

		Google work on authoritative content	Google's improvements to algorithms in Search to prioritize authoritative sources
		YouTube spam policy	Policies restricting spam.
		YouTube impersonation policy	Policy restricting impersonation on YouTube
		Google News content policies	Content policies which require content to be accountable and transparent by providing accurate bylines and datelines and contact information for the publication. News policies also prohibit impersonation, misrepresentation or concealment of ownership or primary purpose, and coordinated activity to mislead users.
		Google Webmaster Guidelines	Guidelines for web publishers explaining the most common forms of deceptive or manipulative behavior that will cause a page to be removed or lower ranked in Google's search products.
		Twitter rules on automation and misrepresentation	Rules and transparency around automated applications or activities on Twitter.
		Twitter impersonation policy	Twitter policy regarding impersonation, for example, accounts portraying another

			person in a confusing or deceptive manner may be permanently suspended under the Twitter impersonation policy.
		Twitter Spam policies	Rules and transparency around how Twitter tackles and defines spammy behaviour, for example, users may not use Twitter's services for the purpose of spamming anyone. Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or the experience of users on Twitter to drive traffic or attention to unrelated accounts, products, services, or initiatives.
		Twitter inactive account policy	Policy and enforcement around inactive accounts.
		Mozilla Conditions of Use Policy	Conditions of use policy which prohibits users from undertaking any activity which would deceive, mislead, defraud, phish, or commit or attempt to commit identity theft via Mozilla's services.
Policies and actions to	Platforms endeavour to tackle disinformation by providing users with	How is Facebook's fact checking program working?	Information on Facebook's partnership with third-party fact-checking organizations.

empower consumers	information, tools and support to empower consumers in their online experience. These measures may also include redress and reporting systems.	Facebook consumer advice on false news	Resources for users on how to identify and limit the spread of false news.
		Facebook trusted sources strategy	Policies that prioritize news content from sources the community rates as trustworthy.
		Facebook News Feed transparency site and Inside Feed blog	Information for consumers about how News Feed works and describing changes in the NF algorithm
		Reporting false news on Facebook	Tools for users to report false news.
		Google fact check tools for developers	Tools for fact check organizations to include their content in Search and News results on Google
		Google ad settings for consumers	Controls for consumers to determine what advertisements they see
		Twitter user personalisation and data settings	User controls and personalisation on how data is used on Twitter.
		Reporting Twitter Ads	Procedures for users on how to report advertising on Twitter.
		Mozilla Information and Trust Initiative (MITI)	MITI is a comprehensive effort to develop products, research, and communities to battle information pollution and disinformation, e.g. Community Repository

			of Misinformation Research
		The Mozilla Firefox 'Facebook Container' extension	An add-on that allows Firefox users manage various parts of their online life without intermingling their accounts.
		Mozilla's lightweight Firefox Focus	Privacy focused mobile browser
		Mozilla's The Coral Project	The Coral Project provides a variety of open source tools to help news organisations engage more closely with their audiences. This provides various ways for journalists to work more closely with their communities to identify misleading or false information, as well as helping community members identify such behavior within the comments, for newsroom action.
		Mozilla's community participation guidelines	Community participation guidelines that are applicable to the broad Mozilla community (staff, volunteers, contributors, etc)
		Mozilla's Transparency Report	Annual transparency report that gives insight into how the company deals with public and private entities across products such as Firefox and Pocket.

Policies and actions to empower the research community	Platforms encourage research into disinformation and political advertising including on their platforms.	Facebook Elections Research Council	Initiative to support independent and credible research on the role of social media in elections and democracies more broadly.
		Facebook Social Science One partnership	Partnership to support research on the effects of social media on democracy and elections, with access to Facebook data.
		Datacommons.org project on sharing fact check data	Cross-industry research project that Google participates in that shared fact check data with academic researchers
		Twitter "Do more with data" initiative	Examples from data scientists for getting the most out of Twitter data.
		Twitter Guest blogpost: Inferring Jakarta Commuting Statistics from Twitter Data.	UN pulse lab example of Twitter data provide real-time information on many issues including the cost of food, availability of jobs, access to healthcare, quality of education, and reports of natural disasters.
		EU DisinfoLab's report on Developing a disinformation detection system and sourcing it live – case study of the 2018 Italian elections	
		Twitter external health metric proposal	Twitter proposal for partnership with outside experts to help identify health is measured on Twitter, touching on issues including: shared attention, shared reality, variety of opinion, and receptivity.

		Mozilla Information and Trust Initiative (MITI)	MITI is a comprehensive effort to develop products, research, and communities to battle information pollution and disinformation, e.g. Community Repository of Misinformation Research
		Mozilla Fellowship Program	Provides a platform for technologists and policy experts to undertake actionable solutions-orientated research into some of the key challenges facing the internet ecosystem today. Several fellows across Mozilla's programs, such as Renee DiResta, have been undertaking cutting-edge research on online disinformation and web literacy.
		Mozilla's Reality Redrawn	A programme sponsoring public demonstrations, using mixed reality and other art media that make the power of misinformation and its potential impacts visible and visceral.

Best practices of the advertising industry in the field of brand safety

Reducing the risk of ad misplacement, upholding brand safety and protecting the integrity of digital advertising requires collective actions by all actors involved in buying, selling and facilitating digital advertising. This includes advertisers, advertising agencies, trading desks, advertising platforms, advertising networks, advertising exchanges, sales houses and publishers.

The following are examples of brand safety-related tools and measures that the advertising industry deploys across different channels in order to minimise the risk that advertisements are placed next to content which advertisers do not wish their advertisements to appear alongside. This could include (but is not limited to) hate speech, child pornography, intellectual property infringement activities, radicalised content, content which incites terrorism, contextually inappropriate content (e.g. an advertisement for an airline alongside a news article about a plane crash) or content which does not match the beliefs or values of the advertiser.			
Advertising	**Contractual agreements:** All parties in the advertising ecosystem may include specific stipulations in service contracts with their media and/or technology partners related to limiting the exposure of their or their clients' ads next to certain types of content.		Relates to commitment 1.1. on Scrutiny of Ad Placement. Why this relevant to disinformation: Agreements can include limited exposure of ads on websites known to host "disinformation content".
Advertising	**Independent content verification technologies**: Where appropriate, advertising intermediaries, and advertisers, work with third party ad verification companies to ensure that certain brand safety standards are met. These companies verify content via keywords, metadata and URL analysis, among others. These companies can be accredited by industry bodies against industry established principles. Their adherence to these standards is independently audited and certified by cross-industry bodies, such as the Media Rating Council in the United	The Media Rating Council in the (MRC) Trustworthy Accountability Group (TAG) Joint Industry Committee for Web Standards in the UK (JICWEBS) Digital Ad Trust in France	Relates to commitment 1.1. on Scrutiny of Ad Placement. Why this relevant to disinformation: Verified content can include content on websites known to host "disinformation content".

	States (MRC), Trustworthy Accountability Group (TAG), Joint Industry Committee for Web Standards in the UK (JICWEBS), Digital Ad Trust in France, and other national cross-industry initiatives.		
Advertising	**Due diligence in media buying**: Advertisers and/or their agencies may negotiate to buy directly from trusted publishers and agree on protective terms and conditions with them. This will depend on the buying model agreed by advertisers.		Relates to commitment 1.1. on Scrutiny of Ad Placement. Why this relevant to disinformation: Publishers host content that has undergone editorial control, which considerably limits the risk of exposure of ads next to"disinformation content".
Advertising	**Use of blacklists or whitelists**: Some advertising intermediaries and advertisers may require the use of internal blacklists or whitelists, which include and/or exclude certain websites, URLs, etc. Advertising intermediaries and/or advertisers may contractually require their partners to implement them. It has to be noted that such lists are illegal in certain countries and/or require a law and controlling entity to be set up in other countries. For example, in the UK the advertising industry has worked together to develop a blacklist of illegal websites backed by law enforcement.	Example of use of blacklists backed by law enforcement: https://bit.ly/2J4NRVZ	Relates to commitment 1.1. on Scrutiny of Ad Placement. Why this relevant to disinformation: blacklists can contain websites/domains that are known to host "disinformation content" or that reportedly engage in clickbait or other illegal practices.
Advertising	**Standards, codes, memorandum of**	Consolidated ICC Code of Advertising and	ICC Code

	understanding: The advertising industry adheres to the International Chamber of Commerce (ICC) Code promoting high standards of ethics, and responsible advertising and marketing communications, which includes, for example, provisions on transparency around different types of content. Advertisers and advertising intermediaries are signatories of the Memorandum of Understanding on online advertising and Intellectual property rights (IPR), which aims to minimise placement of ads on websites and apps that infringe IPR on a commercial scale.	Marketing Communication Practice (ICC Code) Memorandum of Understanding on online advertising and Intellectual property rights (IPR)	Relates to commitment 2.1. on Political advertising Why is this relevant to disinformation: clearly distinguishes advertising from other types of content, e.g. editorial content. It also adds transparency around paid-for communication. MoU Relates to commitment 1.1. on Scrutiny of Ad Placement. Why this relevant to disinformation: The MoU is a successful example of a voluntary industry process, whereby representatives of the advertising ecosystem commit to minimise the placement of advertising on certain websites and mobile applications, thereby disrupting the revenue stream of these websites and apps. In the case of the MoU, such websites and apps infringe copyright or disseminate counterfeit goods. Being associated with such content or practices presents a considerable risk to a brands' safety and reputation.
Transparency in digital advertising	**Ads.txt**: IAB Tech Lab's Ads.txt, which stands for Authorized Digital Sellers, increases transparency in the programmatic	About ads.txt How to & Help with ads.txt	Relates to commitment 1.1. on Scrutiny of Ad Placements.

supply chain	advertising ecosystem. By creating a public record of sellers, ads.txt creates greater transparency in the inventory supply chain, and gives publishers control over their inventory in the market, making it harder for bad actors to profit from selling counterfeit inventory across the ecosystem. As publishers adopt ads.txt, buyers are able to more easily identify the Authorized Digital Sellers for a participating publisher, allowing brands to have confidence they are buying authentic publisher inventory.		Why is this relevant to disinformation/fake news: Ads.txt increases transparency in the programmatic advertising ecosystem. It allows buyers to check the validity of the sellers they purchase from, thus it helps buyers avoid spoofed domains that may be created by purveyors of disinformation with the intention of misleading readers that the website has been created by a credible entity
Transparency, Control and Choice in Digital Advertising Chain	**IAB Europe Transparency and Consent Framework ('Framework')**: The Framework is a global cross-industry effort to help publishers, technology vendors, agencies and advertisers meet the transparency and user choice requirements under the General Data Protection Regulation (GDPR). The Framework has been created to offer flexibility to comply with the law, and provide a means of transmitting signals of consent from a user to third party vendors working with publishers. A registry of vendors has been created as part of the Framework and publishers can use the registry to view which of the vendors they	IAB Europe Transparency and Consent Framework Publishers' resources Vendors' resources Consent Management Providers' resources	Relates to commitments 2.1., 2.2., 2.3. on Political and issue-based advertising. Why is this relevant to disinformation: The Framework allows the recording of user consent for setting cookies or similar technical applications that access information on a device, in line with applicable legal requirements, and signaling of the consent status through the online advertising ecosystem. The user can give consent for the data processing required for ads to be served.

	work with are part of it. The Framework enables companies that collect and process data or access consumers' devices to collect and process data to continue to do so and comply with GDPR law.		