October 2019 · Dr. Julian Jaursch

Regulatory Reactions to Disinformation

How Germany and the EU are trying to tackle opinion manipulation on digital platforms

Stiftung Neue Verantwortung

Think Tank at the Intersection of Technology and Society

Executive Summary

Deliberate deception, spreading falsehoods and hate speech are not new phenomena of the digital media environment but rather age-old societal problems. Disinformation in the digital sphere reaches a new dimension, however, because social networks, video portals and search engines can be easily used and abused for such purposes. The risk arises that political attitudes become distorted, extremist sentiments reinforced and confidence in institutions such as elections, parliaments and the media undermined. That poses serious challenges for democratic societies.

At the German state and federal levels, and at the EU level, political decisionmakers are reacting to the disinformation dilemma. Attempts at crafting regulations and political solutions, however, have so far been hardly suitable for constraining disinformation. The German Network Enforcement Act (NetzDG), for example, which essentially aims to more quickly remove illegal content according to criminal law – such as an inciting tweet – does not apply to most disinformation online. This is mainly due to the fact that disinformation often operates in a legal borderline area, which makes it unclear exactly what is covered by freedom of expression, and what is in fact illegal.

Existing measures by the European Commission are not a suitable means for curbing disinformation, either. The voluntary EU Code of Practice Against Disinformation, for example, called on platforms to disclose online political advertisements. But the publicly accessible databases offered by Facebook, Google and Twitter were underdeveloped and incomplete, and the Code of Practice does not stipulate any sanctioning mechanisms. The EU itself already recognized these weaknesses in self-regulation and is now considering a "Digital Services Act" – a legislative package that could lay down clear rules for platforms, as well as means to sanction.

Effective measures against disinformation could also emerge in other regulatory areas such as media oversight, though this has not been the case so far. One example is the Interstate Media Treaty, which Germany's federal states are developing at the moment. According to the draft treaty, some social networks, search engines and video portals will be put under some type of regulatory oversight for the first time. The proposed reporting obligations for companies to explain their search and sorting algorithms could be helpful in addressing the problem of disinformation. Regulations governing algorithm transparency could, in theory, provide a better understanding of how the algorithm-managed news environment works. But even those rules are not

concrete enough, and the same could be said about transparency rules for online political ads.

Taken as a whole, the approach to tackle disinformation has been uncoordinated and piecemeal. It does, however, mark a first attempt to deal with a societal problem that touches on questions of freedom of expression, the influence of information and communication technologies on political decision-making, the weakening of journalistic gatekeeping and the market power of big global corporations. In the future, precisely because so many difficult topics are concerned, it makes sense to tackle disinformation by combining solutions from different legal and political fields.

First, it is necessary in the short-term to enforce existing rules more stringently. That not only pertains to criminal law, but also to privacy law, because the personalized, attention-propelled news environment of social networks, video portals and search engines – places where disinformation spreads particularly well – only functions by way of extensive tracking and profiling. Strict enforcement of privacy rules, from the EU's General Data Protection Regulation (GDPR), for example, can at least limit such data collection. But for party-political communications on the internet, including political ads, clear guidelines have yet to be created that combine the law on political parties, media regulation and data protection.

In the medium term, a closer integration of data protection and competition law, under consideration now for some time, could account for how the data and market power of some large companies facilitates the spread of disinformation. That begs the question of how appropriate oversight mechanisms for digital services like social networks and search engines could be designed in the future. Such debates are already taking place in other countries. A specialized agency for social networks is already being discussed in France and in the United Kingdom, for example. Such an agency could focus on the ways in which disinformation is spread (as opposed to removing individual pieces of content) and oversee whether and how companies have established the necessary processes.

Any political solution must be evidence-based. This means that research institutions and regulatory authorities must be able to analyze the extent and impact of disinformation in the digital realm. At the current juncture, such analyses are often impossible – large companies rarely allow researchers access to their data. In order to create useful studies, academics and regulatory decisionmakers must have better access to data in accordance with privacy rules.

Acknowledgements

Many thanks to the entire SNV team for their support and exchange of ideas during the initial phase of the project, especially “Team Digital Public Sphere” consisting of Raphael Brendel, Polina Garaev, Stefan Heumann, Riccardo Ramacci, Alina Rathke, Sebastian Rieger, Alexander Sängerlaub and Ben Scott. A heartfelt thanks also goes to numerous partners from government administrations, and the worlds of academia, civil society, media and business, who have contributed their expertise, assessments and experiences in workshops and in cafés, over the phone and at conferences.

Table of Contents

Executive Summary 2

Acknowledgements 4

Introduction 6

How microtargeting, personalization and network effects facilitate the spread of disinformation 10

Regulatory Measures for Tackling Disinformation 12
- Self-regulation 14
- Content Moderation 16
- Media Regulation 19
- Competition X Privacy 22

Conclusion and Outlook 25

Bibliography 31

Introduction

Three days, members of 11 parliaments, and 80 testimonies: The "International Grand Committee on Big Data, Privacy and Democracy," which met in Canada in May 2019, offered an extensive parliamentary forum to address disinformation in the digital realm.[1] In Germany, the dangers of party-political disinformation campaigns had also been discussed in the Bundestag, and the European Union set up an expert group on the topic at the beginning of 2018. Meanwhile, Robert Mueller's special investigation into Russian disinformation in the 2016 US presidential election campaign via Facebook, Instagram, Twitter and YouTube culminated in an over 400-page report. All are evidence that political decisionmakers around the world have been looking for suitable ways to deal with disinformation for several years now. Since at least the 2016 US presidential election, legislative and regulatory measures have been considered at various political levels in order to curb the possible dangers of disinformation on social discourse – from voluntary commitments from social networks, search engines and other companies, to guidelines for moderating and deleting illegal content and new supervisory authorities.

It has been a struggle to design appropriate legislative and regulatory measures to combat disinformation, though some US companies themselves are calling for regulation in this area, and many governments have already passed laws. But tackling disinformation in the digital sphere has hitherto been fragmented, initially due to a self-regulatory focus, followed by various isolated reactive measures. The challenges associated with disinformation should not be underestimated: They concern questions about freedom of expression, the political decision-making process, the power of large corporations and the influence of information and communication technologies on democratic discourse. Political decisionmakers are currently still looking for answers. That is why now is the time to scrutinize how legislative and regulatory interventions can strengthen democratic discourse and peoples' abilities to freely form their own political opinions in the digital realm.

Against this backdrop, this paper provides an overview of regulatory approaches in Germany and the EU for tackling disinformation. It shows past policy

1 Parliamentarians in attendance came from Canada, Costa Rica, Ecuador, Estonia, Germany, Ireland, Mexico, Morocco, Singapore, St. Lucia and the United Kingdom; see Standing Committee on Access to Information, Privacy and Ethics, "International Grand Committee on Big Data, Privacy and Democracy," Standing Committee on Access to Information, Privacy and Ethics, June 2019, https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=10554743.

responses to disinformation campaigns (the EU's Action Plan, for instance), as well as long-planned reforms that could include measures to aid in constraining disinformation (media regulation, for example).

First, a short review will be helpful in gaining a better understanding of disinformation: What is disinformation, what is the ultimate goal in spreading it, and what features of disinformation have to be considered in an age of massive social networks and search engines?

Deception – with false content or misleading messaging. Disinformation is false, inaccurate and deceptive information that is developed and disseminated to impede political processes.[2] It is very important to note that deception can not only be achieved by a piece of information itself (the content of a message). Additionally, the content's context, source and distribution channel must be taken into account.[3] People can also be deceived, and processes for forming opinions hindered, by contextualization and the way in which information is disseminated. For example, correct information can be taken out of context if statistics about crimes committed by immigrants lack explanation or relevance, or if correct content is manipulated[4]. Similarly, it is misleading for individuals or groups on social networks to impersonate someone else in order to reinforce polarizing opinions. This happened, for instance, in the US, where activists had social media accounts for controversial issues such as police violence, racism and migration. The thing was: Some of these accounts did not originate from the US, but rather from Russia, and served to sow "discord in the political system."[5] Additionally, sup-

2 Loosely based on European Commission, "A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation" (Brüssel: European Commission, March 12, 2018), 10, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271; see also the definition via the verb "to disinform" in Clare Melford, "Disinformation Is an Online Harm," Global Disinformation Index, June 26, 2019, https://disinformationindex.org/2019/06/disinformation-is-an-online-harm.

3 For this three-step concept see the idea of "Message - Messenger - Messaging" in Michael Meyer-Resende and Rafael Goldzweig, "Online Threats to Democratic Debate: A Framework for a Discussion on Challenges and Responses" (Berlin: Democracy Reporting International, June 26, 2019), https://democracy-reporting.org/wp-content/uploads/2019/06/BP_Threats-to-digital-democracy.pdf.

4 The SNV study on the 2017 German federal elections shows in detail how in the run-up to the election, false, manipulated and "context-less" content and statistics were spread; see Alexander Sängerlaub, Miriam Meier, and Wolf-Dieter Rühl, "Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017" (Berlin: Stiftung Neue Verantwortung, March 26, 2018), https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf.

5 Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election" (Washington, DC: U.S. Department of Justice, March 2019), 4, https://www.justice.gov/storage/report.pdf.

posed US activists used paid advertising on controversial topics in order to further contribute to polarization. Pretending to represent a widely held opinion using fake or bought followers, or manipulated search engine entries, is also a deception that can damage democratic discourse, as was seen in the run-up to the 2019 elections for the European Parliament, specifically regarding topics relating to migration.[6]

Sowing discord and hindering political decision-making. Disinformation is not only dangerous when it comes to voting and election campaigns. Although the issue received much attention after the Brexit referendum and the US presidential election, disinformation is not necessarily intended to influence voting results: Disinformation serves to amplify social polarization and to undermine confidence in democratic processes and common facts. On the individual level, disinformation hinders citizens' free, self-determined political decision-making. And on the societal level, democratic discourse is weakened.

Major search engines and social networks as amplifiers. In recent years, it has become clear that some social networks, search engines and other digital channels are particularly suited for spreading disinformation. The previously mentioned "Grand Committee" summoned representatives from Amazon, Apple, Google, Facebook, Microsoft and Twitter, among others.[7] Special counsel Mueller's report on the 2016 US election, as mentioned above, named Facebook, Instagram, Twitter and YouTube as channels of Russian influence.[8] A British parliamentary inquiry focused on Facebook.[9] These services can be used and exploited quite cheaply and easily to exacerbate existing social tensions through disinformation. It is important to emphasize: Disin-

6 Trevor Davis, Steven Livingston, and Matt Hindman, "Suspicious Election Campaign Activity on Facebook: How a Large Network of Suspicious Accounts Promoted Alternative Für Deutschland in the 2019 EU Parliamentary Elections" (Washington, DC: The George Washington University, July 22, 2019), https://smpa.gwu.edu/sites/g/files/zaxdzs2046/f/2019-07-22%20-%20Suspicious%20Election%20Campaign%20Activity%20White%20Paper%20-%20Print%20Version%20-%20IDDP.pdf; Avaaz, "Far Right Networks of Deceptions: Avaaz Uncovers Flood of Disinformation, Triggering Shutdown of Facebook Pages with over 500 Million Views Ahead of EU Elections" (New York, NY: Avaaz, May 22, 2019), https://avaazimages.avaaz.org/Avaaz%20Report%20Network%20Deception%2020190522.pdf.

7 Standing Committee on Access to Information, Privacy and Ethics, "International Grand Committee on Big Data, Privacy and Democracy."

8 Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."

9 House of Commons Digital, Culture, Media and Sport Committee, "Disinformation and 'Fake News': Final Report" (London: House of Commons, February 14, 2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

formation has not developed because of these technologies – it is not a new or purely digital phenomenon. Rather, disinformation amplifies the existing social challenges many established democracies face today – be it widespread fears of social decline, racism, political corruption or ethnic conflict.[10]

What is new, however, is the extent of disinformation, and this is connected to the rise of some social networks, search engines and video portals: They can strengthen debates and perspectives that contribute to social division and polarization. Therefore, the specific ways these services function must be taken into account when talking about disinformation in the digital realm. At the core of Facebook, Google, Instagram, Twitter and YouTube, for example, is a logic of maximizing attention – a logic for which anger and lies often work better than kindness and truth (see info box on the following page). This attention maximization logic that characterizes some social networks and search engines is based on extensive data collection. Personal data can be used to create detailed profiles that enable companies to sell targeted ads. A side effect of this is the emergence of personalized, segmented realms of digital information and news that go largely without journalistic gatekeeping. Such realms are particularly susceptible to the spread of disinformation.

10 For this line of argumentation, see also Ben Scott, "Did Google and Facebook Break Democracy?," *Progressive Centre UK*, July 30, 2019, https://www.progressivecentre.uk/did_google_and_facebook_break_democracy; Adam B. Ellick, Adam Westbrook, and Andrew Blackwell, "Operation Infektion: Russion Disinformation from Cold War to Kanye," *The New York Times*, November 12, 2018, https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html.

How microtargeting, personalization and network effects facilitate the spread of disinformation

Deceiving people, but also manipulating societal debates, is easier than ever in the digital public sphere. Social networks not only allow people to consume information and entertainment, but also to produce it.[11] Search engines make knowledge and information about political events quickly and easily available around the globe. This leads to an enormous democratization of political discourse, with more and more citizens able to participate in social and political debates on the internet. But it simultaneously creates new outlets for extremists and contributes to segmenting the public: The millions who use Facebook every day in Germany[12] can personalize their news and information spaces more easily than before. Moreover, due to the structure of many social networks (and a lack of resources in traditional media), journalistic gatekeeping is often missing. For example, an editorial department that researches and selects stories, and corrects false or misleading information.

Without journalistic gatekeepers, the door for manipulating opinions in these segmented, highly personalized information spaces is wide open. There is a risk, for example, that users may build echo chambers in which their existing views are confirmed.[13] Microtargeting[14], for example, allows commercial and political organizations to harness messaging to hone in on those who would most likely be affected and incited by such content. That, in turn, can deepen existing social divisions.

Such microtargeting is at the core of most social networks and other digital services: They make money as marketing platforms by selling personalized ad spaces. They have neither an educational/informational mandate, nor are they subject to the professional ethics of journalism. Users' attention is the sole driver of this system. Therefore, corporations try to keep people on their

11 Cf. Leonhard Dobusch, "Die Organisation der Digitalität: Zwischen grenzenloser Offenheit und offener Exklusion," *netzpolitik.org*, February 1, 2017, https://netzpolitik.org/2017/die-organisation-der-digitalitaet-zwischen-grenzenloser-offenheit-und-offener-exklusion/.

12 In Germany, the use of social media for news consumption is relatively low, but growing; see Nic Newman, "Reuters Institute Digital News Report 2019" (Oxford: Reuters Institute for the Study of Journalism, June 12, 2019), https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-06/DNR_2019_FINAL_0.pdf.

13 It is hard for scientists to check the existence and nature of echo chambers due to a lack of data access with the companies. Some studies have found them; see the literature overview in Jan Philipp Rau and Sebastian Stier, "Die Echokammer-Hypothese: Fragmentierung der Öffentlichkeit und politische Polarisierung durch digitale Medien?," *Zeitschrift für Vergleichende Politikwissenschaft*, August 29, 2019, 1–19, https://doi.org/10.1007/s12286-019-00429-1.

14 This refers to the data-based, targeted addressing of individual people or groups.

sites and in their apps as long as possible (to increase their "engagement"[15]) in order to show them ads. In this undertow of attention maximization, excitement and anger work better than facts and kindness. Anger especially ensures that people share content and reject other views.[16] Journalistic offerings face difficulties in this environment. Combined with the large reach and high speed of many social networks, the loudest and coarsest of voices in any given debate become salient.[17]

The unprecedented concentration of both data and power in some of these companies cyclically reinforces these tendencies: The better companies are in capturing the attention of users, the longer, more frequently and more intensively people will use a social network or search engine; the better these companies can profile their users; better personalize the content and ads they offer; and thus ensure that people use their offerings longer, more frequently and more intensively. This clearly shows how important data collection and positive network effects (the more users a service has, the more useful it becomes) are for many companies.

15 This is a term straight from marketing, meaning user interaction with digital content, i.e. reading, liking, following, subscribing.

16 Dag Wollebæk et al., "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior:," *Social Media + Society*, April 9, 2019, https://doi.org/10.1177/2056305119829859.

17 YouTube and other companies rightly claim that while they have an interest in keeping people on their services, they also have an interest in providing people with a "nice" information and entertainment environment. However, in the past, this has often not worked, which is why the criticism remains valid that illegal and coarse content works particularly well. For the YouTube example, see Mark Bergen, "YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant," *Bloomberg*, April 2, 2019, https://www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant; Neima Jahromi, "The Fight for the Future of YouTube," *The New Yorker*, July 8, 2019, https://www.newyorker.com/tech/annals-of-technology/the-fight-for-the-future-of-youtube; The Economist, "Now Playing, Everywhere: The Tricky Task of Policing YouTube," *The Economist*, May 4, 2019, https://www.economist.com/briefing/2019/05/04/the-tricky-task-of-policing-youtube.

The introduction shows that a discussion on the regulatory reaction to disinformation cannot be limited to correcting individual pieces of false content. Hiding behind the phenomenon of disinformation in the digital realm are questions about the sheer data power of some corporations, the attention-driven system of many social networks, weakened journalistic gatekeepers and the lack of rules for online political communications. Therefore, it is necessary to focus on a number of legal areas and policy fields when searching for legislative solutions. It is important to note, however, that regulatory measures do not necessarily have to be explicitly designed to act *against* disinformation or hate speech, but can also *strengthen users* of social networks, search engines or video portals.

The latter approach is still underdeveloped in Germany and the EU, as previous measures have been characterized by self-regulation and the removal of illegal content. This is explained in more detail in the following overview, which analyzes several approaches.

Regulatory Measures for Tackling Disinformation

Two major disinformation campaigns in Europe and in the US in 2016 (during the Brexit referendum and the presidential election) can be seen as turning points. Since then, more thought has been given to how regulatory and legislative interventions can curb disinformation on both sides of the Atlantic. Previously, there had been only minor regulation of companies such as Facebook and Google, and it was largely left up to them to decide how they contained disinformation on their platforms, if at all. Moreover, such digital technologies have long been seen as (exclusively) beneficial to people's communication and opinion formation. Discussions about the role of Facebook, Twitter and YouTube in promoting democracy during the Arab Spring were a key factor here.[18]

Since at least the 2016 US election, however, this view has changed. The negative effects of social networks and search engines on democratic discourse have become clearer. A new extent of disinformation has been recognized among academics, civil society and policymakers as a potential source of disruption to political decision-making. Reactive countermeasures have emerged around the world. Governments were initially primarily concerned with so-called "harmful" content: Falsehoods must be corrected, and illegal content deleted. The importance of fact checking was stressed, as was the

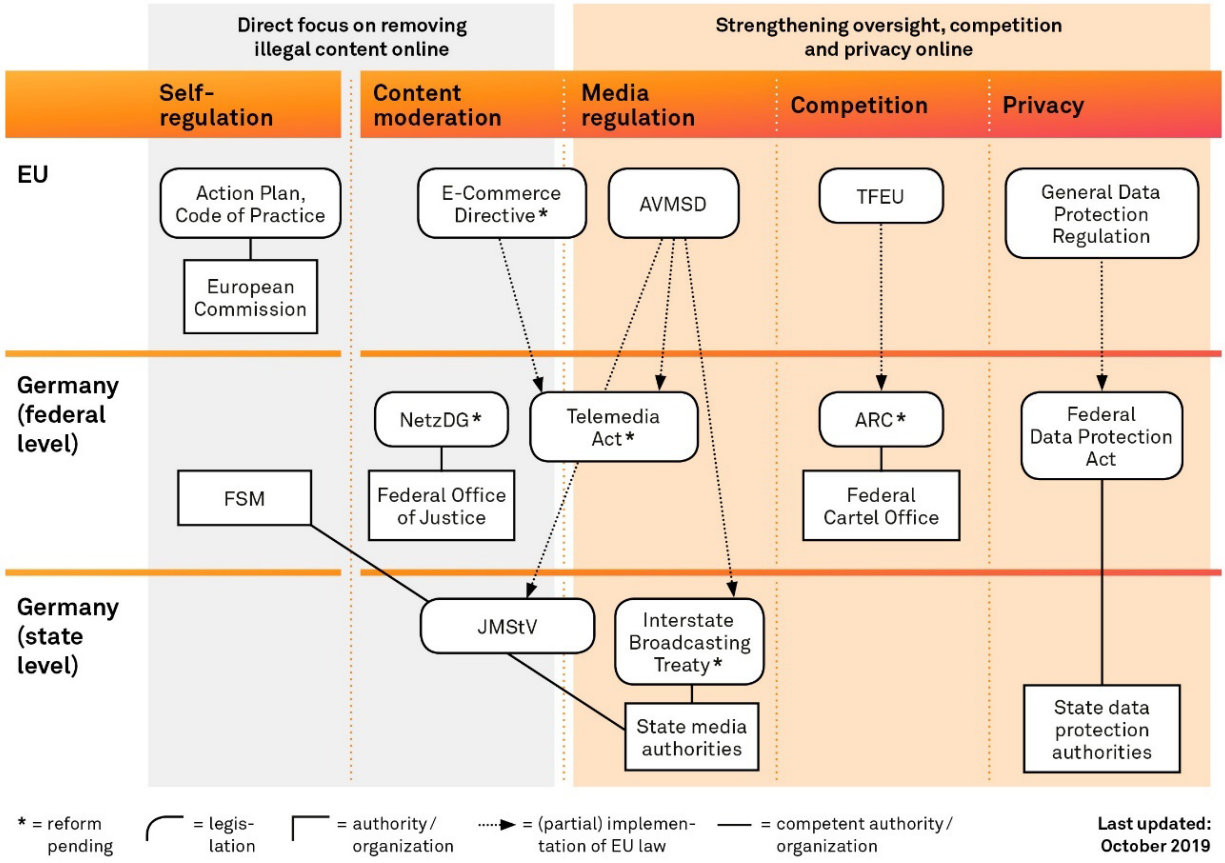
18 Maeve Shearlaw, "Egypt Five Years on: Was It Ever a 'Social Media Revolution'?," *The Guardian*, January 15, 2016, https://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution.

need to more readily apply existing criminal law to online communications. There continued to be a reliance on companies' own measures, such as adopting their own rules for moderating and deleting content or cooperating more closely with fact-checking initiatives. The EU Action Plan against Disinformation, which focuses primarily on voluntary commitments by large corporations, serves as an example of such reactive measures at this stage. The German Network Enforcement Act already departs from this self-regulatory approach but still focuses primarily on the removal of content.

Even so, three years after the US election, not much has changed. Measures taken by corporations themselves, often without a regulatory framework, continue to shape the approach against disinformation. Additionally, many of the reforms already pending in Germany to deal with a society and economy undergoing technological change are not designed to tackle the dangers of disinformation that have become more apparent since 2016. Reforms regarding the digitization of the economy (in competition law), the outsized role of personal data (in data protection) or changing media production and use (in broadcasting regulation), for example, have all been discussed for quite some time. To date, it remains unclear how such deliberations can or should integrate the dangers of disinformation campaigns and previous reactions to them.

Overall, this leads to a fragmented approach in tackling disinformation. The following short analysis of different strategies in dealing with disinformation highlights this fragmentation. The figure on the following page shows five areas that will be more closely analyzed – from self-regulation and content moderation, to issues of media regulation, competition law and data protection. The background of each area will be briefly explained with one or more exemplary measures. Then, each topic's importance to disinformation will be discussed, even if the action itself does not explicitly refer to disinformation. The strengths and weaknesses pointed out afterwards always refer solely to tackling disinformation. The weaknesses will be touched on again in the paper's conclusion. Further information on all abbreviations and laws mentioned in the illustration can be found in the text and/or in the appendix.

How past and potential regulatory approaches tackle disinformation



Regulatory approaches to disinformation in Germany and the EU

Self-regulation

Example and background. The prime example of a self-regulatory approach to dealing with disinformation is the EU's response to the prominent disinformation campaigns of 2016. At the end of 2018, the European Commission presented a Code of Practice[19] for major social networks and search engines, as well as an Action Plan[20] against disinformation.

19 European Commission, "EU Code of Practice on Disinformation," European Commission, September 26, 2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

20 European Commission, "Action Plan against Disinformation," European Commission, December 5, 2018, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

A group of experts had previously drawn up proposals on the topic.[21] The commitments cover several issues, such as media literacy, content moderation and political advertising. As such, self-regulation in this case can be understood as an overarching approach.

The Action Plan stipulates that the European External Action Service will receive more financial resources and more staff for strategic communications. Moreover, an early warning system will be set up, as well as awareness campaigns for citizens. As the European Commission cannot comment on disinformation issues within EU member states, focus was placed instead on possible Russian disinformation campaigns. The Action Plan also includes a section on monitoring the Code of Practice for major social networks and search engines.[22] One of the aims of these voluntary commitments is to close fake accounts more quickly. Additionally, the placement of political ads would be more strictly regulated. To this end, platforms set up publicly accessible databases for political ads. Moreover, corporations are meant to work together with civil society organizations and support research.

Strengths. That there is even an EU-wide response to disinformation developments since 2016 is an important signal: The European Union has recognized the need for strategic communications against disinformation, as well as strengthening cooperation and raising people's awareness. These are precisely the points made in the Action Plan. New resources and networks can help in addressing some of the issues related to disinformation. Additionally, the Code of Practice stands as a symbol for attempting to curb disinformation together with large corporations.

Weaknesses. The EU's self-regulatory measures remain vague, and the Code of Practice lacks enforcement and sanctioning mechanisms.[23] Examples of these weaknesses can be found in abundance. Companies' "support" of research, for example, includes no obligation to make data interfaces accessible to researchers, even though this forms the basis for meaningful scientific studies that can critically evaluate and cross-check the platforms' own

21 European Commission, "A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation."

22 Companies and industry associations having signed the Code are Facebook, Google, Mozilla, Twitter, the European Association of Communications Agencies (EACA), the Interactive Advertising Bureau (IAB Europe) and the World Federation of Advertisers (WFA).

23 For an evaluation of the EU's measures, see Bruno Lupion, "The EU Framework Against Disinformation: What Worked, What Changed and the Way Forward" (Berlin: Democracy Reporting International, August 30, 2019), https://democracy-reporting.org/wp-content/uploads/2019/08/EU-Actions-Against-Disinformation-EP2019-Final.pdf.

measures.[24] Additionally, corporations are likely working on technological solutions to delete fake accounts, even without the Code. The political ad databases were indeed a new development, set up largely in the run-up to elections for the European Parliament in 2019. However, they were incomplete and bug-ridden.[25] There was little the EU could do about that – due to the lack of sanctioning mechanisms. Moreover, it is questionable whether an unblinking focus on Russian influence does justice to the disinformation problem if it is clear that many disinformation campaigns are conducted by domestic people and organizations. During the 2017 federal elections in Germany, for example, domestic right-wing populists were the primary source of spreading disinformation, without direct intervention by foreign states.[26] The EU was aware of these weaknesses from the outset – the Action Plan itself states that upon its evaluation, regulatory measures are possible. Some of those potential measures will be discussed in the next section.

Content Moderation

Examples and background. There are already established liability and deletion rules for dealing with illegal content on the internet. In Germany, examples of such content include the incitement of hate and speech insulting ideological or religious communities. Since 2016, governments around the world have been trying to better enforce the removal of criminal content. There are limits, however, to how well this approach can be used to constrain disinformation because disinformation is not always illegal.[27] Nevertheless, discussing questions about content moderation and deletion is necessary in the realm of disinformation.

The removal of illegal content on the internet works mainly through a procedure of "notice and take down": Social networks, search engines and other

24 For an overview of the difficulties regarding data access for academia and civil society, see Alexander Sängerlaub, "Der blinde Fleck digitaler Öffentlichkeiten" (Berlin: Stiftung Neue Verantwortung, March 21, 2019), https://www.stiftung-nv.de/sites/default/files/blinde.fleck_.digitale.oeffentlichkeit.pdf.

25 Mozilla Corporation, "Facebook and Google: This Is What an Effective Ad Archive API Looks Like," *The Mozilla Blog*, March 27, 2019, https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like.

26 Sängerlaub, Meier, and Rühl, "Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017."

27 On this, see chapters 4 and 6 in particular in Christian Mihr and Daniel Moßbrucker, "Regulierung 2.0: Warum soziale Netzwerke, Suchmaschinen & Co. ein Teil der informationellen Grundversorgung geworden sind - und wie sie reguliert werden sollten, um die Meinungs-und Pressefreiheit zu schützen" (Berlin: Reporter ohne Grenzen, June 12, 2018), https://www.reporter-ohne-grenzen.de/uploads/tx_lfnews/media/Reporter-ohne-Grenzen_Regulierung-2.0-Langfassung.pdf.

internet services must delete illegal content when they learn of its existence. They do not have to actively search for such content. This serves as the basis for many services on the internet. If social networks, search engines, video portals and other digital services had not been at least partially exempt from liability for their users' content, companies such as Google, Facebook and Twitter would hardly have been able to develop. These liability rules and exceptions are laid out in the EU's e-Commerce Directive and are reflected in the German Telemedia Act ("Telemediengesetz," TMG). At the European level, a Digital Services Act is to replace the e-Commerce Directive and update liability rules.[28] In Germany, the Network Enforcement Act ("Netzwerkdurchsetzungsgesetz," NetzDG) calls on large social networks to provide users with a procedure for reporting potentially illegal content. According to the NetzDG, providers must delete such potentially criminal content within a certain period of time after notification.

Strengths. Removing illegal content online is consistent with the application of existing laws. Finding a suitable structure for content moderation and deletion is therefore a positive approach. The NetzDG is a supplement to and extension of the previous liability and deletion practices and introduces some new requirements. In addition to the aforementioned obligation to offer set guidelines for reporting illegal content, companies must designate point persons for complaints and file reports on deletion and moderation procedures. These approaches are sensible because they create rules for the structures and processes within companies that go beyond the removal of individual pieces of content. This can also be helpful in dealing with disinformation if there are clear, transparent and externally verifiable company guidelines for moderating and deleting content.

Weaknesses. The current liability and deletion provisions outlined in the e-Commerce Directive have largely proved their worth, but they still need an overhaul in light of the rise of social networks and search engines since the directive's adoption in the year 2000. The EU itself believes such reforms are necessary[29], and the necessity of such reforms is also mentioned in the

28 Ursula von der Leyen, "A Union That Strives for More: My Agenda for Europe" (Brüssel: European Commission, July 16, 2019), 13, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf; ein geleaktes Arbeitspapier zeigt mögliche Eckpunkte eines Digital Services Act auf, siehe Tomas Rudl and Alexander Fanta, "Geleaktes Arbeitspapier: EU-Kommission erwägt neues Gesetz für Plattformen," *netzpolitik.org*, July 15, 2019, https://netzpolitik.org/2019/geleaktes-arbeitspapier-eu-kommission-erwaegt-neues-gesetz-fuer-plattformen/.

29 Europäische Kommission, "COM(2015) 192 final: Strategie für einen digitalen Binnenmarkt für Europa," Europäische Kommission, May 6, 2015, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52015DC0192&from=EN.

2017 German coalition agreement[30]. When it comes to questions concerning liability and content deletion, however, especially regarding disinformation, there is a fine line between freedom of expression and censorship. This makes the debate on possible reforms and solutions difficult.[31] Of course, illegal content online cannot be tolerated, and its removal needs to be strictly enforced. But, again, with disinformation, it is often difficult to assess what is covered by the right to freedom of expression, and what is punishable by law. It becomes even more problematic if – as is the case with the NetzDG – users have no right to object (when content is removed that should not have been in the first place), and the determination of a breach of law is largely outsourced to companies. Additionally, a focus on content removal does not ensure that people and groups are spared from targeted, manipulative messaging. Nor do the NetzDG obligations necessarily lead to the prosecution of those spreading illegal content.[32] Moreover, the rules governing transparency reports are unclear: Corporate reports are hard to compare and, in some cases, are incomplete due to a lack of specifications.[33] All of this shows that the content moderation approach, at least as it is currently applied to illegal content, cannot be easily transferred to issues arising from disinformation.

30 CDU, CSU, and SPD, "Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode," Christlich Demokratische Union Deutschlands, March 12, 2018, 49; 170, https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1.

31 The NetzDG also runs the risk that authoritarian rulers in other countries are inspired by it and easily adapt its rules to silence critics in the name of curbing illegal content. For an overview of the pros and cons of the NetzDG with regard to questions of freedom of expression, see David Kaye, *Speech Police: The Global Struggle to Govern the Internet*, vol. Columbia Global Reports (New York: Columbia University in the City of New York, 2019); Bundeszentrale für politische Bildung, "Debatte Netzwerkdurchsetzungsgesetz (NetzDG)," Bundeszentrale für politische Bildung, March 16, 2018, https://www.bpb.de/dialog/netzdebatte/262660/debatte-netzwerkdurchsetzungsgesetz-netzdg; Heidi Tworek and Paddy Leerssen, "An Analysis of Germany's NetzDG Law" (Amsterdam: Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, April 15, 2019), https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

32 A few special police units for cybercrime have been set up, focusing on the prosecution of hate speech; see Max Hoppenstedt, "Strafbare Postings in sozialen Netzwerken: 'Woher der Hass kommt, ist wirklich nur schwer zu begreifen,'" *SPIEGEL ONLINE*, June 21, 2019, https://www.spiegel.de/netzwelt/netzpolitik/netzdg-staatsanwalt-christoph-hebbecker-ueber-hass-in-sozialen-netzwerken-a-1273176.html.

33 Facebook, for example, was hit with a fine because the transparency reports are incomplete; see dpa, "Facebook wehrt sich gegen NetzDG-Bußgeld," *heise online*, July 19, 2019, https://www.heise.de/newsticker/meldung/Facebook-wehrt-sich-gegen-NetzDG-Bussgeld-4475699.html.

Media Regulation

Example and background. Reforms to German media oversight – in the form of the planned Interstate Media Treaty ("Medienstaatsvertrag")[34] – are not explicitly designed to curb disinformation. However, the previous Interstate Broadcasting Treaties are partly in place to create news and information environments that do not hinder democratic discourse and political decision-making, but rather cultivate it. Therefore, the Interstate Media Treaty can serve as an example of both the opportunities and risks associated with adapting a regulatory framework built for the analog world to the digital world.

The Interstate Media Treaty is the 23rd amendment to the Interstate Broadcasting Treaty, which creates rules for, among other things, the supervision of television, radio and online media in Germany. For the first time, there is now talk of an Interstate *Media* Treaty instead of an Interstate *Broadcasting* Treaty. This renaming reflects the effort to adapt existing German media regulations to the digital age. The set of rules should also include social networks and search engines: As such services become more and more important for media users to obtain news and information, Germany's federal states would like to assert their own area of expertise with the Interstate Media Treaty.[35] That is because in Germany, the federal states are responsible for supervising radio and TV, as well as "telemedia" (i.e. media offerings over the internet, such as newspapers' online platforms). An important task of such an oversight apparatus concerns the protection of minors from harmful media, which is regulated by the Interstate Treaty on the Protection of Minors from Harmful Media ("Jugendmedienschutz-Staatsvertrag," JMStV). It defines a system of "regulated self-regulation," which includes, for example, the Association for Voluntary Self-Regulation of Digital Media Service Providers ("Freiwillige Selbstkontrolle Multimedia-Diensteanbieter," FSM). Its members are companies such as Facebook and Google, which operate a complaints system for criminal and "youth-endangering" content through the association.

Parts of the Interstate Media Treaty, in particular those pertaining to video portals such as YouTube, implement provisions of the EU's Audiovisual Media Services Directive (AVMSD). This is also the reason why the Interstate Media Treaty must be in place by September 2020: The AVMSD must be trans-

34 Staatskanzlei Rheinland-Pfalz, "Diskussionsentwurf für einen 'Medienstaatsvertrag'" (2019), https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/MStV-E_Synopse_2019-07_Online_.pdf.

35 Helmut Hartung, "Medienstaatsvertrag: Der Vielfalt verpflichtet," *Frankfurter Allgemeine Zeitung*, August 9, 2019, https://www.faz.net/aktuell/feuilleton/medien/medienstaatsvertrag-der-vielfalt-verpflichtet-16324354.html.

posed into national law by that date. The draft Interstate Media Treaty was preceded by a federal-state commission on media convergence[36], which in turn was based on a comprehensive expert opinion[37] written for the federal states' Broadcasting Commission. The latter had already been published in 2014, showing just how long the discussion on adapting German media regulation to the digital age has been taking place.

Strengths. As disinformation can spread easily in the digital realm, the basic idea of defining supervisory standards for large social networks and search engines is sensible and useful. Debates on the matter are not only happening in Germany: In France[38] and in the United Kingdom[39], for instance, there have been proposals for creating central authorities specialized in social networks. Due to the federal structure of media regulation in Germany, the Interstate Media Treaty places the supervision of social networks in the hands of the federal states.

Some of the concrete rules proposed in the draft Interstate Media Treaty may be helpful in curbing disinformation. A promising approach is the algorithm transparency requirements for social networks and search engines. Disclosing how the selection and arrangement of search results and articles work can improve users' awareness of an algorithmically determined news environment. Requirements for naming point persons – similar to the ones in the Network Enforcement Act (see above) – also make sense. Both are measures which are not directly aimed at removing potentially illegal or misleading content but are intended to ensure greater transparency for news consumption.

36 Bund-Länder-Kommission, "Bericht Bund-Länder-Kommission zur Medienkonvergenz" (Berlin: Bund-Länder-Kommission, June 2016), https://www.bundesregierung.de/resource/blob/997532/473870/07ba875e860ada4556526641bd9151b6/2016-06-14-medienkonvergenz-bericht-blk-data.pdf?download=1.

37 Winfried Kluth and Wolfgang Schulz, "Konvergenz und regulatorische Folgen: Gutachten im Auftrag der Rundfunkkommission der Länder" (Mainz: Rundfunkkommission der Länder, 2014), https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/Konvergenz-Gutachten.pdf.

38 Sacha Desmaris, Pierre Dubreuil, and Benoît Loutrel, "Creating a French Framework to Make Social Media Platforms More Accountable: Acting in France with a European Vision" (Paris: French Secretary of State for Digital Affairs, May 2019), https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E1B36873E4&filename=Mission%20Re%CC%81gulation%20des%20re%CC%81seaux%20sociaux%20-ENG.pdf.

39 Department for Digital, Culture, Media & Sport and Home Office, "Online Harms White Paper" (London: Controller of Her Majesty's Stationery Office, April 8, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

Weaknesses. Whether the Interstate Media Treaty is fit for a digital news environment characterized by social networks, search engines, video portals and blogging services remains to be seen in the current draft. Introducing new terminology or adapting existing terminology alone creates uncertainty and ambiguity.[40] The draft treaty speaks of media platforms (roughly meaning Netflix), media intermediaries (roughly Google and Facebook), user interfaces (roughly electronic program guides), video sharing services (roughly YouTube) and "broadcast-like telemedia" (roughly public broadcasters' online media libraries). But the boundaries are blurred and unclear. The latter term in particular demonstrates the basic approach of extending the understanding of broadcasting to social networks, search engines and video portals. The fact that the division into linear and non-linear media (for instance, radio versus streaming services) is maintained is partly due to the provisions of the AVMSD.[41] But even with that in mind, the term "broadcast-like telemedia" in the German draft does not do justice to the digital information and news environment of today.[42]

Rules on transparency make sense in many areas, but much depends on how they are designed. In the Interstate Media Treaty, the minimum goal is that algorithm transparency helps one to better understand the influence of large social networks and search engines in the formation of opinions.[43] There are a total of two short sections in the draft treaty on that: one for media platforms such as Netflix, and one for media intermediaries (i.e. social networks and search engines). In each case, the requirement is that users should be informed directly and in easily understandable language about the "central criteria" of search and sorting algorithms. Clearer, more detailed standards are needed for such transparency rules. Otherwise, a situation similar to existing transparency efforts by Facebook and Twitter arises: Companies may educate users about why they see certain advertising content, but this information is rudimentary and therefore unhelpful. The draft also calls for

40 On the initial difficulties with definitions, see Wolfgang Schulz and Stephan Dreyer, "Stellungnahme zum Diskussionsentwurf eines Medienstaatsvertrags der Länder" (Hamburg: Hans-Bredow-Institut, September 26, 2018), https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/qiuektv_HBI_StellungnahmeMedienstaatsvertrag180926.pdf.

41 Hartung, "Medienstaatsvertrag: Der Vielfalt verpflichtet."

42 Hermann Rotermund, "Neuer Medienstaatsvertrag – alter Rundfunk," *CARTA online*, August 27, 2018, http://carta.info/neuer-medienstaatsvertrag-alter-rundfunk/.

43 Helmut Hartung, "'Das ist ziemlich einmalig': Interview mit Prof. Dr. Wolfgang Schulz, Direktor des Hans-Bredow-Instituts für Medienforschung," *Medienpolitik.net*, September 26, 2018, https://www.medienpolitik.net/2018/09/medienpolitikdas-ist-ziemlich-einmalig/.

labeling political ads on social networks and search engines.[44] Again, concrete details are missing, although there are specific suggestions as to what information presented in which specific way could help users.[45]

Competition X Privacy

Examples and background. For years, discussions have been taking place about more closely integrating competition and data protection authorities in order to cope with the growing data and market power of large social networks and search engines.[46] This approach is not directly aimed at tackling disinformation. Nevertheless, a look at competition and data protection rules is important, as they can indirectly help curb disinformation. The personalized, segmented news feeds of global networks leave the door wide open for disinformation. Limiting data collection and the dominant position that Facebook and Google currently hold in the online advertising market could close this door somewhat, as the segmentation and personalization of news feeds or search engine results via search and sorting algorithms would not be possible without extensive data collection and profiling (see info box on pages 10 and 11).

One example of a link between competition law and data protection is the antitrust proceedings against Facebook in Germany. The federal competition authority (Bundeskartellamt) investigated Facebook's market power against the backdrop of the company's extensive data collection practices. The Bundeskartellamt concluded that Facebook has a dominant market position and abuses it to the detriment of its users. According to the competition authori-

44 Die Medienanstalten, "Stellungnahme der Medienanstalten zum überarbeiteten Diskussionsentwurf der Rundfunkkommission der Länder für einen 'Medienstaatsvertrag,'" Die Medienanstalten, August 9, 2019, 10–11, https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Ueber_uns/Positionen/2019_08_09_Stellungnahme_der_Medienanstalten_zum_Medienstaatsvertrag.pdf.

45 Dipayan Ghosh and Ben Scott, "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet" (Washington, DC: New America, January 23, 2018), https://d1y8sb8igg2f8e.cloudfront.net/documents/Digital_Deceit_2_Final.pdf.

46 For examples at the EU level, in Australia and the United Kingdom, see Europäischer Datenschutzbeauftragter, "Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von „Big Data": Das Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz in der digitalen Wirtschaft" (Brüssel: Europäischer Datenschutzbeauftragter, March 2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_de.pdf; Australian Competition and Consumer Commission, "Digital Platforms Inquiry - Final Report" (Canberra: Australian Competition and Consumer Commission, July 26, 2019), https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf; Competition and Markets Authority, "Online Platforms and Digital Advertising Market Study," GOV.UK, July 3, 2019, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

ty, users lose control over their own data even if they do not suffer any direct financial damage as a result.[47] Specifically, the case was about whether and how Facebook is allowed to merge the data from its services Facebook, Instagram and WhatsApp, and from other sources. The Bundeskartellamt prohibited the practice. In a subsequent legal decision, however, the Düsseldorf Higher Regional Court initially halted the implementation of this prohibition.[48] Whether the Bundeskartellamt will be successful in its attempt to link data protection and competition law will only become clear in the coming months and years: The final judgement is probably months away, the Federal Court of Justice will deal with the case and proceedings before the European Court of Justice are also possible.[49]

Strengths. Combining data protection and competition law in the Bundeskartellamt proceedings represents an attempt to limit the data and market power of Facebook and other dominant digital companies. The competition authority makes its case based on the EU's General Data Protection Regulation (GDPR). The GDPR offers options to limit the collection of data – especially on sensitive topics like political ideology, sexuality and health status – which is at the core of many social networks' advertising models. To provide just one example: Default settings on social networks have to be chosen in such a way as to ensure that they collect and share as little personal data as possible (data minimization and "privacy by default"), which can help restrict tracking and profiling. This improves the chances of not solely receiving information and content that an algorithm has calculated could perhaps

47 Summarized in the press release in Bundeskartellamt, "Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen," *Bundeskartellamt*, February 7, 2019, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2; full decision in Bundeskartellamt, "B6-22/16: Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung" (Bonn: Bundeskartellamt, February 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html;jsessionid=1758AF99E64A2D1B504758D23E7072EB.1_cid378?nn=3591568.

48 Summarized in the press release in Michael Börsch, "Facebook: Anordnungen des Bundeskartellamts möglicherweise rechtswidrig und deshalb einstweilen außer Vollzug," *Oberlandesgericht Düsseldorf*, August 26, 2019, http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/index.php; full decision in Oberlandesgericht Düsseldorf, "Beschluss VI-Kart 1/19 (V) In der Kartellverwaltungssache 1. Facebook Inc., 2. Facebook Ireland Ltd., 3. Facebook Deutschland GmbH, Antragstellerinnen und Beschwerdeführerinnen,Verfahrensbevollmächtigte:... gegen Bundeskartellamt, Antragsgegner und Beschwerdegegner" (Düsseldorf: Oberlandesgericht Düsseldorf, August 26, 2019), http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf.

49 pbe/dpa, "Gericht verpasst Kartellamt im Verfahren gegen Facebook einen Dämpfer," *SPIEGEL ONLINE*, August 26, 2019, https://www.spiegel.de/netzwelt/apps/bundeskartellamt-gegen-facebook-oberlandesgericht-duesseldorf-bremst-a-1283736.html.

lead to high user engagement – content that plays into users' anger or other emotions, for example.[50]

Weaknesses. In the realm of data protection, the GDPR provides a recently updated legal framework to constrain unlawful data collection. Yet, its enforcement is difficult, because data protection authorities often lack the necessary resources. In contrast, antitrust authorities have traditionally had strong enforcement powers. Antitrust authorities, however, are missing a legal framework suitable for the digital age, although they themselves have built up strong expertise regarding technological changes in the economy.[51] The antitrust proceedings against Facebook revealed these institutional weaknesses. This also indirectly hinders the containment of disinformation on large platforms. At least a reform is planned with regard to competition law. The Federal Ministry for Economic Affairs and Energy has set up the "Competition Law 4.0 Commission," which in its report recommends improved data access for citizens and potential competitors, as well as "institutionalized networking" for various supervisory authorities.[52] Until these or similar reforms have arrived, however, the current law of the land remains in place – and this is based on a separation of antitrust and data protection law.

Overall, the review of different approaches dealing with disinformation reveals structural weaknesses. The landscape for tackling disinformation is shaped by reactive measures put in place after 2016, which consisted mainly of self-regulatory measures and stricter guidelines for content moderation. In other legal and policy areas, approaches going beyond this are only slowly beginning to emerge. The planned reforms of media regulation and competition law are examples of this. Disinformation, however, is not viewed holistically, which makes its regulatory framework incomplete. In the following conclusion, some of these weak points are discussed as possible areas of activity for future legislative and regulatory measures.

50 Further examples from the GDPR are rules on purpose limitation, transparency and information obligations and data protection for children. An extension of the data protection impact assessment could also be helpful.

51 Rupprecht Podszun, "Nach dem Facebook-Verfahren: Der Kartellrechts-Clash," *Legal Tribune Online*, September 13, 2019, https://www.lto.de/recht/hintergruende/h/facebook-verfahren-bkarta-ausbeutung-marktbeherrschung/.

52 Kommission Wettbewerbsrecht 4.0, "Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft" (Berlin: Bundesministerium für Wirtschaft und Energie, September 9, 2019), 5, https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=4.

Conclusion and Outlook

On the one hand, the activities described in this paper show that awareness of the problem of disinformation among political and business leaders is growing. On the other hand, they reveal difficulties in curbing disinformation: Self-regulation has not worked, as is evident in the EU's self-assessment of the Action Plan. Transposing the approach for content moderation – so far clearly the preferred method in dealing with illegal content – is also inappropriate. Even planned regulatory projects, such as reforming media regulation, do not adequately address the dangers of disinformation. This creates a patchy regulatory environment that benefits individuals and organizations aiming to spread disinformation.

Democratic societies, however, are not powerless to disinformation. This paper also makes that much clear. There are legislative and regulatory projects at every political level that can help constrain disinformation. Measures that merely fight *against* manipulative and illegal content are less important. Instead, further efforts are necessary *for* creating a digital environment that empowers citizens to freely and independently form their own political opinions. That includes transparency rules for companies, as well as measures that strengthen privacy and oversight mechanisms. Although this is not the primary focus of this paper, the expansion of news and information literacy, as well as support for journalism, are also important, of course.[53] If the individual approaches outlined here are considered as a whole, some overarching points for possible future activities can be identified.

Less reliance on self-regulation. The EU Code of Practice is a symbolic measure. Although the EU deems it a success[54], it is also aware of how limited self-regulatory measures are. The overarching Action Plan therefore states that regulatory measures could also be proposed if no progress is made after a one-year evaluation period. The possible reform of the e-Commerce Directive into a Digital Services Act could include such regulations. The NetzDG and the Bundeskartellamt's aspirations underscore the attitudes of political and regulatory decisionmakers that self-regulation is no longer enough. Social networks and search engines, for example – which make their money as advertising platforms but simultaneously help shape the political opinions of many citizens – need clear rules for this side effect of their work as ad

53 The SNV has separate projects dealing with these issues related to strengthening the digital public sphere.

54 European Commission, "JOIN(2019) 12 Final: Report on the Implementation of the Action Plan Against Disinformation" (Brüssel: European Commission, June 14, 2019), https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf.

providers. That applies today in Germany, especially for Facebook, Google, Instagram and YouTube, but could refer to completely different offerings in the future. This must also be considered when it comes to possible regulatory measures.

Define transparency rules in more detail. Many of the measures taken so far are concerned with transparency: The Interstate Media Treaty deals with transparency rules for algorithms, the Action Plan puts some focus on the transparency of political ads, and the NetzDG emphasizes the appointment of point persons and companies' reporting obligations. For users, insights into how social networks and search engines function can be helpful. Such insights are even more important for researchers, so they can understand the nature and impact of digital services and then make their findings accessible to the public. To this end, transparency rules must become clearer. For example, the guidelines for algorithm transparency and accountability need to be defined in more detail. Moreover, scientists must be able to work with data from social networks and search engines.[55] With meaningful scientific findings, policy makers can then make evidence-based policy decisions. At present, researchers and policymakers often have to rely on case studies or on companies' voluntary initiatives to obtain data. That has not worked very well so far.[56] Reports with figures on deleted content, a requirement of the NetzDG, have also been met with criticism because they are inconsistent and incomplete.[57] On matters of transparency, it is important to consider the interplay between transparency and data protection. Demands for transparency for researchers should not be rejected on flimsy grounds referring to data protection. And data protection must not be weakened to enable research. In principle, the GDPR offers avenues for allowing anonymized, aggregated data analysis for research purposes.

Transparency is also necessary for online political communications. The Action Plan alludes to political advertising on the internet, and the Digital Services Act could contain clear EU rules in this respect. Right now, citizens are dependent on the voluntary measures corporations themselves have developed over the years. There is both plenty of criticism of this self-regulato-

55 Sängerlaub, "Der blinde Fleck digitaler Öffentlichkeiten."

56 Katie Paul, "Funders Threaten to Quit Facebook Project Studying Impact on Democracy," *Reuters*, August 28, 2019, https://www.reuters.com/article/us-facebook-election-research-idUSKCN1VI04F.

57 Moritz Koch and Dietmar Neuerer, "Netzwerkdurchsetzungsgesetz: Die Bundesregierung erreicht im Kampf gegen Hate-Speech im Netz nur wenig," *Handelsblatt*, August 6, 2019, https://www.handelsblatt.com/politik/deutschland/netzwerkdurchsetzungsgesetz-die-bundesregierung-erreicht-im-kampf-gegen-hate-speech-im-netz-nur-wenig/24874984.html.

ry practice and concrete suggestions for improvements.[58] In this area, both data protection and media regulation approaches must be combined, and Germany's law on political parties must also be considered. Ideally, European rules would take into account country-specific electoral laws.

Enhance enforcement. Before new laws for the digital public sphere are created, existing laws should be strictly enforced. This was the thinking behind the Network Enforcement Act with regard to criminal law. Instead of focusing on criminal law, however, an emphasis on data protection law would be helpful. At first glance, it may not be obvious what data protection has to do with disinformation: The GDPR is not designed to remove broad swaths of illegal content from the internet. If attention is turned to the data-driven logic behind Facebook, Google, Twitter, YouTube and other companies, however, privacy rules can very well aid in curbing disinformation (see Competition X Privacy above). Demands for better law enforcement in the realm of data protection are by no means new or controversial – there is just a lack of resources. For years, decisionmakers with states' data protection authorities have complained about too few personnel and too little financial resources. Precisely because privacy rights are becoming more important in an age of surveillance capitalist corporations such as Facebook and Google[59], it is important to provide expertise and resources to enforce them.

Improve coordination and consider a holistic approach to oversight. For the foreseeable future, reforms at various political levels in various policy fields – from media supervision to content moderation and competition law – will shape the regulatory response to disinformation and also online hate speech. In order to avoid potentially conflicting objectives and decisions in this fragmented regulatory framework, it is useful to improve coordination bet-

58 Dipayan Ghosh und Ben Scott in Anja Zimmer, ed., *Smart Regulation for Digital Media Pluralism* (Berlin: Medienanstalt Berlin-Brandenburg, 2019), https://mediapolicylab.de/files/content/document/Policy%20Statements/White_Book_MPL_July2019.pdf; Jochen König and Juri Schnöller, "Wie digitale Plattformen sich um Transparenz bemühen," *Politik & Kommunikation*, July 9, 2019, https://www.politik-kommunikation.de/ressorts/artikel/wie-digitale-plattformen-sich-um-transparenz-bemuehen-1923588873; Privacy International, "Social Media Companies Have Failed to Provide Adequate Advertising Transparency to Users Globally," *Privacy International*, October 3, 2019, http://privacyinternational.org/long-read/3244/social-media-companies-have-failed-provide-adequate-advertising-transparency-users; for a detailed look from a British perspective with implications also for Germany and the EU, see Michela Palese and Josiah Mortimer, eds., *Reining in the Political 'Wild West': Campaign Rules for the 21st Century* (London: Electoral Reform Society, 2019), https://www.electoral-reform.org.uk/latest-news-and-research/publications/reining-in-the-political-wild-west-campaign-rules-for-the-21st-century/.

59 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

ween respective authorities. This refers to the interplay between competition and data protection law, for example. Another example is data protection for children: This currently falls within the Interstate Treaty on the Protection of Minors from Harmful Media and the GDPR, albeit without institutionalized coordination. Whenever possible, closer cooperation between German oversight bodies and ministries and European partners is also helpful in establishing EU-wide common standards. The Digital Services Act could remedy this situation. Attention must be paid, however, to country-specific contexts with regard to internet use, media systems and oversight structures, for example. For good reason, Germany's media supervision is purposefully removed from government influence and has a federal structure.

Even in light of the historical imperatives shaping German media regulation, it is worth considering future forms of supervision specifically designed for social networks and search engines. For instance, the idea of an "internet general manager's office" ("Internetintendanz") would include, among other mechanisms, a supervisory authority for questions of disinformation.[60] As mentioned above (see Media Regulation), after months of research on Facebook in France, a central supervisory authority for social networks was proposed to the government. Such an authority is also being discussed in Great Britain. Interestingly, French experts compared their proposal with financial market regulation: The focus is on processes (not products) and there is an overarching supervisory authority for the market. The comparison could be expanded to pharmaceutical regulation. The primary oversight objective is not to withdraw a specific financial product or specific drug from circulation, but to ensure that suitable compliance processes and structures are established within companies at the outset in order to avert possible damage to citizens.

Some of these measures can be tackled in the short term, while others require long-term structural reforms. For example, the consideration of a special oversight mechanism for social networks raises constitutional questions in Germany that are difficult to quickly and easily resolve. Certain areas, though, would lend themselves to immediate regulatory and legislative action. Strict enforcement of the GDPR would be one example of an immediate measure. It is also vital to think about clear rules for online political communications as soon as possible. Even if the danger of disinformation via political online ads in Germany is still low and should not be dramatized, it is not hard to predict that political communications will shift even more intensely into the digital realm.

60 Christoph Bieber, Leonhard Dobusch, and Jörg Müller-Lietzkow, "Die Internetintendanz," *Medienkorrespondenz*, April 28, 2019, https://www.medienkorrespondenz.de/leitartikel/artikel/die-internetintendanz.html.

If such short-term and long-term solutions are combined, a holistic policy agenda emerges that addresses the dangers of disinformation. Otherwise, the problem of disinformation will become further aggravated by a fragmented regulatory approach.

Regulatory Measures and Options for Tackling Disinformation

Stiftung Neue Verantwortung

Level	European Union				Germany (federal level)			Germany (state level)	
Focus	**Self-regulation**	**Privacy**	**Content moderation**				**Competition**	**Content mod.**	**Media regulation**
Name and abbreviation	**Code of Practice and Action Plan**	**General Data Protection Regulation (GDPR)**	**Audiovisual Media Services Directive (AVMSD)**	**E-Commerce Directive, possible future Digital Services Act (DSA)**	**Network Enforcement Act (NetzDG)**	**Telemedia Act (TMG)**	**Act against Restraints of Competition (GWB)**	**State Treaty on the Protection of Minors in the Media (JMStV)**	**Interstate Broadcasting Treaty (RStV), possible future Interstate Media Treaty**
Explicit reference to disinformation	Yes	No	No	No (but indirectly on illegal content via liabilty rules)	No (but on illegal content such as incitement to hatred)	No (but indirectly on illegal content via liabilty rules)	No	No (but on content harmful to minors such as glorification of violence)	No
In effect since	2018	2018	2010	2000	2017	2007	1957	2002	1987
Status	Evaluation in 2019/2020	Evaluation in 2020	Last modified 2018, must be implemented in member states by 2020	Reform in 2020	Reform planned for 2019/2020	Last modified 2019	Last modified 2018, reform planned	Last modified 2016	Last modified 2018, reform until September 2020
EU connection	Yes, EU measure	Yes, EU measure, implementation in GER mostly via Federal Data Protection Act (BDSG)	Yes, EU measure	Yes, EU measure	No	Yes, partial implementation of E-Commerce Directive	Yes, partly determined by the Treaty on the Functioning of the European Union (TFEU)	Implementation of AVMSD open	Yes, planned reform partially implents AVMSD
Origin	European Commission	European Commission	European Commission	European Commission	Fed. Ministry of Justice and Consumer Protection	Fed. Ministry for Economic Affairs and Energy	Fed. Ministry for Economic Affairs and Energy	State chancelleries	State chancelleries
Key points regarding disinformation	Code: **Commitment** for companies regarding online political ads, cooperation with civil society, academia Action Plan: More resources and personnel for strategic communication, early warning system	**Limits on data collection and profiling** with rights for internet users (data subjects' rights), including rights of access, deletion and rectification, privacy by default, purpose limitation, data portability	Guidelines for independent national **media supervisory bodies**, latest version with focus on video portals	**Liability rules** and exceptions for internet service providers with regard to **illegal content** In DSA possibly EU-wide rules for content moderation, reform of liability rules, rules for political ads, specialized supervisory body	**Provisions based on criminal law** for social networks for reporting **illegal content** and deadlines for its removal; naming of contact persons for authorities; reporting obligations	**Liability rules** and exceptions for internet service providers with regard to **illegal content**	**Limits to market power**, most recently amended to account for digital era with merger control rule, extension of the factor catalog for determining market power	Requirements for illegal or **development-impairing content**; responsibility for voluntary self-regulatory bodies, e.g. multimedia service providers (FSM)	**Supervision over** TV, radio, telemedia New definitions in the planned version and **algorithm transparency rules** for search engines, video portals, social networks, etc.

Last updated: October 2019

Bibliography

Australian Competition and Consumer Commission. "Digital Platforms Inquiry - Final Report." Canberra: Australian Competition and Consumer Commission, July 26, 2019. https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

Avaaz. "Far Right Networks of Deceptions: Avaaz Uncovers Flood of Disinformation, Triggering Shutdown of Facebook Pages with over 500 Million Views Ahead of EU Elections." New York, NY: Avaaz, May 22, 2019. https://avaazimages.avaaz.org/Avaaz%20Report%20Network%20Deception%2020190522.pdf.

Bergen, Mark. "YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant." *Bloomberg*, April 2, 2019. https://www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant.

Bieber, Christoph, Leonhard Dobusch, and Jörg Müller-Lietzkow. "Die Internetintendanz." *Medienkorrespondenz*, April 28, 2019. https://www.medienkorrespondenz.de/leitartikel/artikel/die-internetintendanz.html.

Börsch, Michael. "Facebook: Anordnungen des Bundeskartellamts möglicherweise rechtswidrig und deshalb einstweilen außer Vollzug." *Oberlandesgericht Düsseldorf*, August 26, 2019. http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/index.php.

Bundeskartellamt. "B6-22/16: Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung." Bonn: Bundeskartellamt, February 7, 2019. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html;jsessionid=1758AF99E64A2D1B504758D23E7072EB.1_cid378?nn=3591568.

———. "Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen." *Bundeskartellamt*, February 7, 2019. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2.

Bundeszentrale für politische Bildung. "Debatte Netzwerkdurchsetzungsgesetz (NetzDG)." Bundeszentrale für politische Bildung, March 16, 2018. https://www.bpb.de/dialog/netzdebatte/262660/debatte-netzwerkdurchsetzungsgesetz-netzdg.

Bund-Länder-Kommission. "Bericht Bund-Länder-Kommission zur Medienkonvergenz." Berlin: Bund-Länder-Kommission, June 2016. https://www.bundesregierung.de/resource/blob/997532/473870/07ba875e860ada4556526641bd9151b6/2016-06-14-medienkonvergenz-bericht-blk-data.pdf?download=1.

CDU, CSU, and SPD. "Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode." Christlich Demokratische Union Deutschlands, March 12, 2018. https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1.

Competition and Markets Authority. "Online Platforms and Digital Advertising Market Study." GOV.UK, July 3, 2019. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

Davis, Trevor, Steven Livingston, and Matt Hindman. "Suspicious Election Campaign Activity on Facebook: How a Large Network of Suspicious Accounts Promoted Alternative Für Deutschland in the 2019 EU Parliamentary Elections." Washington, DC: The George Washington University, July 22, 2019. https://smpa.gwu.edu/sites/g/files/zaxdzs2046/f/2019-07-22%20-%20Suspicious%20Election%20Campaign%20Activity%20White%20Paper%20-%20Print%20Version%20-%20IDDP.pdf.

Department for Digital, Culture, Media & Sport, and Home Office. "Online Harms White Paper." London: Controller of Her Majesty's Stationery Office, April 8, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

Desmaris, Sacha, Pierre Dubreuil, and Benoît Loutrel. "Creating a French Framework to Make Social Media Platforms More Accountable: Acting in France with a European Vision." Paris: French Secretary of State for Digital Affairs, May 2019. https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E1B36873E4&filename=Mission%20Re%CC%81gulation%20des%20re%CC%81seaux%20sociaux%20-ENG.pdf.

Die Medienanstalten. "Stellungnahme der Medienanstalten zum überarbeiteten Diskussionsentwurf der Rundfunkkommission der Länder für einen 'Medienstaatsvertrag.'" Die Medienanstalten, August 9, 2019. https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Ueber_uns/Positionen/2019_08_09_Stellungnahme_der_Medienanstalten_zum_Medienstaatsvertrag.pdf.

Dobusch, Leonhard. "Die Organisation der Digitalität: Zwischen grenzenloser Offenheit und offener Exklusion." *netzpolitik.org*, February 1, 2017. https://netzpolitik.org/2017/die-organisation-der-digitalitaet-zwischen-grenzenloser-offenheit-und-offener-exklusion/.

dpa. "Facebook wehrt sich gegen NetzDG-Bußgeld." *heise online*, July 19, 2019. https://www.heise.de/newsticker/meldung/Facebook-wehrt-sich-gegen-NetzDG-Bussgeld-4475699.html.

Ellick, Adam B., Adam Westbrook, and Andrew Blackwell. "Operation Infektion: Russion Disinformation from Cold War to Kanye." *The New York Times*, November 12, 2018. https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html.

Europäische Kommission. "COM(2015) 192 final: Strategie für einen digitalen Binnenmarkt für Europa." Europäische Kommission, May 6, 2015. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52015DC0192&from=EN.

Europäischer Datenschutzbeauftragter. "Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von „Big Data": Das Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz in der digitalen Wirtschaft." Brüssel: Europäischer Datenschutzbeauftragter, March 2014. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_de.pdf.

European Commission. "A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation." Brüssel: European Commission, March 12, 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271.

———. "Action Plan against Disinformation." European Commission, December 5, 2018. https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

———. "EU Code of Practice on Disinformation." European Commission, September 26, 2018. https://ec.europa.eu/newsroom/dae/document.cfm?-doc_id=54454.

———. "JOIN(2019) 12 Final: Report on the Implementation of the Action Plan Against Disinformation." Brüssel: European Commission, June 14, 2019. https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf.

Ghosh, Dipayan, and Ben Scott. "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet." Washington, DC: New America, January 23, 2018. https://d1y8sb8igg2f8e.cloudfront.net/documents/Digital_Deceit_2_Final.pdf.

Hartung, Helmut. "'Das ist ziemlich einmalig': Interview mit Prof. Dr. Wolfgang Schulz, Direktor des Hans-Bredow-Instituts für Medienforschung." *Medienpolitik.net*, September 26, 2018. https://www.medienpolitik.net/2018/09/medienpolitikdas-ist-ziemlich-einmalig/.

———. "Medienstaatsvertrag: Der Vielfalt verpflichtet." *Frankfurter Allgemeine Zeitung*, August 9, 2019. https://www.faz.net/aktuell/feuilleton/medien/medienstaatsvertrag-der-vielfalt-verpflichtet-16324354.html.

Hoppenstedt, Max. "Strafbare Postings in sozialen Netzwerken: 'Woher der Hass kommt, ist wirklich nur schwer zu begreifen.'" *SPIEGEL ONLINE*, June 21, 2019. https://www.spiegel.de/netzwelt/netzpolitik/netzdg-staatsanwalt-christoph-hebbecker-ueber-hass-in-sozialen-netzwerken-a-1273176.html.

House of Commons Digital, Culture, Media and Sport Committee. "Disinformation and 'Fake News': Final Report." London: House of Commons, February 14, 2019. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

Jahromi, Neima. "The Fight for the Future of YouTube." *The New Yorker*, July 8, 2019. https://www.newyorker.com/tech/annals-of-technology/the-fight-for-the-future-of-youtube.

Kaye, David. *Speech Police: The Global Struggle to Govern the Internet*. Vol. Columbia Global Reports. New York: Columbia University in the City of New York, 2019.

Kluth, Winfried, and Wolfgang Schulz. "Konvergenz und regulatorische Folgen: Gutachten im Auftrag der Rundfunkkommission der Länder." Mainz: Rundfunkkommission der Länder, 2014. https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/Konvergenz-Gutachten.pdf.

Koch, Moritz, and Dietmar Neuerer. "Netzwerkdurchsetzungsgesetz: Die Bundesregierung erreicht im Kampf gegen Hate-Speech im Netz nur wenig." *Handelsblatt*, August 6, 2019. https://www.handelsblatt.com/politik/deutschland/netzwerkdurchsetzungsgesetz-die-bundesregierung-erreicht-im-kampf-gegen-hate-speech-im-netz-nur-wenig/24874984.html.

Kommission Wettbewerbsrecht 4.0. "Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft." Berlin: Bundesministerium für Wirtschaft und Energie, September 9, 2019. https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=4.

König, Jochen, and Juri Schnöller. "Wie digitale Plattformen sich um Transparenz bemühen." *Politik & Kommunikation*, July 9, 2019. https://www.politik-kommunikation.de/ressorts/artikel/wie-digitale-plattformen-sich-um-transparenz-bemuehen-1923588873.

Leyen, Ursula von der. "A Union That Strives for More: My Agenda for Europe." Brüssel: European Commission, July 16, 2019. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

Lupion, Bruno. "The EU Framework Against Disinformation: What Worked, What Changed and the Way Forward." Berlin: Democracy Reporting International, August 30, 2019. https://democracy-reporting.org/wp-content/uploads/2019/08/EU-Actions-Against-Disinformation-EP2019-Final.pdf.

Melford, Clare. "Disinformation Is an Online Harm." Global Disinformation Index, June 26, 2019. https://disinformationindex.org/2019/06/disinformation-is-an-online-harm/.

Meyer-Resende, Michael, and Rafael Goldzweig. "Online Threats to Democratic Debate: A Framework for a Discussion on Challenges and Responses." Berlin: Democracy Reporting International, June 26, 2019. https://democracy-reporting.org/wp-content/uploads/2019/06/BP_Threats-to-digital-democracy.pdf.

Mihr, Christian, and Daniel Moßbrucker. "Regulierung 2.0: Warum soziale Netzwerke, Suchmaschinen & Co. ein Teil der informationellen Grundversorgung geworden sind - und wie sie reguliert werden sollten, um die Meinungs-und Pressefreiheit zu schützen." Berlin: Reporter ohne Grenzen, June 12, 2018. https://www.reporter-ohne-grenzen.de/uploads/tx_lfnews/media/Reporter-ohne-Grenzen_Regulierung-2.0-Langfassung.pdf.

Mozilla Corporation. "Facebook and Google: This Is What an Effective Ad Archive API Looks Like." *The Mozilla Blog*, March 27, 2019. https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like.

Mueller, III, Robert S. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." Washington, DC: U.S. Department of Justice, March 2019. https://www.justice.gov/storage/report.pdf.

Newman, Nic. "Reuters Institute Digital News Report 2019." Oxford: Reuters Institute for the Study of Journalism, June 12, 2019. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-06/DNR_2019_FINAL_0.pdf.

Oberlandesgericht Düsseldorf. "Beschluss VI-Kart 1/19 (V) In der Kartellverwaltungssache 1. Facebook Inc., 2. Facebook Ireland Ltd., 3. Facebook Deutschland GmbH, Antragstellerinnen und Beschwerdeführerinnen,Verfahrensbevollmächtigte:... gegen Bundeskartellamt, Antragsgegner und Beschwerdegegner." Düsseldorf: Oberlandesgericht Düsseldorf, August 26, 2019. http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf.

Palese, Michela, and Josiah Mortimer, eds. *Reining in the Political 'Wild West': Campaign Rules for the 21st Century*. London: Electoral Reform Society, 2019. https://www.electoral-reform.org.uk/latest-news-and-research/publications/reining-in-the-political-wild-west-campaign-rules-for-the-21st-century/.

Paul, Katie. "Funders Threaten to Quit Facebook Project Studying Impact on Democracy." *Reuters*, August 28, 2019. https://www.reuters.com/article/us-facebook-election-research-idUSKCN1VI04F.

pbe/dpa. "Gericht verpasst Kartellamt im Verfahren gegen Facebook einen Dämpfer." *SPIEGEL ONLINE*, August 26, 2019. https://www.spiegel.de/netzwelt/apps/bundeskartellamt-gegen-facebook-oberlandesgericht-duesseldorf-bremst-a-1283736.html.

Podszun, Rupprecht. "Nach dem Facebook-Verfahren: Der Kartellrechts-Clash." *Legal Tribune Online*, September 13, 2019. https://www.lto.de/recht/hintergruende/h/facebook-verfahren-bkarta-ausbeutung-marktbeherrschung/.

Privacy International. "Social Media Companies Have Failed to Provide Adequate Advertising Transparency to Users Globally." *Privacy International*, October 3, 2019. http://privacyinternational.org/long-read/3244/social-media-companies-have-failed-provide-adequate-advertising-transparency-users.

Rau, Jan Philipp, and Sebastian Stier. "Die Echokammer-Hypothese: Fragmentierung der Öffentlichkeit und politische Polarisierung durch digitale Medien?" *Zeitschrift für Vergleichende Politikwissenschaft*, August 29, 2019, 1–19. https://doi.org/10.1007/s12286-019-00429-1.

Rotermund, Hermann. "Neuer Medienstaatsvertrag – alter Rundfunk." *CARTA online*, August 27, 2018. http://carta.info/neuer-medienstaatsvertrag-alter-rundfunk/.

Rudl, Tomas, and Alexander Fanta. "Geleaktes Arbeitspapier: EU-Kommission erwägt neues Gesetz für Plattformen." *netzpolitik.org*, July 15, 2019. https://netzpolitik.org/2019/geleaktes-arbeitspapier-eu-kommission-erwaegt-neues-gesetz-fuer-plattformen/.

Sängerlaub, Alexander. "Der blinde Fleck digitaler Öffentlichkeiten." Berlin: Stiftung Neue Verantwortung, March 21, 2019. https://www.stiftung-nv.de/sites/default/files/blinde.fleck_.digitale.oeffentlichkeit.pdf.

Sängerlaub, Alexander, Miriam Meier, and Wolf-Dieter Rühl. "Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017." Berlin: Stiftung Neue Verantwortung, March 26, 2018. https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf.

Schulz, Wolfgang, and Stephan Dreyer. "Stellungnahme zum Diskussionsentwurf eines Medienstaatsvertrags der Länder." Hamburg: Hans-Bredow-Institut, September 26, 2018. https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/qiuektv_HBI_StellungnahmeMedienstaatsvertrag180926.pdf.

Scott, Ben. "Did Google and Facebook Break Democracy?" *Progressive Centre UK*, July 30, 2019. https://www.progressivecentre.uk/did_google_and_facebook_break_democracy.

Shearlaw, Maeve. "Egypt Five Years on: Was It Ever a 'Social Media Revolution'?" *The Guardian*, January 15, 2016. https://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution.

Staatskanzlei Rheinland-Pfalz. Diskussionsentwurf für einen "Medienstaatsvertrag" (2019). https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/MStV-E_Synopse_2019-07_Online_.pdf.

Standing Committee on Access to Information, Privacy and Ethics. "International Grand Committee on Big Data, Privacy and Democracy." Standing Committee on Access to Information, Privacy and Ethics, June 2019. https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=10554743.

The Economist. "Now Playing, Everywhere: The Tricky Task of Policing YouTube." *The Economist*, May 4, 2019. https://www.economist.com/briefing/2019/05/04/the-tricky-task-of-policing-youtube.

Tworek, Heidi, and Paddy Leerssen. "An Analysis of Germany's NetzDG Law." Amsterdam: Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, April 15, 2019. https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

Wollebæk, Dag, Rune Karlsen, Kari Steen-Johnsen, and Bernard Enjolras. "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior:" *Social Media + Society*, April 9, 2019. https://doi.org/10.1177/2056305119829859.

Zimmer, Anja, ed. *Smart Regulation for Digital Media Pluralism*. Berlin: Medienanstalt Berlin-Brandenburg, 2019. https://mediapolicylab.de/files/content/document/Policy%20Statements/White_Book_MPL_July2019.pdf.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state. In order to guarantee the independence of its work, the organization adopted a concept of mixed funding sources that include foundations, public funds and businesses.

Issues of digital infrastructure, the changing pattern of employment, IT security or internet surveillance now affect key areas of economic and social policy, domestic security or the protection of the fundamental rights of individuals. The experts of the SNV formulate analyses, develop policy proposals and organize conferences that address these issues and further subject areas.

About the Author

Julian Jaursch is head of the project "Strengthening Digital Public Spheres | Policy". He analyzes and evaluates existing approaches to strengthen the digital public and identifies possible future regulatory measures. The aim of the project is to develop concrete policy recommendations for political and social decision-makers.

How to Contact the Author

Dr. Julian Jaursch
Project Director Strengthening Digital Public Sphere | Policy
jjaursch@stiftung-nv.de
+49 (0)30 81 45 03 78 93
@jjaursch

Imprint

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Editing:
Austin Davis
www.austinchandlerdavis.com

Graphic Design:
Anne-Sophie Stelke
www.annesophiestelke.com