Research Paper

Sophia Ignatidou
International Security Department | September 2019

EU–US Cooperation on Tackling Disinformation

CHATHAM HOUSE
The Royal Institute of International Affairs

Contents

Summary

- EU and US cooperation on tackling disinformation needs to be grounded in an international human rights framework in order to bridge the differences of both parties and include other countries facing this challenge.
- The disinformation debate needs to be reformulated to cover systemic issues rather than merely technical or security concerns. A lag in regulatory development has led to systemic vulnerabilities. In this context, policymakers need to push for more evidence-based analysis, which is only attainable if technology companies engage in honest debate and allow meaningful access to data – as determined by government appointed researchers rather than the companies themselves – taking into account and respecting users' privacy.
- Data governance needs to be the focus of attempts to tackle disinformation. Data's implications for information, market and power asymmetries, feed into and exacerbate the problem.
- Policymakers should focus on regulating the distribution of online content rather than the subject matter itself, which may have implications for freedom of speech.
- Disinformation is mainly the result of inefficient gatekeeping of highly extractive digital companies. The old gatekeepers, journalists and their respective regulators, need to be actively engaged in devising the new regulatory framework.
- Legacy media need to urgently consider the issue of 'strategic silence' and avoid being co-opted by political actors aiming to manipulate the accelerated, reactive news cycle by engaging in divisive 'clickbait' rhetoric verging on disinformation and propaganda. When strategic silence is not an option, contextual analysis is fundamental.
- The EU delegation should assist the coordination of EU–US efforts to tackle disinformation by drawing on the work and expertise at the G7 Rapid Response Mechanism (RRM), the Transatlantic Commission on Election Integrity (TCEI), the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the High-level Panel on Digital Cooperation, and work with the International Telecommunication Union (ITU) to foster a long-term interdisciplinary forum to harness technological innovation to protect and support democracy from threats such as disinformation.
- The EU and US must avoid rushed regulation that may condone enhanced surveillance or vilify journalism that scrutinizes those in power in the name of security.[1]

[1] Bradshaw et al. found that since 2016 at least 43 countries around the world have passed regulations to address the issue of disinformation or electoral interference. See Bradshaw, S., Howard, P. N. and Neudert, L. (2018), *Government Responses to Malicious Use of Social Media*, StratCom Coe, November 2018, https://www.stratcomcoe.org/government-responses-malicious-use-social-media (accessed 29 Jul. 2019).

1. Introduction

Disinformation, as the latest iteration of propaganda suitable for a digitally interconnected world, shows no signs of abating. Instead, it mutates and expands, threatening states' political security, civil rights,[2] and even public health.[3] The Delegation of the European Union to the United States commissioned this Chatham House paper with the aim of contributing to global efforts to tackle disinformation. The paper provides a holistic overview of the current state of play and outlines how EU and US cooperation can mitigate disinformation in the future.

After defining disinformation as a term, the paper maps legislative, institutional and technological actions to counter disinformation taken by governments, civil society and digital intermediaries (social media, search engines and app platforms) both in the US and the EU. The paper looks at previous and ongoing global interventions to tackle the problem and investigates how international efforts can inform and empower future EU–US cooperation. Echoing other researchers in the field it finds human rights rather than security to be the most appropriate basis for ongoing research and deliberations on disinformation. The paper recommends that the EU should harness its normative power to provide direction and share best practices from different member states that have been tackling disinformation.

Methodology

The author interviewed legal scholars, as well as officials in US agencies, EU institutions, NATO and advocacy organizations engaged in the research of disinformation or tasked with addressing hybrid threats more broadly. The paper also draws on panel discussions at the Conference on Data Protection and Democracy (CPDP) in Brussels and presentations by researchers working in the field of data governance, privacy and political campaign reform. Desk research included articles, official EU and US reports, and outputs from other research organizations. A first draft of this paper was presented at the EU–US Young Leaders Seminar 2019 in Brussels and debated among participants from the Fulbright US Student and EU-funded exchange programmes, as well as EU and US officials, all of which informed the final draft. The selected disinformation case studies were chosen due to the scale of their global impact and their potential implications for future political campaigning, foreign interference and internet governance more broadly. Given the speed of developments in the field of tech policy and disinformation, it is important to note this paper reflects the state of play in September 2019.

[2] Mozur, P. and Myers, S. L. (2019), 'China is waging a disinformation war against Hong Kong protesters', *New York Times*, 13 August 2019, https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html (accessed 14 Aug. 2019).
[3] UN News (2019), 'Misinformation and growing distrust on vaccines, "dangerous as a disease" says UNICEF chief', 28 June 2019, https://news.un.org/en/story/2019/06/1041571 (accessed 19 Aug. 2019).

2. Disinformation in Context

Definition and scope

After gaining notoriety on both sides of the Atlantic, the term 'fake news' has gradually been succeeded by the now prevailing 'disinformation', but a level of confusion around related terminology persists. Ambiguous definitions make it more difficult to find possible remedies. 'Fake news' insinuates that news producers and journalists should be held accountable for the pollution of the information space, and therefore are also implicitly responsible for tackling the problem. While 'fake news' scapegoats journalists, 'information warfare' alludes to offensive strategies that are often less nuanced and specific. The term 'foreign influence', although at times accurate, also runs the risk of cordoning off domestic propaganda purveyors such as political actors or foreign proxies. The scope of foreign influence is also broader than disinformation and according to the US Department of Justice (DoJ), the former may include hacking, malicious cyber activity, identity theft and fraud.[4] Although it is often used interchangeably with these other descriptions, use of the term disinformation enables a more nuanced and holistic analysis of what has become a global problem, by focusing on communication vectors and processes.

> Disinformation is defined as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm'.

According to the European Commission's Action Plan against Disinformation,[5] disinformation is defined as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm'. Harm can entail threats to democratic political and policymaking processes by undermining 'the trust of citizens in democracy and democratic institutions'. The inclusion of intentionality in the description also differentiates the term from misinformation.[6]

Disinformation can be overt, displaying factually false content but it can also take more subtle forms, such as the cherry-picking of statistics to mislead audiences and prime them in certain

[4] US Department of Justice (2018), *Justice Manual*, https://www.justice.gov/jm/jm-9-90000-national-security#9-90.730 (accessed 8 Mar. 2019).

[5] European Commission (2018), *Contribution to the European Council: Action Plan Against Disinformation*, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf (accessed 8 Mar. 2019).

[6] For more on disinformation typology, see Derakhshan, H. and Wardle, C. (2017), *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making – Council of Europe report, DGI(2017)09*, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (accessed 8 Mar. 2019).

ways,[7] or re-contextualized[8] or even tampered[9] visual material. Narratives can be adjusted to take advantage of the existing information space by tapping into divisive issues.[10]

Disinformation's shape-shifting nature and agility makes it a useful vehicle for hybrid threats or what the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) defines as a 'coordinated and synchronised action, that deliberately targets democratic states' and institutions' systemic vulnerabilities, through a wide range of means [political, economic, military, civil, and information]'.[11] Coordinated and amplified disinformation can crowd-out rational debate and sow confusion and discord,[12] numbing decision-making capacities. Indeed, hybrid threats aim to exploit the target's vulnerabilities and generate ambiguity to 'hinder decision-making processes'.[13]

Big data and its Faustian deal

Technological developments such as the 'datafication'[14] of different aspects of life, the rise of smart homes and smart cities, the Internet of Things (IoT), accelerating artificial intelligence (AI) development, and internet and mobile phone penetration, have vastly exacerbated the combined ripple effects of disinformation's complexity and scale. The prevailing data governance ambiguities, a tech sector far removed from public scrutiny and a utopian vision of how humanity and the market would interact with the internet – encapsulated in the famous Declaration of the Independence of Cyberspace by John Perry Barlow[15] – created cracks in the system and enabled privacy encroaching surveillance systems to be developed and refined. As Zuboff has highlighted, there is a need to attend to the anti-democratic implications of allowing the concentration of privacy rights 'among private and public surveillance actors', at the very moment those same

[7] Bump, P. (2018), 'Tucker Carlson's rhetoric on immigrants and crime is wildly misleading', *Washington Post*, 24 August 2018, https://www.washingtonpost.com/news/politics/wp/2018/08/24/tucker-carlsons-rhetoric-on-immigrants-and-crime-is-wildly-misleading (accessed 8 Mar. 2019).

[8] Dixon, H. (2017), 'Russian bot behind false claim Muslim woman ignored victims of Westminster terror attack', *Telegraph*, 13 November 2017, https://www.telegraph.co.uk/news/2017/11/13/russian-bot-behind-false-claim-muslim-woman-ignored-victims (accessed 8 Mar. 2019).

[9] Owen, L. H. (2019), 'What do we do about the "shallowfake" Nancy Pelosi video and others like it?', Nieman Lab, 31 May 2019, https://www.niemanlab.org/2019/05/what-do-we-do-about-the-shallowfake-nancy-pelosi-video-and-others-like-it (accessed 14 Jul. 2019).

[10] Research by SafeGuard Cyber into Russia-led disinformation ahead of the European parliamentary elections outlined seven different narrative categories the country had been employing to serve its interests: Freire, O. (2019), *Contactless Actions Against The Enemy: How Russia Is Deploying Misinformation on Social Media to Influence European Parliamentary Elections*, SafeGuard Cyber, 7 May 2019, https://www.safeguardcyber.com/blog/the-bots-never-left-how-russia-is-using-social-media-to-influence-european-parliamentary-elections (accessed 1 Jul. 2019).

[11] Hybrid CoE (n.d.), The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/hybrid-threats (accessed 5 Aug. 2019).

[12] Stamos, A. (2017), 'An update on information operations on Facebook', Facebook Newsroom, 6 September 2017, https://newsroom.fb.com/news/2017/09/information-operations-update (accessed 27 Mar. 2019).

[13] European Commission (2016), *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats – a European Union Approach JOIN(2016) 18 Final*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en (accessed 10 Mar. 2019).

[14] Cukier, K. and Mayer-Schoenberger, V. (2013), 'The Rise of Big Data: How It's Changing the Way We Think About the World', Foreign Affairs, Vol. 92, No. 3.

[15] Barlow, J. P. (1996), 'A Declaration of the Independence of the Cyberspace', Electronic Frontier Foundation, 8 February 1996, https://www.eff.org/cyberspace-independence (accessed 5 Aug. 2019).

rights are summarily and habitually removed from citizens resigned to the 'Faustian deal' of exchanging the right of privacy for a simulacrum of an effective digital life.[16]

Governments need to act to reverse this trend, which will only exacerbate the problem of disinformation. That is why the answer is not more surveillance of the online space or more debunking initiatives, but a re-appropriation of gatekeeper roles to responsible actors that have been or can be regulated sufficiently to fulfil them.

Key manifestations

Some suspicions of Russia's influence operations in relation to the Syrian war,[17] the downing of flight MH17,[18] the US 2016 national elections,[19] the US midterm elections,[20] and the Novichok attacks in the UK, have been confirmed but, to a large extent, they have mostly been debunked. However, the country remains the main source of disinformation in Europe.[21] Other state actors, such as Iran,[22] China,[23] or North Korea have also employed disinformation, as has been established both by the US and the European Parliament.[24]

Meanwhile, state-level domestic propaganda has also grown in recent years. Alarmingly, research indicates that over 28 state actors around the world have manipulated social media to target domestic as well as foreign audiences.[25] On both sides of the pond domestic actors such as politicians, commentators, or the far-right,[26] have also proved to be purveyors of disinformation,

[16] Zuboff, S. (2015), 'Big other: surveillance capitalism and the prospects of an information civilization', *Journal of Information Technology*, 30, pp. 83–84.
[17] Czuperski, M., Herbst, J. E., Higgins, E., Hof, F. and Nimmo, B. (2016), *Distract, Deceive, Destroy: Putin at War In Syria*, Atlantic Council, April 2016, https://publications.atlanticcouncil.org/distract-deceive-destroy (accessed 13 Mar. 2019).
[18] Alder-Nissen, R. and Golovchenko, Y. (2018), 'Who spread disinformation about the MH17 crash? We followed the Twitter trail', *Washington Post*, 20 September 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/09/20/who-spread-information-disinformation-about-the-mh17-crash-we-followed-the-twitter-trail (accessed 14 Mar. 2019).
[19] See Special Counsel Robert Mueller's indictment against Russia's Internet Research Agency, U.S. Department of Justice, https://www.justice.gov/file/1035477/download (accessed 27 Mar. 2019).
[20] Seligman, L. (2018), 'Mattis confirms Russia interfered in U.S. midterm elections', Foreign Policy, 1 December 2018, https://foreignpolicy.com/2018/12/01/mattis-confirms-russia-interfered-in-us-midterm-elections-putin-trump (accessed 27 Mar. 2019).
[21] European Parliament – Committee on Foreign Affairs (2019), *Report on a European Parliament recommendation to the Council and the Vice-President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties* (2018/2115(INI)), 28 January 2019, http://www.europarl.europa.eu/doceo/document/A-8-2019-0031_EN.pdf (accessed 8 Mar. 2019).
[22] Bing, C. and Stubbs, J. (2018), 'Exclusive: Iran-based political influence operation - bigger, persistent, global', Reuters, 18 August 2018, https://www.reuters.com/article/us-usa-iran-facebook-exclusive/exclusive-iran-based-political-influence-operation-bigger-persistent-global-idUSKCN1LD2R9 (accessed 28 Mar. 2019).
[23] For a comparative analysis of China's and Russia's different approach to influence operations see Garnaut, J. and Rosenberger, L. (2018), 'The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response', The Asan Forum, 8 May 2018, https://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response (accessed 14 Mar. 2019).
[24] European Parliament – Committee on Foreign Affairs (2019), *Report on a European Parliament recommendation to the Council and the Vice-President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties* (2018/2115(INI)).
[25] Bradshaw, S. and Howard, P. N. (2018), 'The global organization of social media disinformation campaigns', Journal of International Affairs 71 (1.5), 23–32, School of International and Public Affairs at Columbia University, https://jia.sipa.columbia.edu/global-organization-social-media-disinformation-campaigns.
[26] Frenkel, S. (2018), 'Facebook tackles rising threat: Americans aping Russian schemes to deceive', *New York Times*, 11 October 2018, https://www.nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html (accessed 27 Mar. 2019); Apuzzo, M. and Satariano, A (2019), 'Russia Is Targeting Europe's Elections. So Are Far-Right Copycats', *New York Times*, 21 March 2019, https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html (accessed 14 May 2019).

sometimes outperforming foreign actors in terms of reach. A case in point is research indicating that just two misleading claims by UK politicians during the EU referendum campaign were cited in 10.2 times more tweets than Brexit-related posts by Russian trolls.[27]

The objectives and vectors of disinformation vary just as much as the differing agents of influence operations. Armed and civilian non-state actors have both deployed disinformation to serve their ideological or financial goals, with Islamic State of Iraq and Syria (ISIS)[28] and a community of young Macedonians in Veles,[29] respectively, being well-documented examples. These two instances showcase how multifaceted the problem of disinformation is, in terms of different objectives pursued and the dissemination vectors used. While ISIS broadcast its radicalization messages on YouTube, the Macedonian actors took advantage of Google's AdSense interface.[30] The latter is part of a worldwide ad tech infrastructure that has only recently come under scrutiny as it uses online tracking,[31] data-driven targeting and real-time bidding via ad exchanges to reward attention-grabbing clickbait, which has supported the monetization of 'fake news' content.[32] Despite actions taken thus far, disinformation continues to be a profitable business.[33]

> Disinformation has manifested itself as first and foremost a systemic issue, not solely an agent problem. Agents exploit in-built vulnerabilities of the current digital ecosystem and the regulatory gaps in political environments that are already dislocated or prone to influence.

The issue has become more complex due to the divergence in the motivations of individuals who receive, share and amplify disinformation. Internet and social media users may willfully or unwittingly share false news in an attempt to signal their identity or values,[34] rather than influence their peers per se.

Disinformation has manifested itself as first and foremost a systemic issue, not solely an agent problem. Agents exploit in-built vulnerabilities of the current digital ecosystem and the regulatory gaps in political environments that are already dislocated or prone to influence.

[27] Bontcheva, K., Gorrell, G., Bakir, M., Roberts, I., Greenwood, M. and Iavarone, B. (2019), 'Partisanship, propaganda and post-truth politics: quantifying impact in online debate', University of Sheffield, arxiv.org/pdf/1902.01752.pdf (accessed 5 Aug. 2019).

[28] US Office of the Director for National Intelligence (2018), *First Responder's Toolbox*, 9 August 2018, https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/NCTC_DHS_FBI_First_Responders_Toolbox_-_Terrorist_Disinformation.pdf (accessed 5 Aug. 2019).

[29] Subramanian, S. (2017), 'The Macedonian teens who mastered fakes news', Wired, 15 February 2017, https://www.wired.com/2017/02/veles-macedonia-fake-news (accessed 13 Mar. 2019).

[30] As stated in its February 2019 CoP report, Google has taken steps to thwart the monetization of 'fake news' websites through its policy on insufficiently original content: See *Second monthly intermediate results of the EU Code of Practice against disinformation*, 20 March 2019, https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation.

[31] Media scholar Jonathan Albright has written an insightful blog post on tracking: 'Who hacked the election? Ad Tech did. Through "Fake News," Identity Resolution and hyper-personalization', Medium, 31 July 2017, https://medium.com/tow-center/who-hacked-the-election-43d4019f705f (accessed 27 Mar. 2019).

[32] As stated in Moore, M. (2018), *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age*, Oneworld Publications, 'advertisers would no longer be buying space on media outlets: they would be buying you'. Also, for more detailed analysis, see Ryan, J. (2018), *Behavioural advertising and personal data,* submitted with his complaint to the Irish Data Protection Commissioner over Ad Tech's data breaches: https://brave.com/Behavioural-advertising-and-personal-data.pdf.

[33] Duffy, C. (2019), 'Websites that peddle disinformation make millions of dollars in ads, new study finds', *CNN*, 18 August 2019, https://edition.cnn.com/2019/08/18/tech/advertising-disinformation-money-reliable-sources/index.html (accessed 19 Aug. 2019).

[34] Marwick, A. E. (July 2018), 'Why do people share fake news? A sociotechnical model of media effects', *Georgetown Law Technology Review*, 474, p. 505.

Context is paramount in any response and as Benkler et al. highlighted in their study of US media propaganda, ‘each country’s institutions, media ecosystems, and political culture will interact to influence the relative significance of the internet’s democratizing affordances relative to its authoritarian and nihilistic affordances.’[35] Any attempt to move towards solving or containing the problem should be grounded on a common set of principles by the cooperating actors and a deep awareness and respect of each system’s distinctive circumstances.

[35] Benkler, Y., Faris R. and Roberts H. (2018), *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, New York: Oxford University Press, p. 8.

3. Countermeasures to Disinformation

3.1 The view from the EU

In the run-up to the 2019 European elections,[36] almost three-quarters (73 per cent) of European citizens expressed concern about disinformation during pre-election periods[37] and 83 per cent considered it a problem in general.[38] Despite a fragmented media, political and regulatory environment, the EU appeared unified in its determination to deal with the issue of disinformation.

The UK, France,[39] Spain and Germany are just some examples of EU countries that have been the target of disinformation aiming to affect political processes. Nevertheless, EU responses are driven not just by political security concerns but also by human rights considerations too. The High-Level Group of Experts, set up by the European Commission to advise on policy to counter disinformation, concluded the problem should be addressed within the framework of the European Union Charter of Fundamental Rights (CFR) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).[40]

Data-driven microtargeted disinformation campaigns are particularly challenging for the rights enshrined in ECHR's articles 9 and 10, which relate to freedom of thought, conscience and religion and freedom of expression, respectively.[41] The stealth profiling of these influence operations, in combination with the subtext of plausible deniability, threaten the autonomy of targets and their freedom to 'hold opinions and to receive and impart information and ideas without interference'.

In a report on internet intermediaries, the Council of Europe (CoE) highlighted that 'the protection of privacy and personal data is fundamental to the enjoyment and exercise of most of the rights and freedoms' guaranteed in ECHR.[42] Even though the CoE is an international organization distinct from the EU,[43] cooperation between the two bodies has been reinforced

[36] Preliminary analysis from the Computational Propaganda Project ahead of the elections indicated most 'junk news' circulating on Twitter and Facebook revolved around divisive issues such as immigration and Islamophobia, rather than focusing on the Euroscepticism and European political leaders. See: Howard, P., Kollanyi, B., Marchal, N. and Neudert, L .(2019), 'Junk News During the EU Parliamentary Elections: Lessons from a Seven-Language Study of Twitter and Facebook', COMPROP, http://comprop.oii.ox.ac.uk/research/eu-elections-memo.

[37] European Commission (2018), *Special Eurobarometer 477: Democracy and Elections*, September 2018, http://data.europa.eu/euodp/en/data/dataset/S2198_90_1_477_ENG.

[38] European Commission (2018), *Flash Eurobarometer 464: Fake news and disinformation online*, April 2018, https://data.europa.eu/euodp/data/dataset/S2183_464_ENG.

[39] Avaaz (2019), *Yellow Vests Flooded by Fake News: Over 100m Views of Disinformation on Facebook*, 12 March 2019, https://www.politico.eu/wp-content/uploads/2019/03/AVAAZ_YellowVests_100miofake.pdf.pdf.pdf.

[40] European Commission (2018), *A Multi-Dimensional Approach to Disinformation: Report of the Independent High level Group on Fake News and Online Disinformation*, 12 March 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

[41] Council of Europe (1950), *European Convention on Human Rights*, https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[42] Council of Europe (2018), *Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries*, https://rm.coe.int/1680790e14 (accessed 8 Mar. 2019).

[43] Not to be confused with the Council of the European Union or the European Council.

recently and the formal accession of the EU to ECHR is still at the forefront of the debate.[44] In its report, CoE's recommendations for states included oversight and redress mechanisms in their regulatory frameworks, consideration of the size, structure and nature of intermediaries in their proposals, and the introduction of human rights impact assessments. CoE also highlighted the responsibility of intermediaries to protect users' human rights under the UN Guiding Principles on Business and Human Rights and the 'Protect, Respect and Remedy' Framework.[45]

CoE's recommendations for intermediaries were ambitious, including adequate training for content moderators, human rights impact assessments for automated content management, transparency in regard to user tracking and profiling, and banning of user data migration across devices and services without consent. However, industry pushback is expected – most likely in the form of either legal confrontation or deflective PR strategies – as these recommendations would impact algorithmic systems that are core components of digital platforms – such as Facebook's News Feed – as well as their data governance and their dominance of digital markets.

Following a toughening stance by EU policymakers, US counterparts are growing vocal about the need for tech regulation with various congressional committees moving it to the front of a broader reform agenda.

Nevertheless, following a toughening stance by EU policymakers, US counterparts are growing vocal about the need for tech regulation with various congressional committees moving it to the front of a broader reform agenda. Recent bills introduced to the House of Representatives, such as the Algorithmic Accountability Act by US senators Cory Booker and Ron Wyden,[46] the Deceptive Experiences To Online Users Reduction Act[47] by senators Mark Warner and Deb Fischer, or Senator Josh Hawley's Do Not Track Act,[48] may be ambitious at this point, but they definitely indicate the tide is turning. Both the EU and the US are facing similar systemic problems and similar adversarial actors, so drawing on the CoE's guidelines for digital intermediary regulation to create a common path is a wise step.

EU institutional responses

The 2019 European parliament elections put the EU on high alert, calling for active engagement in the fight against disinformation from all member states. The European Commission's Action Plan against Disinformation established four key pillars: 1) a coordinated response by the EU, mobilizing all government departments; 2) improving detection, analysis

[44] The process of accession was stalled after the Court of Justice of the European Union ruled the draft of accession was not compatible with EU law in December 2014.

[45] United Nations (2011), *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*, Office of the United Nations High Commissioner for Human Rights, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (accessed 1 Jul. 2019).

[46] US Congress (2019), *S.1108 - Algorithmic Accountability Act of 2019*, https://www.congress.gov/116/bills/s1108/BILLS-116s1108is.pdf (accessed 1 Jul. 2019). The act would authorize the FTC to mandate companies conduct impact assessments of automated decision systems among others.

[47] US Congress (2019), *S. 1084: Deceptive Experiences To Online Users Reduction Act*, https://www.govtrack.us/congress/bills/116/s1084/text.

[48] US Congress (2019), Do Not Track Act, https://www.congress.gov/bill/116th-congress/senate-bill/1578/text (accessed 1 Jun. 2019).

and exposure capabilities; 3) mobilizing the private sector; and 4) building societal resilience and raising awareness through conferences, debates, specialized training and media literacy programmes to enable citizens to spot disinformation.

As part of the third pillar, in September 2018, digital intermediaries committed to a Code of Practice (CoP)[49] and were tasked with providing monthly reports on its application, with the Commission warning that if there was no improvement in the fight against disinformation by the end of 2019 it would consider regulation. The list of signatories included Facebook, Google, YouTube, Twitter, Mozilla, as well as advertisers and trade associations representing online platforms and the advertising industry. The European Regulators Group for Audio-visual Media Services (ERGA) would assist the Commission in assessing the effectiveness of these commitments. The Commission called on the signatories to ensure 'full transparency of political ads', access to data for research purposes and to facilitate close cooperation between them and national governments through the Rapid Alert System (RAS).

Advocacy groups highlighted the fact that the CoP remains a voluntary, self-regulatory measure and that they demand clearer objectives and an effective monitoring system enforcing compliance via sanctions or other actions. CoP's efficiency will be judged in the long term as the results thus far have been mixed and at times, highly inadequate. Although the monthly reports of social media platforms have listed substantial fake account takedowns and similar actions, the Commission has repeatedly called for improvements in terms of monitoring efficiency, sufficient information delivery, and more clarity in terms of their strategy to tackle disinformation.[50] Even after the European parliament elections, the Commission still criticized companies' insufficient progress in increasing the transparency and trustworthiness of websites hosting ads.[51]

As months progressed, various events compromised technology companies' trust capital. In January 2019 despite being a signatory to the CoP thereby committing to 'support good faith independent efforts to track disinformation and understand its impact' and to refrain from prohibiting or discouraging 'good faith research into disinformation', Facebook limited access to information that ProPublica, Mozilla and WhoTargetsMe built tools to monitor,[52] leading to an outcry from the researcher community.[53] Facebook did eventually open its Ad Library API in late March 2019,[54] but researchers expressed their concerns that the API did not provide all the necessary data,[55] and subsequently reported a wealth of technical issues that impeded on their

[49] European Commission (2018), *Code of Practice on Disinformation*, 26 September 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[50] European Commission (2019), *Code of Practice Against Disinformation: Commission Calls on Signatories to Intensify their Efforts*, 29 January 2019, https://ec.europa.eu/commission/news/code-practice-against-disinformation-2019-jan-29_en.

[51] European Commission (2019), *A Europe that Protects: EU Reports on Progress in Fighting Disinformation ahead of European Council*, 14 June 2019, https://europa.eu/rapid/press-release_IP-19-2914_en.htm.

[52] Schmidt, C. (2019), 'Facebook roadblocks ProPublica's ad transparency tool (gee, what a good time for a safe harbor)', Nieman Lab, 31 January 2019, https://www.niemanlab.org/2019/01/facebook-roadblocks-propublicas-ad-transparency-tool-gee-what-a-good-time-for-a-safe-harbor (accessed 13 Mar. 2019).

[53] Mozilla (2019), 'Open letter to Facebook', https://foundation.mozilla.org/en/campaigns/eu-misinformation (accessed 13 Mar. 2019).

[54] Shukla, S. (2019), 'A Better Way to Learn About Ads on Facebook', 28 March 2019, https://newsroom.fb.com/news/2019/03/a-better-way-to-learn-about-ads (accessed 5 May 2019).

[55] Mozilla (2019), 'Facebook's Ad Archive API is Inadequate', 29 April 2019, https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadequate (accessed 14 May 2019).

work.[56] After months of deliberations, progress has been slow. Irrespective of improved monitoring of disinformation during the EU elections, those wishing to influence political events are reportedly able to circumvent checks by using the business manager account feature on Facebook,[57] which highlights the cat and mouse nature of policymakers' approach to technology companies.

The RAS, launched in March 2019, is an interface to enable information sharing among stakeholders and for issuing alerts about foreign malign influence campaigns in real time. Each EU member state appointed a contact point for RAS and its editorial control rests with the East StratCom Task Force.[58] East StratCom has long-term expertise, dealing with malign foreign influence operations in the Eastern Neighbourhood – especially from Russia – so it plays a central role in advising the EU on how to analyse and respond to disinformation. The taskforce tries to support media plurality in the region and improve EU communication on its objectives. East StratCom also participated in a tripartite group with the Commission and the European parliament preparing for the European elections. The Action Plan called for the reinforcement of the Strategic Communication Task Forces of the European External Action Service (EEAS) and the establishment of close cooperation between RAS and the G7 Rapid Response Mechanism to support the resilience of allies to disinformation.

It will be easier for the EU to successfully communicate what the union stands for if divisive actors within individual countries advocating fragmentation are challenged and counteracted by coherent political, economic and social arguments.

The EEAS also engages in proactive communication to avoid leaving space for malign actors to spread disinformation. Strategic communication is deployed by the European Commission, too, which also tries to counteract disinformation that attacks the EU's legitimacy with positive messaging.[59] It will be easier for the EU to successfully communicate what the union stands for if divisive actors within individual countries advocating fragmentation are challenged and counteracted by coherent political, economic and social arguments.

An internal network on disinformation has been established within the Commission, to build awareness and exchange information between the different directorates-general and representations in member states. Their monitoring is mainly focused on disinformation that targets the EU while an equivalent group has been established within the European parliament to monitor disinformation against individual parties and politicians. In January 2019, Federica Mogherini, the high representative for foreign affairs and security policy, highlighted that

[56] Ahead of the EU elections Facebook's Ad Transparency tool, for example, was mired in bugs and technical issues, impeding the work of researchers. Rosenberg, M. (2019), 'Ad tool Facebook built to fight disinformation doesn't work as advertised', *New York Times*, 25 July 2019, https://www.nytimes.com/2019/07/25/technology/facebook-ad-library.html (accessed 13 Aug. 2019).

[57] Waterson, J. (2019), 'Revealed: Johnson ally's firm secretly ran Facebook propaganda network', *Guardian*, 1 August 2019, https://www.theguardian.com/politics/2019/aug/01/revealed-johnson-allys-firm-secretly-ran-facebook-propaganda-network (accessed 13 Aug. 2019).

[58] East StratCom is also running the EUvsDisinfo website: https://euvsdisinfo.eu.

[59] Two examples are the EU Protects or the EU And Me campaigns.

attention needs to be paid to different kinds of disinformation both inside and outside the EU.[60] In terms of building public resilience, the European Commission also supports a European network of fact-checkers that was initially coordinated by East StratCom. Fact-checking efforts although fundamental should not be seen as a silver bullet, as their ability to mitigate the effect of information campaigns is limited.

The European Union Agency for Cybersecurity (ENISA) also recommended robust cybersecurity measures for political organizations' systems, infrastructures, and data, as well as – following the example of the US Department of Homeland Security (DHS) – the classification of election systems as critical infrastructure.[61]

Notable member state responses

The below list of member states is by no means exhaustive, and the examples were selected on the basis of actions that have proved to be best practices.

- **The Czech Republic** approached the disinformation issue from a security perspective when it included foreign influence operations in the areas covered in its 2016–17 National Security Audit. According to a report by the European Values think-tank, the audit's recommendations made the system more resilient.[62]
- **Finland** has also proved resilient to disinformation by taking similar steps.[63] In January 2016, 100 officials were trained to identify and understand the phenomenon, with the intention to produce a coherent government response. The country is also investing in media and information literacy more broadly.[64]
- **France** passed its own anti-disinformation law following incidents of malign influence campaigns during the 2017 pre-election period. The law concerns solely pre-election periods (three months before a vote) and makes intermediaries accountable to the Superior Audiovisual Council (CSA). Media literacy is also a component. Although it was originally opposed[65] on the basis of the 48-hour take-down window, which was seen as too short, and on freedom of expression considerations, the Constitutional Court upheld the

[60] European Union (2019), 'Mogherini and EU Foreign Ministers: Moving ahead with the Action Plan against Disinformation', 21 January 2019, https://eeas.europa.eu/headquarters/headquarters-homepage/56854/mogherini-and-eu-foreign-ministers-moving-ahead-action-plan-against-disinformation_my.

[61] ENISA (2019), *Election Cybersecurity: Challenges and Opportunities*, February 2019, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities/view (accessed 5 Aug. 2019).

[62] European Values (2018), *Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe*, 30 April 2018, https://www.europeanvalues.net/vyzkum/prague-manual (accessed 5 Aug. 2019).

[63] Standish, R. (2017), 'Why Is Finland Able to Fend Off Putin's Information War?', Foreign Policy, 1 March 2017, https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war (accessed 11 Mar. 2019).

[64] National Audiovisual Institute, Finland (2017), *Finnish Media Education: Promoting Media and Information Literacy in Finland*, https://kavi.fi/sites/default/files/documents/mil_in_finland.pdf; Finland recently came first in a Media Literacy Index mapping 35 countries. See Mackintosh, E. (2019), ' Finland is winning the war on fake news. What it's learned may be crucial to Western democracy', CNN, May 2019, https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl (accessed 21 May 2019).

[65] Ricci, A. D. (2018), 'French opposition parties are taking Macron's anti-misinformation law to court', Poynter, 4 December 2018, https://www.poynter.org/fact-checking/2018/french-opposition-parties-are-taking-macrons-anti-misinformation-law-to-court (accessed 7 Mar. 2019).

statute as constitutional. Researchers have argued the statute has blind spots, such as the narrow framing of what constitutes false information without paying much attention to the actual process of online manipulation (revealing the actors and the incentives).[66]

- **Germany** ratified the Network Enforcement Act, or so-called NetzDG, in January 2018, which obliges large digital intermediaries to remove material 'obviously illegal' under the German penal code in less than 24 hours. When content legality can be disputed, the time frame may be extended to seven days. Fines can reach €50 million. The main criticism of NetzDG relates to its short compliance time frame, freedom of speech concerns,[67] as well as fear of pre-emptive self-censorship by the platforms themselves.[68]

  In February, Germany's antitrust regulator ruled that Facebook had to stop the 'unrestricted collection and assigning of non-Facebook data to their Facebook user accounts'[69] without meaningful consent. Competition law has been mobilized by various EU states[70] that examine the market repercussions of intermediaries' business models and strategies.[71]

- **Spain** launched a taskforce to fight disinformation comprising experts from the National Security Department, the Office for the State Secretary for Communication and other ministries.[72] According to Hybrid CoE, the country was the target of disinformation operations in relation to the Catalan independence referendum.[73]

- **Sweden**, along with other Nordic and Baltic countries, has been widely praised for measures against disinformation. Sweden's best practice for example was to take a holistic approach in the run-up to its 2018 elections and train over 10,000 civil servants on how to spot influence operations, reform its elementary and high school curriculum to include digital and media literacy,[74] while its Civil Contingencies Agency even produced a 'Countering Information Influence Activities' handbook for public-sector employees.

- **The UK** House of Commons' Digital, Culture, Media and Sport (DCMS) Committee launched an inquiry into disinformation and 'fake news' in response to the Cambridge Analytica scandal. The Committee invited parliamentarians from nine countries around

[66] Author interview with Kamel Ajji, Phd Candidate at Paris 2 University.

[67] Delcker, J. and Scott, M. (2018), 'Free speech vs. censorship in Germany', Politico, 1 April 2018, https://www.politico.eu/article/germany-hate-speech-netzdg-facebook-youtube-google-twitter-free-speech (accessed 19 May 2019).

[68] Schulz, W. (2018), 'Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG', in Albers, M. and Scarlet, I., (eds)*, Personality and Data Protection Rights on the Internet*, forthcoming.

[69] Dreyfuss, E. (2019), 'German regulators just outlawed Facebook's whole ad business', Wired, 7 February 2019, https://www.wired.com/story/germany-facebook-antitrust-ruling (accessed 7 Mar. 2019).

[70] Hern, A. (2018), 'Italian regulator fines Facebook £8.9m for misleading users', *Guardian*, 7 December 2018, https://www.theguardian.com/technology/2018/dec/07/italian-regulator-fines-facebook-89m-for-misleading-users (accessed 8 Mar. 2019).

[71] Article 102 of the Treaty on the Functioning of the European Union (TFEU) prohibits the abuse of market dominance. That abuse can be exclusionary, discriminatory or exploitative, such as the excessive collection of data of predatory data protection policies. Thankfully the debate on consumer welfare is moving from price differentiations to changes in choices and quality.

[72] Abellán, L. (2019), 'Spain launches unit to fight disinformation ahead of elections', El País, 11 March 2019, https://elpais.com/elpais/2019/03/11/inenglish/1552290997_611483.html (accessed 27 Mar. 2019).

[73] Arcos, R. (2018), *Strategic Analysis October 2018: Post-Event Analysis of the Hybrid Threat Security Environment: Assessment of Influence Communication Operations*, Hybrid CoE, 7 November 2018, https://hybridcoe.fi/wp-content/uploads/2018/11/Strategic-Analysis-2018-10-Arcos.pdf.

[74] Cederberg, G. (2018), *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, Harvard Kennedy School Belfer Center for Science and International Affairs, August 2018, https://www.belfercenter.org/publication/catching-swedish-phish-how-sweden-protecting-its-2018-elections (accessed 14 Jul. 2019).

the world (Argentina, Belgium, Ireland, Latvia, Brazil, Canada, Singapore, France and the UK) to participate in an International Grand Committee on disinformation that would nurture cross-border cooperation, starting with a meeting in November 2018 that led to the signing of the declaration on the Principles of the Law Governing the Internet.[75] The final report of the DCMS committee was published in February 2019,[76] recommending among other things, the establishment of a new category of tech company, a compulsory Code of Ethics, the protection of inferred data as personal data, a levy on tech companies to support the expanded work of the Information Commissioner's Office (ICO), enhanced powers for the Electoral Commission to make it efficient for the 21st century, an audit of the online advertising market as well as strategic communications companies, primary legislation regulating the use of personal information in political campaigns. Finally, it recommended the re-introduction of 'friction' into social media platforms to allow time for deliberation before stories are shared or interacted with. The UK government responded to the DCMS report's recommendations by announcing digital imprints for political advertising and the introduction of a new regulatory framework for social media companies with a statutory duty of care outlined in the Online Harms White Paper (OHWP).[77] The introduction of a new concept of legal entity that would be relevant to the power, responsibilities and scale of digital intermediaries that the DCMS suggested, although not adopted by the UK government, merits further examination by the EU and the US, as the multifaceted and multi-domain implications of evolving technologies merit new and equally innovative thinking.

OHWP was to a certain extent trapped by its vast ambitions and its commendable consultation process led civil society and research institutions to voice concerns such as the lack of nuance and clarity in definition of harms, or the ambiguity of how disinformation is defined.[78] OHWP also suggested 'duty of care' as an approach to regulate digital intermediaries but has been criticized as inadequate or in need of reframing, as it does not automatically translate from an offline to an online context, and more clarity in terms of companies' duties is needed.[79]

Civil society and academia

To this day the EU has dedicated substantial funding not just towards expanding the capabilities of its existing institutions but also into academic research and technology initiatives tasked with addressing the disinformation threat. For instance, the European Research Council has supported

[75] UK House of Commons – Digital, Culture, Media and Sport Committee (2018), 'Parliamentarians from across the world sign declaration on the "Principles of the Law Governing the Internet"', 27 November 2018, https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/declaration-internet-17-19 (accessed 5 Aug. 2019).
[76] UK House of Commons – Digital, Culture, Media and Sport Committee (2019), *Disinformation and 'Fake News': Final Report*, 14 February 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf (accessed 5 Aug. 2019).
[77] UK Department for Digital, Culture, Media and Sport (2019), *Online Harms White Paper*, 8 April 2019, https://www.gov.uk/government/consultations/online-harms-white-paper (accessed 1 Jul. 2019).
[78] The Alan Turing Institute (2019), *Response of the Public Policy Programme to the DCMS and the Home Office's Online Harms White Paper*, https://www.turing.ac.uk/research/publications/dcms-and-home-office-consultation-online-harms-white-paper.
[79] Nash, V. (2019), 'Internet Regulation and the Online Harms White Paper: Stakeholder Workshop Summary', Oxford Internet Institute, 1 July 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3412790 (accessed 1 Jul. 2019).

the work of the Computational Propaganda Research Project (COMPROP) in Oxford, which monitors and analyses social media-driven manipulation of public opinion.

Through the Horizon 2020 research programme, the EU has also provided funding for the Social Observatory for Disinformation and Social Media Analysis, and the projects it coordinates (SocialTruth, Provenance, Eunomia, WeVerify[80]) creating a multidisciplinary network of academic researchers, fact-checkers, technologists, media organizations and policymakers. Horizon 2020 also supports the three-year Provenance project at Dublin City University's Institute for Future Media and Journalism (FuJo) that's working on a free verification tool using blockchain. The European Parliament's Science-Media Hub is also contributing to the efforts of raising awareness and supporting research on disinformation.[81]

LSE's Arena, as well as its Truth, Trust & Technology Commission have conducted research[82] and organized events on disinformation, while four Nordic universities from Denmark, Sweden and Norway, have launched an interdisciplinary network to study the impact of online disinformation on democratic processes.[83] The network launched a series of disinformation conferences in Aarhus in May.[84]

Further independent initiatives in Europe

Debunk.eu: The Lithuanian initiative incorporates AI tools, volunteer fact-checkers and journalists, to monitor disinformation on a daily basis, and assists academic research and media outlets with debunking.

Global Disinformation Index (GDI): With the support of the Knight Foundation – among others – UK-based non-profit GDI is working to create a global rating system for media outlets.

Newtral and **Maldito Bulo:** The two Spanish fact-checking initiatives provided much needed assistance in the fight against disinformation in the last national elections.[85]

Transparent Referendum Initiative: The Irish volunteer-run organization was launched in the lead-up to the referendum on the repeal of the 8th Amendment with the aim of enabling 'fair, truthful and respectful debate', by collecting and publicizing data on Facebook Ads. Its founder went on to broaden its scope by launching Digital Action.[86]

[80] WeVerify are developing next-generation verification tools enabling cross-modal verification, which can target affected users by verification, catalogue and file disinformation and use a blockchain database of debunked content.

[81] Ignatidou, S. (2019), 'The promise and limitations of technological solutions to disinformation', European Science-Media Hub, 20 March 2019, https://sciencemediahub.eu/2019/03/20/the-promise-and-limitations-of-technological-solutions-to-disinformation (accessed 5 Aug. 2019).

[82] The LSE Commission on Truth, Trust and Technology (2018), *Tackling the Information Crisis*, http://www.lse.ac.uk/media-and-communications/truth-trust-and-technology-commission/The-report (accessed 1 Jul. 2019).

[83] Online disinformation: an Integrated View, https://nordis.research.it.uu.se.

[84] In the context of the same conference the EU Center for Research in Social Media and Information Disorder (EU REMID) was also launched.

[85] Tardáguila, C. (2019), 'Spain has a new government and its fact-checkers had an impact on the campaign', Poynter, 3 May 2019, https://www.poynter.org/fact-checking/2019/spain-has-a-new-government-and-its-fact-checkers-had-an-impact-on-the-campaign (accessed 14 May 2019).

[86] Digital Action, https://digitalaction.co.

3.2 US responses

The US context

According to Pew,[87] more Americans are now accessing news through social media than print newspapers, with television remaining the most popular platform for news consumption (49 per cent of adults use it to stay informed). The combined percentage of social media and news website regulars (43 per cent) is edging closer to that of TV. With the widening gap between the habits of news consumption among the young (online) and over-50s (TV), and an increasing percentage of audiences receiving news through social media and search engines rather than direct visits to media websites, it's a matter of time before digital platforms become the leading source of news for US citizens.

The US media ecosystem features asymmetric media dynamics, mainly skewed by hyper-partisan outlets that, as Benkler et al. have noted, leave a percentage of the population 'systematically disengaged from objective journalism'.[88] Alarmingly, a 2018 Ispos survey of over 1,000 adults, found that despite overwhelming support for freedom of the press (85 per cent), almost a third of American respondents agreed with the assertion that the media are 'the enemy of the American people' (29 per cent).[89] Persistent attacks on the press have permeated political discourse, creating challenges for journalists and the democratic system that relies on the Fourth Estate.

According to a report by cybersecurity firm Recorded Future, hyper-partisanship is being exploited by certain Russian influence operations, which have moved from disseminating disinformation to amplifying hyper-partisan messages and polarizing statements by politicians, often sourced in traditional media.[90] Polarization is indeed becoming a problem in European political discourse too.

> In the US, the First Amendment's protection of freedom of speech imposes its own constraints on US policymakers and officials, who thus far opted for transparency as an approach to the disinformation problem rather than outright bans.

In the US, the First Amendment's protection of freedom of speech imposes its own constraints on US policymakers and officials, who thus far opted for transparency as an approach to the disinformation problem rather than outright bans. Nevertheless, the merits of meaningful transparency may be more obvious for researchers, journalists and actors as a means to hold politicians, companies and advertisers to account rather than for the public itself, which tend to avoid the 'friction' of reading terms of service or scrutinizing ad transparency tools as part of their

[87] Shearer, E. (2018), 'Social media outpaces print newspapers in the U.S. as a news source', Pew Research Center, 10 December 2018, https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source (accessed 8 Mar. 2019).

[88] Benkler, Faris and Roberts (2018), *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*.

[89] Ipsos (2018), 'Americans' view on the media', Ipsos, 7 August 2018, https://www.ipsos.com/en-us/news-polls/americans-views-media-2018-08-07 (accessed 6 Mar. 2019).

[90] Insikt Group (2019), *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion*, Recorded Future, 6 March 2019, https://www.recordedfuture.com/china-social-media-operations (accessed 28 Mar. 2019).

day-to-day digital activities. Digital and media literacy initiatives may inoculate the public to a certain extent by raising awareness of the cost of a frictionless online existence and of not confronting disinformation, which may lead to long-term positive outcomes.

Institutional responses

Congressional oversight: The US Senate Select Committee on Intelligence (SSCI) has convened hearings inviting Facebook's COO, Sheryl Sandberg, Twitter's CEO, Jack Dorsey[91] (Alphabet's CEO Larry Page declined) and commissioned two reports on the online influence tactics of the Russian Internet Research Agency.[92] Google's CEO Sundar Pichai eventually testified in front of the House Committee on the Judiciary.

From January 2019 onwards, the House Energy and Commerce, Intelligence and Judiciary committees launched a series of probes into how tech companies and their strategies affect competition, consumers and society.[93] A session by the House Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce[94] uncovered some issues such as the need to distinguish between various data practices that pose threats to consumers, avoid regulatory patchwork across states, and outline clear prohibitions on a range of harmful and unreasonable data collection practices.

Federal agencies: The 2017 National Defense Authorization Act, signed into law by then US President Barack Obama in December 2016, established the Global Engagement Center (GEC) at the Department of State. GEC became the central hub tasked with integrating inter-agency efforts to recognize, analyse and expose disinformation efforts that threaten US national security interests globally, particularly focusing on threats from Russia, China, North Korea and Iran. Apart from working closely with the White House's National Security Council, the center also engages with foreign state partners, the private sector[95] and civil society (funding media literacy efforts and research among others). GEC is in communication with the EU's StratCom East Task Force, NATO's StratCom Centre of Excellence in Riga and Hybrid CoE, but most channels of communication with the EU are established on a bilateral basis.

In November 2017, the FBI created the Foreign Influence Task Force (FITF) to identify and counteract 'malign foreign influence operations targeting the United States',[96] by monitoring mainly the domestic environment. FITF takes an agent-focused approach, observing foreign

[91] US Senate Select Committee on Intelligence (2018), 'Hearing on foreign influence operations' use of social media platforms', 5 September 2018, https://www.intelligence.senate.gov/hearings/open-hearing-foreign-influence-operations%E2%80%99-use-social-media-platforms-company-witnesses.

[92] US Senate Select Committee on Intelligence (2018), 'New Reports Shed Light on Internet Research Agency's Social Media Tactics', 17 December 2018, https://www.intelligence.senate.gov/press/new-reports-shed-light-internet-research-agency%E2%80%99s-social-media-tactics (accessed 7 Mar. 2019).

[93] Romm, T. (2019), 'Democrats vow Congress will "assert itself" against tech — starting with Silicon Valley's privacy practices', *Washington Post*, 26 February 2019, https://www.washingtonpost.com/technology/2019/02/26/democrats-vow-congress-will-assert-itself-against-tech-starting-with-silicon-valleys-privacy-practices (accessed 13 Mar. 2019).

[94] US House Committee on Energy & Commerce (2019), 'Hearing on "protecting consumer privacy in the era of big data"', 26 February 2019, https://energycommerce.house.gov/committee-activity/hearings/hearing-on-protecting-consumer-privacy-in-the-era-of-big-data.

[95] GEC also has a team dedicated to emerging and existing technologies.

[96] FBI (2018), 'Combating foreign influence', https://www.fbi.gov/investigate/counterintelligence/foreign-influence (accessed 5 Aug. 2019).

actors known to deploy disinformation campaigns, in an effort to avoid any First Amendment conflicts. In March 2019, FBI Director Christopher Wray stated that divisive foreign influence campaigns against Americans had continued 'virtually unabated'[97] but expressed his optimism in the potential of FITF working closely with social media companies, GEC, the National Security Agency (NSA), the Department of Homeland Security (DHS), and the Office of the Director of National Intelligence. DHS's Cybersecurity and Infrastructure Security Agency (CISA), launched in November 2018, is tasked with dealing with foreign influence. Former Director of National Intelligence Dan Coats stated the intelligence community needs to be restructured to deal with the 'evolving flood of technological changes' and warned that foreign actors will try to influence the 2020 US elections.[98]

The work of the Department of Defense's Cyber Command (USCYBERCOM) during the 2018 midterm elections has been praised by senators on both sides of the aisle, for deterring Russian hackers suspected of conducting disinformation campaigns by signaling to them that they had been identified. According to press reports and under the 'defend forward' strategy,[99] USCYBERCOM also disrupted the internet access of the Russian Internet Agency on the day of the 2018 midterms.[100] DoD's Defense Advanced Research Projects Agency (DARPA) is also working on developing tools to spot disinformation campaigns and detect 'deep fakes'.[101]

> The US Agency for Global Media (USAGM) is running training programmes for spotting disinformation, has Russian language services in Eastern Europe, two Korean services, a new Persian channel, and is looking to expand its Mandarin output too.

The Department of Justice (DoJ) was also mobilized against disinformation in February 2018, with the then-Attorney General Jeff Sessions establishing the Cyber-Digital Task Force. The DoJ has also reviewed the US Attorney's Manual and introduced Section 9-90.730, which provided guidelines for the DoJ to disclose information about foreign influence operations either publicly or privately to the targets or the tech companies hosting the operations. The remit of the Manual's amendment is strictly influence campaigns when foreign government attribution can be made

[97] RSA Conference (2019), 'The FBI: at the heart of combating cyberthreats', 5 March 2019, https://www.rsaconference.com/videos/the-fbi-at-the-heart-of-combating-cyberthreats (accessed 10 Mar. 2019).
[98] US Senate Select Committee on Intelligence (2019), 'Hearing to consider worldwide threats', 29 January 2019, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats.
[99] US Department of Defense (2018), *Department of Defense Cyber Strategy: Summary 2018*, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed 10 Mar. 2019). For a useful analysis also see Chesney, R. (2018), 'The 2018 DOD Cyber Strategy: understanding "defense forward" in light of the NDAA and PPD-20 changes', 25 September 2018, https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes (accessed 10 Mar. 2019).
[100] Nakashima, E. (2019), 'U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms', *Washington Post*, 27 February 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html (accessed 10 Mar. 2019).
[101] Knight, W. (2018), 'The Defense Department has produced the first tools for catching deepfakes', MIT Technology Review, 7 August 2018, https://www.technologyreview.com/s/611726/the-defense-department-has-produced-the-first-tools-for-catching-deepfakes (accessed 26 Mar. 2019).

with ‘high confidence’, leaving campaigns of unknown or domestic sources outside its scope. This approach appears selective in its interpretation of how networks operate and may create serious vulnerabilities in the system that the US will be forced to face sooner rather than later.

Employing counter-narratives is another approach the US is taking. The US Agency for Global Media (USAGM) is running training programmes for spotting disinformation, has Russian language services in Eastern Europe, two Korean services, a new Persian channel, and is looking to expand its Mandarin output too. According to USAGM, the agency has editorial independence from the US government. In terms of foreign broadcasters operating within the US, since September 2018 and following the National Defense Authorization Act 2019, the Federal Communication Commission mandates foreign media outlets to provide reports disclosing any relationship to foreign principals, essentially putting them under the scope of the US Federal Agents Registration Act (FARA). Russian state-owned outlets RT and Sputnik, among others, had to register as foreign agents.

Federal and state-level legislation: The Honest Ads Act, introduced by US senators Amy Klobuchar, Mark Warner and John McCain, was the first legislative effort to regulate digital intermediaries, aiming to expand the remit of the Federal Election Campaign Act (FECA) to encompass paid digital ads, and require platforms to make sure disclaimers identified them as such, create a publicly accessible record of political advertising requests costing over $500, and ensure no foreign actors were able to purchase political ads. On 1 March 2019, the Honest Ads Act was included in an omnibus reform bill called the For the People Act (or H.R. 1). Even though H.R. 1 passed in the House on 8 March 2019, it’s unlikely to be scheduled for a vote in the Senate.

Regulating paid political ads is just one piece of the disinformation puzzle. It is promising that the bills on algorithmic accountability and tracking mentioned earlier started reflecting on the complexities of regulating digital intermediaries. The same can be said about a July 2018 white paper circulated by Senator Mark Warner.[102] Its proposals included modifying Section 230 of the Communications Decency Act that immunizes digital intermediaries from state tort and state criminal liability, bot labelling (the so-called ‘Blade Runner law’), examining the concept of an information fiduciary,[103] comprehensive data protection legislation, data transparency and portability bills, employment of ‘essential facility’ labels for market dominant companies and providing the Federal Trade Commission (FTC) with rulemaking authority.

There are increasing calls for more power to be given to the FTC, which fined Facebook $5 billion[104] after an investigation into whether it broke the 2011 consent decree, but given the technology company’s revenue, even that amount can be seen as merely the cost of doing business.[105] The investigation was launched following the Cambridge Analytica scandal that revealed the data of 87 million Facebook users were passed on to the third party. FTC’s new

[102] McCabe, D. (2018), ‘Scoop: 20 ways Democrats could crack down on Big Tech’, Axios, 30 July 2018, https://www.axios.com/mark-warner-google-facebook-regulation-policy-paper-023d4a52-2b25-4e44-a87c-945e73c637fa.html (accessed 6 Mar. 2019).

[103] For more on fiduciaries see Balkin, J. M. (2016), ‘Information Fiduciaries and the First Amendment’, *UC Davis Law Review*, 49:4, https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf (accessed 5 Aug. 2019).

[104] The FTC has also already imposed a $5.7 million fine on China’s TikTok for collecting personal data from children.

[105] Wong, J. C. (2019), ‘Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports’, *Guardian*, 12 July 2019, https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations (accessed 13 Jul. 2019).

order for Facebook to create new layers of oversight for handling of users' data may seem like a step in the right direction, but the settlement has been criticized for effectively allowing the company to decide for itself the extent of user privacy without any meaningful change to its structure and financial incentives, which constitute the root of the problem.[106] Additionally, the fact the settlement shielded Facebook in regard to unspecified violations has been strongly criticized,[107] as the broad immunity given to its executives, sets a dangerous precedent.

The FTC has also launched a Technology Task Force[108] dedicated to investigating competition in the technology sector[109] that also intends to review previous acquisitions. FTC Chair Joel Simon stated he would be open to breaking up Big Tech,[110] but Facebook's settlement leaves serious questions in regard to the agency's willingness to take drastic measures contravening dominant market players. Facebook's plans to merge with WhatsApp and Instagram, despite being promoted as a step towards enhanced privacy by CEO Mark Zuckerberg,[111] are viewed with scepticism by critics[112] and antitrust authorities on both sides of the Atlantic.[113] Certainly the suggestion Facebook could become the US equivalent of China's omnipresent WeChat is alarming.[114] Regulators should take action before Facebook moves forward with merging its three different services, to ensure due diligence in terms of users' personal data and the functionalities of the future unified interface.

Data governance has entered the debate in the US, too, with California passing the California Consumer Privacy Act (CCPA), a bill that according to former FTC Chief Technologist Ashkan Soltani, Facebook was supporting in public but lobbying against behind the scenes. CCPA passed into law in June 2018 but will not become enforceable until 1 January 2020. It draws on the General Data Protection Regulation (GDPR) and aims to give internet users more control of their data. Furthermore, in 2018, New York passed the Democracy Protection Act, California passed the Social Media Disclose Act (to take effect in 2020), and Maryland passed the Online Electioneering Transparency and Accountability Act. A federal court blocked the latter under the First Amendment but the law could be amended to alleviate some of the concerns raised. While

[106] Federal Trade Commission (2019), *Dissenting Statement of Commissioner Rohit Chopra*, 14 July 2019, https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf (accessed 21 Aug. 2019).

[107] Isaac, M. and Singer, N. (2019), 'Facebook agrees to extensive new oversight as part of $5bn settlement', *New York Times*, 24 July 2019, https://www.nytimes.com/2019/07/24/technology/ftc-facebook-privacy-data.html (accessed 13 Aug. 2019).

[108] Federal Trade Commission (2019), 'FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets', 26 February 2019, https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology (accessed 5 Aug. 2019).

[109] Shubber, K. and Stacey, K. (2019), 'New FTC task force to tackle competition in tech sector', *Financial Times*, 26 February 2019, https://www.ft.com/content/2801ced2-39f7-11e9-b856-5404d3811663 (accessed 8 Mar. 2019).

[110] McLaughlin, D. (2019), 'FTC chief says he's willing to break up big tech companies', *Bloomberg*, 13 August 2019, https://www.bloomberg.com/news/articles/2019-08-13/ftc-chief-says-willing-to-break-up-companies-amid-big-tech-probe (accessed 19 Aug. 2019).

[111] Zuckerberg, M. (2019), 'A Privacy-Focused Vision for Social Networking', 6 March 2019, https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634 (accessed 5 Aug. 2019).

[112] Kakaes, K. (2019), 'Zuckerberg's new privacy essay shows why Facebook needs to be broken up', MIT Technology Review, 7 March 2019, https://www.technologyreview.com/s/613084/zuckerbergs-new-privacy-essay-shows-why-facebook-needs-to-be-broken-up (accessed 7 Mar. 2019).

[113] Kottasová, I. (2019), 'Europe will fight Mark Zuckerberg's plans for Facebook', CNN, 7 March 2019, https://edition.cnn.com/2019/03/07/tech/facebook-whatsapp-europe/index.html (accessed 7 Mar. 2019).

[114] Liao, S. and Statt, N. (2019), 'Facebook wants to be WeChat', The Verge, 8 March 2019, https://www.theverge.com/2019/3/8/18256226/facebook-wechat-messaging-zuckerberg-strategy (accessed 14 Mar. 2019).

there is a lot of movement at state level,[115] a weaker federal privacy and data protection law that would pre-empt state-level victories should remain a concern. Technology companies may be advocating for federal level legislation they can still influence, only to override state-level laws.

> Targeted influence campaigns rely either on segmented audiences or individual profiles, and the latter is essentially the business model of data brokers.

In 2018, Vermont became the first US state to address another piece of the puzzle, particularly in regard to micro-targeted disinformation: the hyper-personalized influence campaigns that by virtue of operating at the granular level can evade detection by oversight bodies and watchdogs. Targeted influence campaigns rely either on segmented audiences or individual profiles, and the latter is essentially the business model of data brokers. Although in the EU various organizations and individuals have started taking on the data brokers,[116] in the US relevant steps are in their infancy. For example, the Vermont law on data brokers,[117] requires them to register as such, and mandates data security standards and the provision of information about an opt-out policy for customers, where available. However, the law does not apply to consumer-facing companies who are first-party data collectors such as websites apps or e-commerce platforms.[118] Frustratingly, it also does not require data brokers to disclose what information they collect or who is purchasing it.[119]

Civil society, academia and think-tanks in the US

The Data & Society Research Institute in New York, the Tow Center for Digital Journalism at Columbia University, the Berkman Klein Center and the Shorenstein Center (Information Disorder Lab) at Harvard, have all produced and continue to create broad-ranging research that tackles the issue of disinformation through reports, events or digital tool development.

The non-profit organizations Social Science Research Council and Social Science One have also partnered with Facebook to provide funding for independent research on 'the effects of social media on democracy and elections',[120] but the project also includes funding from seven non-profit foundations in an effort to counterbalance any financial influence from Facebook.

[115] New York also introduced the New York Privacy Act. See New York State Senate (2019), Senate Bill S5642, https://www.nysenate.gov/legislation/bills/2019/s5642 (accessed 1 Jul. 2019).

[116] Privacy International (2018), 'Why we've filed complaints against companies that most people have never heard of – and what needs to happen next', 8 November 2018, https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what (accessed 1 Jul. 2019)

[117] Coldewey, D. (2018), 'Vermont passes first law to crack down on data brokers', Tech Crunch, https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers (accessed 6 Mar. 2019).

[118] Ahmad, H. (2018), 'Analysis: Vermont's data broker regulation', The International Association of Privacy Professionals, 11 July 2018, https://iapp.org/news/a/analysis-vermonts-data-broker-regulation (accessed 7 Mar. 2019).

[119] Melendez, S. and Pasternack, A. (2019), 'Here are the data brokers quietly buying and selling your personal information', Fast Company, 2 March 2019, https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information (accessed 8 Mar. 2019).

[120] Social Science One (n.d.), Home page, https://socialscience.one.

Credibility Coalition is another broad researching community, supported by the Google News Initiative, the Facebook Journalism Project and Craig Newmark Philanthropies among others. Their aim is to create a comprehensive framework for the study of disinformation, define and validate efficient signals of content and source credibility.

Poynter's International Fact-Checking Network unit has created a global network of fact-checkers. It provides training and has created a code of principles that fact-checking teams from around the world can apply for accreditation.

Atlantic Council's Digital Forensics Research Laboratory, the Alliance for Securing Democracy[121] (affiliated with the German Marshall Fund), the GMF's Digital Innovation & Democracy Initiative, the Center for Strategic & International Studies, the Brookings Institution, New America, the National Democratic Institute, and the Design 4 Democracy Coalition, are all engaged in debates, reports and research on the issue of disinformation.

Further independent initiatives in the US

New Knowledge is an Austin-based private cybersecurity company specializing in disinformation that has testified in front of the SSCI and has produced a report on the influence of Russia's Internet Research Agency. However, the *New York Times* criticized its research methods when it revealed the firm's chief executive employed tactics similar to those conducting influence operations in the 2016 elections.[122] The company responded by explaining this action was taken for the purposes of an experiment, but the incident demonstrates the risks of employing techniques that could be construed as counter-propaganda. In the fight against disinformation integrity is paramount. State, civil society and private-sector actors in the EU and the US should also avoid replicating the methods of adversaries or they risk losing credibility.

NewsGuard is a start-up using 'nutrition labels' to classify reliable news sources according to nine criteria. Defying the prevailing drive towards automation, the company employs trained analysts and journalists who will review 7,500 sites that account for 98 per cent of US news consumption. It has also been rolled out in the UK, France, Germany, and Italy and is in talks with British ISPs about the potential of flagging up suspect news sites.

3.3 Action taken by digital intermediaries

This section focuses on key actions taken by Alphabet – the parent company of Google – Facebook, Twitter, and their subsidiaries as dominant players and influential normative powers in the current information ecosystem. With the exception of Pinterest, these companies have also signed up to the CoP.

[121] The Alliance created a tool to track Russian disinformation online, Hamilton 68.

[122] Rutenberg, J. (2019), 'Fake News as "Moral Imperative"? Democrats' Alabama Move Hints at Ugly 2020', *New York Times*, 12 January 2019, https://www.nytimes.com/2019/01/13/business/media/democrats-disinformation-election-interference.html (accessed 14 Mar. 2019).

Alphabet

Google

- **Fact-checking:** Google supports fact-checking initiatives such as First Draft[123] through its Google News Initiative.
- **Media literacy:** Although not ready for radical changes to their business model, digital intermediaries have pulled their weight in supporting the drive towards media literacy programmes. In the UK, for example, Google has funded NewsWise,[124] a free news literacy project for nine to 10-year-old children set up by the Guardian Foundation, the National Literacy Trust and the PSHE Association. The company has also supported media literacy programmes across the European continent, and in US high schools.
- **Policy changes:** Google also continues to demonetize sites with more ads than content (as some 'fake news' sites are).
- **Political advertising:** In August 2018 and ahead of the US midterms, Google launched the original version of its Ad Library, and in April 2019 its EU edition was released in preparation for the European elections. Since March 2019 the company required verification for purchasing political ads in Europe too.[125]
- **Supporting journalism:** Google provided training for European journalists and funded newsrooms through its Digital News Initiative. The company has signed up – along with Facebook and Bing – to The Trust Project, an international initiative that designed eight 'trust indicators' that can send machine-readable signals to news distribution platforms that will surface content and prioritize it as trustworthy. The project was incubated in the Markkula Center for Applied Ethics at Santa Clara University. It also supports the Journalism Trust Initiative (JTI) created by Reporters without Borders and joined by the European Broadcasting Union, Agence France-Presse and the Global Editors Network, which works to create machine-readable credentials for media outlets that relate to their ownership, journalistic methods and ethics. JTI has recently been joined by GDI and NewsGuard to coordinate their efforts.

YouTube

In February 2019, the Google subsidiary reported to the European Commission that since November 2018 it had removed one channel linked to Russia's Internet Research Agency and 34 YouTube channels linked to Iranian influence operations. Two new features promoting 'authoritative' sources were introduced – the Top News shelf in search and Breaking News on the homepage. The YouTube recommendation algorithm generates more than 70 per cent of the views.[126] After complaints its algorithm was surfacing many conspiracy videos, the company

[123] First Draft's CrossCheck and Comprova are two more fact-checking initiatives addressing disinformation.
[124] *Guardian* (2019), 'NewsWise evaluation report 2018–19', 18 July 2019, https://www.theguardian.com/newswise/2019/jul/18/newswise-evaluation-report-2018-19 (accessed 13 Aug. 2019).
[125] Google (2019), 'Verification for election advertising in the European Union (Jan 2019)', https://support.google.com/adspolicy/answer/9227372 (accessed 5 Aug. 2019).
[126] Guillaume Chaslot has researched and raised awareness about Google's recommendation algorithm. He is a former Google programmer who worked on YouTube's recommendation system and went on to fund algotransparency.org.

announced changes to deprioritize them.[127] It labels RT and Sputnik as affiliated with the Russian government,[128] and after disinformation campaigns against Hong Kong protesters led by China-backed media, it is under pressure to ban state-backed media ads replicating the example of Twitter.[129] YouTube has also announced it is going to roll out a new feature, an information panel appearing next to videos that relate to topics prone to disinformation.[130]

Jigsaw

Jigsaw is a technology incubator within Alphabet that attempts to find technological tools to tackle disinformation, hate speech and terrorist recruitment.

Issues for consideration: In regard to its CoP compliance and according to its second implementation report,[131] Google removed tens of thousands of ads in violation of its misrepresentation policies, but the percentage of those pertaining to disinformation campaigns remains unclear. That report listed the UK as having the most 'misrepresentation violations' followed by Estonia and Romania. It would be helpful for researchers to have access to adverts that violate Google policy to establish an informed view of the specific actors trying to pollute the information space. Lack of clarity in terms of Google's issue-based ad policy remains. Additionally, reports about the power of YouTube's algorithm to radicalize views via its recommendation system, proves companies' algorithmic systems need to be audited.[132]

Facebook

Facebook

- **Account takedowns:** Facebook also continues to remove accounts of disinformation networks fomenting dissent in various EU states, such as the UK or Romania, and the US.
- **De-ranking and content moderation:** One of Facebook's most important actions was its demotion of content flagged as potentially false by fact-checkers in its News Feed algorithm.[133] According to its CoP January 2019 report, this decreases views by more than 80 per cent. Facebook uses AI to identify clickbait articles and 'ad farms' and de-ranks them in its News Feed. Facebook also penalizes false headlines even when the copy is accurate,

[127] Dwoskin, E. (2019), 'YouTube is changing its algorithms to stop recommending conspiracies', *Washington Post*, 25 January 2019, https://www.washingtonpost.com/technology/2019/01/25/youtube-is-changing-its-algorithms-stop-recommending-conspiracies (accessed 28 Mar. 2019).

[128] In the UK, RT and Sputnik were found to perform 'damage control' for Russia following the Skripal poisoning, and employ disinformation or conspiracy theories to do so. See Ramsay, G. and Robertshaw, S. (2019), *Weaponising News: RT, Sputnik and targeted disinformation,* King's College, London, https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf.

[129] Alexander, J. (2019), 'YouTube pressured to ban Chinese state media ads that spread misinformation about protesters', *The Verge*, 21 August 2019, https://www.theverge.com/2019/8/21/20826568/youtube-cctv-hong-kong-china-ads-state-media-twitter-facebook (accessed 21 Aug. 2019).

[130] This feature is currently only available in the US and South Korea. See https://support.google.com/youtube/answer/9004474?hl=en-GB.

[131] European Commission (2019), 'First monthly intermediate results of the EU Code of Practice against disinformation', 28 February 2019, https://ec.europa.eu/digital-single-market/en/news/first-monthly-intermediate-results-eu-code-practice-against-disinformation.

[132] Fischer, M. and Taub, A. (2019), 'How YouTube radicalized Brazil', *New York Times*, 11 August 2019, https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html (accessed 19 Aug. 2019).

[133] For analysis of the US countermeasures to disinformation also see Legg, H. and Kerwin, J. (2018), *The Fight Against Disinformation in the U.S.: a Landscape Analysis*, Harvard Kennedy School: Shorenstein Center on Media, Politics and Public Policy, 1 November 2018, https://shorensteincenter.org/the-fight-against-disinformation-in-the-u-s-a-landscape-analysis (accessed 7 Mar. 2019).

by demoting the story.[134] Following the examples of Pinterest and YouTube, Facebook also downranked anti-vaccination pages and groups. The company uses machine-learning to prevent fake accounts from being created and, following a consultation period, it announced an Oversight Board. The latter has already attracted criticism,[135] not least because what the company is attempting to pursue is 'something like a constitution'[136] of unprecedented normative power. Despite its democracy-promoting rhetoric the sight of a corporation defiantly claiming powers that in democracies are bestowed to elected governments by their own people, might look like corporate overreach if not hubris. A one size-fits-all approach may be more financially desirable for Facebook but this level of centralization of the power to dictate what free speech effectively means across the world should alert governments, activists, journalists and citizens across the world.

- **Digital literacy:** As part of its efforts to enhance digital literacy, Facebook launched the Digital Literacy Library,[137] in consultation with the Berkman Klein Center for Internet & Society at Harvard, and has added a context button to help users assess the credibility of posts.

- **Policy changes:** Facebook's prohibition of coordinated inauthentic behaviour (CIB) seems in compliance with First Amendment considerations, as it is behaviour-based and 'content-agnostic', observing patterns of activity. The company continues to remove pages, groups and accounts displaying CIB,[138] and has removed hundreds related to Russia, Iran and Venezuela.[139] The CIB policy has also had unintended consequences such as the banning of activists who want to scale up their communications via coordination.[140] It also proved flawed as it failed to foresee operations such as those enabled by the aforementioned 'business manager' account feature.[141]

- **Political advertising:** Along with Google and Twitter, Facebook has forced political advertising to be marked as such and introduced user verification requirements for purchasing entities.[142] In 2018, Facebook launched its first Ad Archive in the US, followed by a pan-EU Ad Library in 2019, which includes political and issue-based advertising. Pages now provide information on the ads they are running, their name changes and, for pages with greater reach, the location of the administrators. Nevertheless, the system still has

[134] Funke, D. (2018), 'Facebook is now downranking stories with false headlines', Poynter, 25 October 2018, https://www.poynter.org/fact-checking/2018/facebook-is-now-downranking-stories-with-false-headlines (accessed 27 Mar. 2019).

[135] See Lomas, N. (2019), 'Facebook's content oversight board plan is raising more questions than it answers', Tech Crunch, June 2019, https://techcrunch.com/2019/06/28/facebooks-content-oversight-board-plan-is-raising-more-questions-than-it-answers (accessed 13 Jul. 2019).

[136] Facebook (2019), Oversight Board Consultation Report, p. 34.

[137] Facebook, Digital Literacy Library, https://www.facebook.com/safety/educators. The library has been translated into over 30 languages.

[138] Gleicher, N. (2019), 'Removing Coordinated Inauthentic Behavior from Iran, Russia, Macedonia and Kosovo', Facebook Newsroom, 26 March 2019, https://newsroom.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo (accessed 27 Mar. 2019).

[139] Wong, J. C. (2019), 'Facebook and Twitter removed hundreds of accounts linked to Iran, Russia and Venezuela', *Guardian*, 31 January 2019, https://www.theguardian.com/technology/2019/jan/31/facebook-and-twitter-removed-hundreds-of-accounts-linked-to-iran-russia-and-venezuela (accessed 13 Mar. 2019).

[140] Tynan, D. (2018), 'Facebook accused of censorship after hundreds of US political pages purged', *Guardian*, 16 October 2018, https://www.theguardian.com/technology/2018/oct/16/facebook-political-activism-pages-inauthentic-behavior-censorship (accessed 27 Mar. 2019).

[141] Waterson, J. (2019), 'Revealed: Johnson ally's firm secretly ran Facebook propaganda network', *Guardian*, 1 August 2019, https://www.theguardian.com/politics/2019/aug/01/revealed-johnson-allys-firm-secretly-ran-facebook-propaganda-network (accessed 19 Aug. 2019).

[142] For more analysis on industry responses also see Bradshaw, S., Taylor, E. and Walsh, S. (2018), *Industry Responses to the Malicious Use of Social Media*, Nato StratCom CoE, https://www.stratcomcoe.org/industry-responses-malicious-use-social-media (accessed 7 Mar. 2019).

blind spots. Apart from the name of the group sponsoring the ad, the actual identities of the individuals or the source of funds is difficult to track. Indicative examples of the problem include the pro-Brexit campaign by the once elusive Mainstream Network[143] – now revealed to be run by CTF affiliates – in the UK or Vice impersonating 100 US senators to buy ads before the midterms.[144] Ahead of the EU elections Facebook decided to ban cross-border advertising by authorized advertisers, a decision that created problems for pan-EU political groups and led to the Secretaries-General of the European Commission, the European Parliament and the Council of the European Union to protest it would have 'huge political and institutional consequences'.

Instagram

Facebook's Ad Library includes ads posted on Instagram. Users can now also flag fake content and AI tools are employed to spot misleading content.

WhatsApp

- **Funding research:** The subsidiary has committed funds through its Misinformation and Social Science Research Awards to researchers around the globe investigating issues of news credibility, variables influencing sharing habits, digital literacy, disinformation deployed in electoral contexts, virality and more.
- **Policy changes:** In a first effort to contain the disinformation problem parent company Facebook decided to limit WhatsApp's forwarding limit from 20 to five times, although the effectiveness of this measure is up for debate according to a study into disinformation in Nigeria funded by WhatsApp itself.[145]

> Growing criticism from fact-checking teams that have collaborated with Facebook are troubling.

Issues for consideration: Growing criticism from fact-checking teams that have collaborated with Facebook are troubling.[146] Even the announcement of fact-checking initiatives for Instagram has been received with scepticism.[147] Ad Library technical issues, a series of revelations that confound policymakers such as the 'business manager' account option, and a persistently evasive approach to meaningful public scrutiny, have created a substantial trust deficit.

[143] Volpicelli, G. (2018), 'How a suspicious Facebook page is pushing pro-Brexit ads to millions', Wired UK, 19 October 2018, https://www.wired.co.uk/article/brexit-facebook-ads-mainstream-chequers-89up-dcms (accessed 8 Mar. 2019).

[144] Turton, W. (2018), 'We posed as 100 Senators to run ads on Facebook. Facebook approved all of them', Vice, 30 October 2018, https://news.vice.com/en_ca/article/xw9n3q/we-posed-as-100-senators-to-run-ads-on-facebook-facebook-approved-all-of-them (accessed 14 Mar. 2019).

[145] The study showed that despite the changes, a member of five WhatsApp groups could still forward a message to 1,280 people with ease and speed. See Hitchen, J., Fisher, J., Cheeseman, N., and Hassan, I. (2019), 'How WhatsApp influenced Nigeria's recent election — and what it taught us about "fake news"', *Washington Post*, 15 February 2019, https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/15/its-nigerias-first-whatsapp-election-heres-what-were-learning-about-how-fake-news-spreads (accessed 5 May 2019).

[146] Owen, L. (2019), 'Full Fact has been fact-checking Facebook posts for six months. Here's what they think needs to change', 29 July 2019, https://www.niemanlab.org/2019/07/full-fact-has-been-fact-checking-facebook-posts-for-six-months-heres-what-they-think-needs-to-change (accessed 14 Aug. 2019).

[147] Harrison, S. (2019), 'Instagram now fact-checks, but who will do the checking', *Wired*, 16 August 2019, https://www.wired.com/story/instagram-fact-checks-who-will-do-checking (accessed 19 Aug. 2019).

Researchers have also pointed out that the company has been selective with the data it offers for research. Oversight has to stop being defined predominantly on Facebook's terms, especially since the company's actions to address issues relevant to disinformation, such as user privacy, tend to come too little, too late. A case in point is the promised and heavily promoted 'Clear History' tool, which was eventually rebranded as 'Off-Facebook Activity'. Instead of clearing anything meaningful, the tool disconnects the browsing data of third parties[148] from personal account profiles. Even if users decide to opt-out, their browsing history will remain on Facebook servers. There is also no mention of Facebook offering an opt out of targeting based on data it collects itself from its own platform. Additionally, since anonymized browsing histories can become part of aggregate data they can potentially still inform and refine the audience segmentation used to target ads anyway.

Mozilla

The company is engaged in civil society debates, signed up to the CoP, and announced a new anti-tracking policy that covers browser fingerprinting[149] and supercookies. In May, Mozilla also launched the Firefox EU Elections Toolkit to help EU voters recognize and avoid online manipulation.[150]

Pinterest

In view of the health risks, the social media company took the radical step of blocking anti-vaccination content, setting an example for other digital intermediaries.

Twitter

- **Removal of fake and violating accounts:** Twitter continues to investigate bots, fake accounts and suspend millions of them.[151] At the time of writing, the company investigates between 8.5 and 10 million accounts on a weekly basis. Another critical policy the company has implemented is the removal of accounts found to distribute hacked materials.
- **Political advertising:** Twitter has also produced a publicly accessible archive of potential foreign information operations for researchers. It now allows users to report fake accounts and has also launched its Ads Transparency Center, which has been expanded to EU political ads too. In preparation for the 2018 midterms, Twitter set up a cross-functional analytical

[148] Other apps and websites send data to Facebook using tools such as Facebook Pixel and Facebook Login. See more about the Off-Facebook Activity tool at https://newsroom.fb.com/news/2019/08/off-facebook-activity and https://engineering.fb.com/data-infrastructure/off-facebook-activity.

[149] Briz, N. (2018), 'This is Your Digital Fingerprint', Mozilla Blog, 26 July 2018, https://blog.mozilla.org/internetcitizen/2018/07/26/this-is-your-digital-fingerprint (accessed 14 Mar. 2019).

[150] Mozilla (2019), 'The Firefox EU Election Toolkit', https://www.mozilla.org/en-US/firefox/election.

[151] Dwoskin, E. and Timberg, C. (2018), 'Twitter is sweeping out fake accounts like never before, putting user growth at risk', *Washington Post*, 6 July 2018, https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk (accessed 7 Mar. 2019).

team tasked with detecting and responding to 'inauthentic, election-related coordinated activity'.[152] Mirroring Facebook, it now requires verification for the purchase of political ads. In line with the CoP, Twitter provided detailed insights.[153]

- **Funding research:** Twitter provides funding for research, including the Atlantic Council's Digital Forensic Research Lab and has also assisted European researchers by releasing information pertaining to information operations.[154] The company also provides funding to the EU DisinfoLab.

> Protecting citizens from disinformation is incumbent upon government authorities, as technology companies lack the expertise, foresight or willingness to identify the electoral or national security implications of gaps in their policies.

Issues for consideration: Despite Twitter's offer of data for analysis, researchers have been asking for more clarity in terms of how data sets are selected in the first place or information on which users viewed disinformation campaigns.[155] The targeting information users have access to – through the Why Am I Seeing this Ad? feature – needs to be more granular in order to be informative. Following the purchase of disinformation ads by China's state-backed media outlet Xinhua News to attack Hong Kong protesters,[156] Twitter announced its ban of state-controlled media outlets purchasing ads. Nevertheless, the incident highlighted the fact that protecting citizens from disinformation is incumbent upon government authorities, as technology companies lack the expertise, foresight or willingness to identify the electoral or national security implications of gaps in their policies.

3.4 Global efforts and best practices

Australia: In terms of research, the final report of the Australian Competition & Consumer Commission's Digital Platforms Inquiry,[157] with its broad scope, covering digital intermediaries' market power, digital advertising, journalism, consumer welfare and new technologies constitutes a comprehensive analysis of the elephant in the disinformation room: Big Tech's business models. Australia also launched its own version of FARA, its Foreign Influence

[152] Twitter (2019), *Retrospective Review Twitter, Inc. and the 2018 Midterm Elections in the United States*, 4 February 2019, https://blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf.
[153] Twitter (n.d.), 'How Twitter Ads Work', https://business.twitter.com/en/help/troubleshooting/how-twitter-ads-work.html.
[154] Gadde, V. and Roth, Y. (2018), 'Enabling further research of information operations on Twitter', Twitter blog, 17 October 2018, https://blog.twitter.com/official/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html.
[155] Harrison, S. (2019), 'Twitter's disinformation data dumps are helpful — to a point', *Wired*, 7 July 2019, https://www.wired.com/story/twitters-disinformation-data-dumps-helpful (accessed 19 Aug. 2019).
[156] Lakshmanan, R. (2019), 'China is paying Twitter to publish propaganda against Hong Kong protesters', *The Next Web*, https://thenextweb.com/twitter/2019/08/19/china-is-paying-twitter-to-publish-propaganda-against-hong-kong-protesters (accessed 19 Aug. 2019).
[157] Australian Competition & Consumer Commission (2018), *Digital Platforms Inquiry: Final Report*, June 2019, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf (accessed 13 Aug. 2019).

Transparency Scheme where companies with foreign principals are called to sign up to a publicly available Transparency Register.[158]

The Indian Centre for Internet & Society: The non-profit has offices in Bengaluru and Dehli and is conducting interdisciplinary research on digital technologies and their impact on societies, as well as the different facets of disinformation, such as data governance issues, political ads, user perceptions in the digital realm and more.

The Partnership on AI: The international consortium[159] is looking into disinformation as part of its AI and Media Projects. More specifically, it is investigating how to leverage AI to create disinformation alert and detection coordination mechanisms, authentication layers for branded news and a clear disinformation taxonomy among others.

[158] Australian Government Attorney-General's Department (n.d.), 'Transparency Register', https://transparency.ag.gov.au (accessed 5 Aug. 2019).

[159] The partnership was initially founded by Google, Amazon, Facebook, IBM and Microsoft, but now includes partners as diverse as Access Now, the BBC, ACLU, Baidu, Article 19 and Chatham House.

4. Existing Forums for Cooperation

Leadership engagement: The Transatlantic Commission on Election Integrity (TCEI), a non-governmental panel established in 2018 to contribute to the efforts against election interference, is a promising initiative attempting to mobilize policymakers and bridge political divides to protect democracy. Joe Biden is a co-chair of the group, which also includes former NATO secretary-general Anders Fogh Rasmussen and former US homeland security secretary Michael Chertoff. The group has called for US and European political candidates and parties to sign a pledge not to 'aid and abet' foreign election interference.[160] Calls for politicians to pledge not to use disinformation for domestic campaigns have also surfaced from US independent parties and politicians concerned that influence operations might become the 'new normal'.[161] The growing number of states affected by disinformation and the professionalization of political manipulation indicate their concerns are justified.[162]

Training ground: Another crucial forum for tackling disinformation is the Hybrid CoE in Helsinki, which operates as a hub of experts in the field and facilitates a dialogue between NATO allies and EU member states. Its work is practical, focusing on capacity-building through research, open source intelligence and countering election interference training sessions, and educational projects. In 2019, the Hybrid CoE is also hosting a workshop on legal resilience to disinformation.

Training, analysis and multi-stakeholder dialogue have also been at the core of the operations of the NATO-accredited StratCom Centre of Excellence in Riga, putting Latvia at the forefront of disinformation research and engagement.

Emergency mechanism: The EU Commission's Action Plan highlighted the need for the EU to work closely with NATO and the G7. During the Charlevoix Summit in June 2018[163] the G7 committed to establishing a Rapid Response Mechanism (RRM), tasked with defending democracies from foreign threats, by coordinating efforts in identifying, analysing, understanding and responding to those threats, with disinformation being one of the key issues identified.[164] Canada will be coordinating RRM on an ongoing basis to ensure continuity, its Coordination Unit will work closely alongside G7 presidencies, and following assessment

[160] Transatlantic Commission on Election Integrity (n.d.), *The Pledge for Election Integrity*, https://electionpledge.org (accessed 5 Aug. 2019).

[161] Hendrix, J. (2019), 'Can American political candidates help stop the flood of disinformation with a pledge?', Just Security, 31 January 2019, https://justsecurity.org/62432/american-political-candidates-stop-flood-disinformation-pledge (accessed 28 Mar. 2019).

[162] Cabato, R. and Mahtani, S. (2019), 'Why crafty Internet trolls in the Philippines may be coming to a website near you', *Washington Post*, 26 July 2019, https://www.washingtonpost.com/world/asia_pacific/why-crafty-internet-trolls-in-the-philippines-may-be-coming-to-a-website-near-you/2019/07/25/c5d42ee2-5c53-11e9-98d4-844088d135f2_story.html (accessed 14 Aug. 2019).

[163] G7 (2018), *Charlevoix Commitment on Defending Democracy from Foreign Threats*, June 2018, http://publications.gc.ca/collections/collection_2018/amc-gac/FR5-144-2018-30-eng.pdf (accessed 5 Aug. 2019).

[164] G7 (2018)*, Defending Democracy – Addressing Foreign Threats*, http://publications.gc.ca/collections/collection_2018/amc-gac/FR5-144-2018-7-eng.pdf (accessed 5 Aug. 2019).

procedures, decisions to implement specific actions will be at the discretion of national decision-making bodies. RRM's collaboration with the RAS will be coordinated through the EU Focal Point (EU's designated official).

Drawing on experience: NATO approaches disinformation through the lens of hybrid threats and has intensified its efforts to address them, especially after Russia's annexation of Crimea and the disinformation strategy it employed in Ukraine. Following its 'Enhanced Forward Presence' posture in Baltic States and Poland and in order to protect those deployments from disinformation NATO set up a system of social and legacy media monitoring. According to Piers Cazalet, deputy spokesperson at NATO, the organization's strategy of monitoring, verifying and responding directly from senior level to disinformation has been effective. For instance, claims by the Russian embassy in the UK, in November 2018, of NATO aggression at Russian borders were addressed head on by NATO spokeswoman Oana Lungescu, and the number of the debunks far exceeded the disinformation the embassy was pushing online.[165] At the same time, strategic silence is being deployed when a story does not get traction. Cazalet noted the organization tries to avoid the pitfall of wasting resources and instead tries to maintain them for proactive strategic communications: 'There is a point to be made about the use of disinformation to try to distract and divert resource from your opponent.' NATO has also committed to working with the EU on hybrid threats.

[165] EU vs Disinfo (2018), '"Funeral Teams for NATO Soldiers" – a Week of Disinformation Scare-Mongering, Exaggeration and Mockery', 8 November 2018, http://euvsdisinfo.eu/funeral-teams-for-nato-soldiers-a-week-of-disinformation-scare-mongering-exaggeration-and-mockery (accessed 5 May 2019).

5. EU and US Cooperation: Opportunities and Challenges

Rising political polarization, allegations of subverting democratic processes and an increasingly aggressive far-right that uses online platforms – both legacy and digital – to amplify its message, have demonstrated the impact of technology and social media companies' structures. Policymakers on both sides of the Atlantic are still grappling with their technical complexities, network dynamics, social nuances and political implications. This lack of deep understanding of technology's affordances, the market dynamics of the new information space and the absence of a robust international framework to address this global issue, render democratic states vulnerable to the insidious influence of disinformation campaigns threatening to upend norms, the rule of law, institutions and social trust.

Extrapolating legal scholar Lawrence Lessig's assertion about the internet's architecture, digital intermediaries could fill the role of 'a kind sovereign governing the community that lives in that space'.[166] This would mean that leaving such an online community would entail high exit costs due to the social capital users develop within it. Digital platforms are political actors in their own right, which mould 'the global infrastructure of free expression'.[167]

Democratic governments – not corporate tech actors – have a positive duty to protect the rights of the citizens that elect them. To overcome the disinformation issue and its manifold externalities it is necessary to meaningfully interrogate the underlying infrastructure and the business models that enable the rise of disinformation. The current information and power asymmetry has to be addressed decisively. After drip-feeding data sets to researchers and funding disinformation projects, tech companies are still being criticized for being conveniently selective in what they provide.

Despite the merits of self-regulation as an agile, short-term remedy that the EU's CoP embraced, pre-emptive self-regulatory pledges should not be seen as an alternative to statutory regulation. In the current information market, digital intermediaries are lacking the incentives to self-regulate efficiently as that would place them at an economic disadvantage. If the tide is changing it is partly due to a series of scandals that relate to infringements of users' privacy or vulnerabilities for manipulation. The scale of digital intermediaries' reach and the opacity of their operations merit immediate public scrutiny.

The delicate balance between regulating content and distribution, demands the active engagement of a broad range of stakeholders including journalists, civil society, academia, politics, the legal profession and technology. Simply privatizing content moderation without

[166] Lessig, L (2006), *Code: Version 2.0*, New York: Basic Books, p. 293.

[167] Gorwa, R. (2019), 'What is platform governance?', *Information, Communication & Society*, p. 4, doi: 10.1080/1369118X.2019.1573914.

meaningful transparency and redress mechanisms can lead to censorship.[168] AI-powered moderation tools purported as a solution to disinformation should be also available for external audits, as they have proved either unreliable or subject to biases.

The EU and US diverge in terms of constitutional and human rights priorities – e.g. freedom of expression *vis*-à-*vis* privacy or surveillance and security – and the trade-offs they have settled with feed into their non-aligned approach to disinformation. Aggravating the complexity of coordinating regulatory efforts is the fact that the debate in the US revolves around freedom of expression and the framing of efforts to constrain the power of Big Tech as being anti-free market, when in the EU freedom of expression is a qualified right that has to be balanced with other rights such as privacy.[169] The EU sees regulation as mainly a systemic issue and seeks to address disinformation by looking across different domains, from tech regulation to privacy frameworks and information markets, while the US institutional approach indicates an interpretation as an agent problem and allocates responsibility to federal agencies to focus on manipulation campaigns of state actors like Russia, Iran or China. Nevertheless, investigations launched this year by US Congress committees and the FTC, indicate the tide may be changing and a window of opportunity for alignment may manifest.

> This paper suggests that EU and US policymakers should not get fixated on specific agents as such an approach would be counterproductive towards building resilience.

In any case, this paper suggests that EU and US policymakers should not get fixated on specific agents as such an approach would be counterproductive towards building resilience. Adversaries are learning from each other, and so should long-term allies like the EU and the US. US agencies tend to work with EU counterparts on a bilateral basis so there is obviously room for improvement by moving to more multi-stakeholder forums. GEC, as the main coordinator of US efforts could bring other US agencies into the fold, and the FTC would need to be involved too. Coordination is paramount and reactively addressing the problem is not enough.

EU and US cooperation in tackling disinformation should be grounded on common principles and awareness of common values. Apart from the disrupting and divisive impact of disinformation campaigns in the political debate, influence operations impinge on the autonomy of citizens themselves. Article 19 of the Universal Declaration of Human Rights (UDHR) that seeks to protect citizens' right to hold opinions without interference[170] can be used as an ethical

[168] See, The Internet Policy Observatory (n.d.), *The Santa Clara Principles on Transparency and Accountability of Content Moderation Practices*, http://globalnetpolicy.org/research/the-santa-clara-principles-on-transparency-and-accountability-of-content-moderation-practices (accessed 5 Aug. 2019).

[169] As evidenced by the renowned case of Google Spain v AEPD and Mario Costeja González that led to the 'right to be forgotten' ruling. https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (accessed 13 Jul. 2019).

[170] United Nations (n.d.), Universal Declaration of Human Rights, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf (accessed 5 Aug. 2019).

compass in the debate. Under the UN Guiding Principles on Business and Human Rights, business enterprises – including digital intermediaries – have a responsibility to respect human rights throughout their operations.[171]

It is only through an effective US and EU collaboration on the issue of regulatory reform and disinformation countermeasures that we can set meaningful baseline norms, avoid a regulatory patchwork, duplication of efforts and overcome jurisdiction conflicts. The US and the EU should also lead the effort of convergence in terms of data protection. Security and privacy are intertwined.

While in the EU data-driven disinformation campaigns have ignited debates about data governance, the US is slowly but surely joining in. Data is crucial in campaigning. According to Brendan Fischer, director of federal reform at Campaign Legal Center in the US, 'you have organizations that are supposed to be operating independently of candidates, sharing data with candidates which in many ways is more valuable than giving them money'.[172]

The two sides of the Atlantic do not share perfectly aligned positions on notions of privacy,[173] but the EU's GDPR displays normative power, with legal experts and policymakers in the US considering its merits. Nevertheless, establishing a balance between meaningful and comprehensive data subject rights on one hand, with a public and private surveillance infrastructure seen as vital to national security, will be extremely challenging.

> In the search for common ground, the US and the EU should use the existing human rights framework enshrined in international treaties as a basis for their efforts to tackle disinformation

US scholars have proposed another legal framework that could serve as common ground in order to hold digital intermediaries to account: their 'duty of care' in regards to their customers and a 'duty to deal', in regards to sustaining market competition.[174] The unwarranted data mining operations that social media companies have been engaged in, which eventually supercharged tailored disinformation campaigns, and the lock-in effects of their architecture are symptoms of market failure[175] – a side-effect of oligopolistic competition between leading technology companies.[176] Also, as noted earlier, the concept of duty of care if not appropriately redefined in the digital space, is bound to prove inefficient.

[171] United Nations Global Compact (2011), 'Guiding Principles on Business and Human Rights', https://www.unglobalcompact.org/library/2.
[172] Author phone interview with Brendan Fischer, director of federal reform at Campaign Legal Center in the US, 14 March 2019.
[173] In contrast to the EU, the US does not have comprehensive privacy legislation.
[174] Wheeler, T. (2018), *The Root of the Matter: Data and Duty*, Shorenstein Center, 1 November 2018, https://shorensteincenter.org/wp-content/uploads/2018/11/Root-of-the-Matter-Wheeler.pdf (accessed 13 Jul. 2019).
[175] Peacock, S. E. (2019), 'How web tracking changes user agency in the age of Big Data: the used user', *Big Data & Society*, July–December 2014, pp. 3–5.
[176] Dolata provides an excellent analysis of this. See Dolata, U. (2019), 'Working paper: Apple, Amazon, Google, Facebook, Microsoft: Market concentration – competition – innovation strategies', Research Contributions to Organizational Sociology and Innovation Studies, SOI Discussion Papers 2017-01, University of Stuttgart, Institute for Social Sciences, Department of Organizational Sociology and Innovation Studies.

In the search for common ground, the US and the EU should use the existing human rights framework enshrined in international treaties as a basis for their efforts to tackle disinformation. A closer examination is required to find out which rights are undermined by disinformation, and how they are effected. The current ambiguity in terms of the effectiveness of psychographically tailored, microtargeted disinformation is not conducive to create appropriate benchmarks in terms of regulation.

Policymakers need to coordinate their actions with an expansive research community already working on disinformation, to signpost its current and perspective vectors. Companies will need to provide all the data deemed necessary for robust evaluation of the scale and various manifestations of disinformation. While considering the privacy of their users, companies need to become more accommodating to the resource needs of researchers and oversight bodies. Any industry with such a record of irregularities would have already been closely scrutinized.

In terms of the actions of digital intermediaries, despite their cooperative efforts with independent journalists, legacy media and fact-checkers, one should not lose sight of the fact that in a time of dwindling digital ad revenue for news publishers, Google and Facebook in 2017 accounted for more than 80 per cent of the global digital ad spend, excluding China.[177] After years of struggling to adjust to the digital transition, legacy media are still not out of the woods and with Big Tech dominating such a huge portion of ad revenue, many outlets have been forced to seek alternatives such as renewed subscription models and donations.[178]

[177] See Garrahan, M. (2017), 'Google and Facebook dominance forecast to rise', *Financial Times*, 4 December 2017, https://www.ft.com/content/cf362186-d840-11e7-a039-c64b1c09b482 (accessed 7 Mar. 2019); Lacy, L. (2018), 'Amazon takes third in the latest digital ad rankings', 20 September 2018, Ad Week, https://www.adweek.com/programmatic/amazon-takes-third-in-the-latest-digital-ad-rankings (accessed 7 Mar. 2019).

[178] Fletcher, R., Kalogeropoulos, A., Newman, N. and Nielsen, R. K. (2018), *Digital News Report 2018*, Reuters Institute for the Study of Journalism, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/digital-news-report-2018.pdf (accessed 5 Aug. 2019).

6. Recommendations

Cooperation between the US and EU is paramount in tackling disinformation. Their collaboration should adopt a broad-based strategy that:

- **Sees the big picture:** Joint responses should be multipronged, coordinated, integrated, sustainable and their efficiency continuously evaluated as disinformation vectors and techniques evolve, adapt and migrate rapidly.
- **Forms a united front:** By engaging all relevant actors: electoral commissions, media regulators, competition authorities, journalists, civil society, human rights and communication experts, technologists and legislators.
- **Changes the narrative:** Technological innovation is not an end-in-itself, it should be seen as a tool, there to serve the needs of society not left to uncritically define how the latter operates. As a tool it can assist in tackling disinformation.
- **Learns to learn:** The Fourth Industrial Revolution is upon us and it demands upskilling and training at all levels, all the way to the executives and heads of state, so key decision-makers are in a position to deal with externalities such as vulnerabilities in the information space.

Recommendations for the EU Delegation in the US

The EU Delegation in Washington is uniquely placed to facilitate coordination between the EU and the US in their efforts to tackle disinformation. An immediate action could be convening a day-long workshop where the European Commission would share best practices following the May 2019 elections and liaise with US counterparts to discuss how to improve and expand the CoP, consider its adaptation in the US environment, refine its goals and build in an effective monitoring mechanism able to impose sanctions to transgressors. Even though the final report on the CoP implementation will not be produced before the end of 2019, with the next US presidential election coming up in 2020, US counterparts would profit from the Commission's experience in tackling the distorting effects of disinformation ahead of elections.

The EU Delegation can serve as a conduit between the internal network on disinformation established within the Commission and US counterparts. It should also have a presence at the next Digital Assembly co-organized by the European Commission and the Presidency of the Council of the European Union, as well as its future incarnations. The EU Delegation should establish a working group, bridging the two sides of the Atlantic and linking their long-term strategies in terms of protecting democratic processes from disinformation coming both from within and without. The working group should aim to reduce disinformation based on an agreed set of principles and set out the institutional capacity necessary to facilitate future closer cooperation.

Recommendations for EU–US cooperation

Both the US and the EU are members of G7's RRM, as such the two allies should take the lead and build on the mechanism's analysis and work towards creating a multi-stakeholder forum that brings together professionals from different disciplines, from both the private and the public sector. More broadly, working with Hybrid CoE and the TCEI, the EU Delegation can assist the coordination of global efforts, led by the EU and the US. What follows is a series of recommendations that both the EU and the US could follow.

Common short-term recommendations

Regulate digital intermediaries and broaden oversight

Despite authorities' understandable wariness of reversing mergers[179] and acquisitions, they should examine all possible options, including imposing a moratorium on political microtargeting[180] and multivariate political ad testing, auditing their business models and algorithmic systems, or even breaking up Big Tech.[181] The latter option was aired in the European Parliament in regards to Google,[182] and even though the US has been predominantly averse to interventions of this scale, the FTC's statements may be pointing to a change of direction.

Still, momentum for the break-up of Big Tech is not likely to build in the home country of these companies so EU partners should take the lead in reformulating the debate based on a robust evidence base and in a way that could alleviate the political burden from US counterparts. A reorientation of the concept of monopolies in a market increasingly controlled by 'data power' is needed.[183] While big technology companies continue to diversify and expand into new markets, a first step could be restricting the markets they can actually enter,[184] at least until meaningful oversight of their current operations is in place.

Oversight should be broader than just covering Big Tech, to include increasingly popular platforms such as Instagram,[185] Reddit,[186] Telegram, and messaging apps in general in order to pre-empt the vulnerabilities created by the upcoming shift in disinformation dissemination.

[179] Any future reforms should ensure authorities can become informed about mergers in a timely manner, which allows for scrutiny a priori. Article 21 of the EU Merger Regulation allows the blocking of certain mergers to protect legitimate interests, such as media plurality.

[180] The UK's Institute Practitioners in Advertising (IPA) has also called for a ban in April 2018.

[181] See Warren, E. (2019), 'Here's how we can break up Big Tech', Medium, 8 March 2019, https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c (accessed 5 Aug. 2019); Finley, K. (2019), 'Legal Scholar Tim Wu says the US must enforce antitrust laws', Wired, 11 March 2019, https://www.wired.com/story/tim-wu-says-us-must-enforce-antitrust-laws (accessed 21 Aug. 2019); Lynn, B. and Stoller, M. (2018), 'Facebook must be restructured. The FTC should take these nine steps now', *Guardian*, 22 March 2018, https://www.theguardian.com/commentisfree/2018/mar/22/restructure-facebook-ftc-regulate-9-steps-now (accessed 15 Jul. 2019).

[182] Ahmed, M., Barker, A., and Mance, H. (2014), 'Google break-up plan emerges from Brussels', *Financial Times*, 21 November 2014, https://www.ft.com/content/617568ea-71a1-11e4-9048-00144feabdc0 (accessed 15 Jul. 2019).

[183] For an analysis of 'data power', see Lynskey, O. (2019), 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy', *Theoretical inquiries in Law*, 20: 1, pp. 189–220.

[184] Waters, R. (2019), 'Three ways that Big Tech could be broken up', *Financial Times*, 7 June 2019, https://www.ft.com/content/cb8b707c-88ca-11e9-a028-86cea8523dc2 (accessed 13 Jul. 2019).

[185] Instagram's user base nearly doubled in the last two years and it has also become a valuable tool for US politicians. See Murphy, H. and Sevastopulo, D. (2019), 'Why US politicians are turning to Instagram ahead of 2020 election', *Financial Times*, 22 February 2019, https://www.ft.com/content/737d2428-2fdf-11e9-ba00-0251022932c8 (accessed 15 Jul. 2019).

[186] Lytvynenko, J. and Silverman, C. (2019), 'Reddit has become a battleground of alleged Chinese trolls', Buzzfeed, 14 March 2019, https://www.buzzfeednews.com/article/craigsilverman/reddit-coordinated-chinese-propaganda-trolls (accessed 14 Mar. 2019).

Any future regulators should incorporate resilient monitoring workflows for newcomers in the digital information space too. The practices of global non-US or EU companies such as WeChat, Weibo and TikTok should also be monitored.

Internet Service Providers (ISPs) and big telecom companies should be included in any regulatory overhaul, if not to re-examine liability, to re-evaluate their responsibilities in terms of protecting users' data that can leave them exposed to disinformation campaigns. For example, in the US, Comcast provided data to NBC for its audience targeting platform and after the 2017 repeal of the FCC's Broadband Consumer Privacy Rules in the US, ISPs are allowed to sell consumers' information without consent.[187] In March 2019, the FTC launched an inquiry into the privacy practices of ISPs, indicating the US has started taking notice.[188]

Urgent research into sociotechnical systems

Evidence-based research is the priority before moving on with statutory regulation, so policymakers can ascertain the real impact of disinformation in the EU and the US based on real data and testimonies. Regrettably, clear and verifiable links between cause and effect are still lacking in disinformation research. The effectiveness of present approaches such as prioritizing transparency have to be properly audited, too, as without appropriate oversight and enforcement mechanisms, transparency can become a red herring.

Create state-level technology and digital intermediary regulators

New state regulators should be tasked with monitoring market penetration, conduct human rights audits of terms of service, platform structure and interactivity, content moderation updates, and technological adoption more broadly. Regulators should employ research, standardize the format of transparency reports and processes, and adopt a speculative outlook. They should launch inquiries into ad tech operations[189] and development, tracking[190] across platforms and devices, Big Tech and data broker profiling, as well as into private strategic communication companies. Regulators should also have oversight of new technological tools created to tackle problems that arise, and be able to access removed illegal content. State regulators should have a platform to convene on a regular basis, to exchange best practices and advise on federal or EU-wide policy.

Establish safeguards against conflicts of interest and regulatory capture

Protect policymaking processes by refining conflict of interest disclosure policies, being vigilant in terms of assembling stakeholders that can advance the public interest, and drawing on expertise that is verifiably independent from vested interests. Ensure balanced representation

[187] Fung, B. (2017), 'Trump has signed repeal of the FCC privacy rules. Here's what happens next', *Washington Post*, 4 April 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next (accessed 11 Jul. 2019).

[188] US Federal Trade Commission (2019), 'FTC Seeks to Examine the Privacy Practices of Broadband Providers', https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers (accessed 11 Jul. 2019).

[189] Ryan, J. (2018), *Behavioural Advertising and Personal Data*, Brave, 5 September 2018, https://brave.com/Behavioural-advertising-and-personal-data.pdf (accessed 5 Aug. 2019).

[190] For a case in point see, Schmidt, D. (2018), *Google Data Collection*, Digital Content Next, August 2018, https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research (accessed 5 Aug. 2019).

in decision-making forums that includes small and often under-represented stakeholders,[191] and avoid regulatory capture by digital intermediaries or other actors. There should not be a 'revolving door' between policymaking and highly paid tech jobs. Capture of policymakers or other stakeholders can take various forms, from campaign contributions[192] and lobbying[193] to the long-term establishment of structural or financial dependencies.[194]

Avoid rushed regulation

Adaptive principles and evidence-based regulation is appropriate for the fast-moving technology sector. Evaluate whether existing regulatory frameworks can be extrapolated to the digital intermediaries or new ones need to be created. Regulation should start with distribution, not content. Digital intermediaries may prefer regulation of the latter, as the former is the key driver of engagement, which is precisely what they monetize at scale, but a focus on regulating distribution and therefore, amplification, would alleviate freedom of expression concerns. New regulatory frameworks should not be exploited to suppress political dissidents, journalists or freedom of expression. Appeal and recourse mechanisms for intermediary or regulatory overreach should be put in place.

Support media plurality, public-service journalism and address media reform

Media pluralism[195] is important in avoiding the 'propaganda feedback loop'.[196] Legacy media's code of practice and journalistic codes of ethics should be updated so actors that have proved to disseminate disinformation or misinformed claims should eventually lose the credibility and amplification that legacy media provide. Media ownership has to be transparent across the board and media plurality preserved from the negative externalities of mergers. On the journalism front, impartiality should not be conflated with an uncritical provision of a platform to false claims and repeated disinformation offenders. Balanced reporting does not mean a free-for-all. In a highly polarized or polluted information environment, strategic silence needs to be selectively employed by journalists[197] and editors based on the public interest, independently of online engagement metrics and ratings. Participants in debates need to be selected on the basis of their credibility and demonstrable commitment to informed, evidence-based dialogue advancing democratic values, not their entertainment value. Media reform that includes

[191] Big Tech tends to dominate multi-stakeholder deliberations with smaller start-ups and companies often excluded.

[192] For a look at Big Tech contributions to US candidates visit https://www.opensecrets.org.

[193] The amount of money invested in EU and US lobbying by the tech giants is staggering. See for example, Richter, F. (2019), 'The Companies Spending the Most on EU Lobbying', Statista, 29 April 2019, https://www.statista.com/chart/17837/companies-spending-the-most-on-eu-lobbying.

[194] For structural dependencies between Big Tech and legacy media for example see Nechushtai, E. (2018), 'Could digital platforms capture the media through infrastructure?', *Journalism* 19 (8), pp. 1043–1058.

[195] The Florence based Media Pluralism Monitor (co-founded by the EU) tasked with identifying vulnerabilities among EU member states, reported in 2017 that risks for media pluralism are increasing.

[196] Benkler, Faris and Roberts (2018), *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*.

[197] Two prominent researchers of digital communication and sociotechnical systems advocated as much: Boyd, D. and Donovan, J. (2018), 'The case for quarantining extremist ideas', https://www.theguardian.com/commentisfree/2018/jun/01/extremist-ideas-media-coverage-kkk (accessed 19 May 2019).

updating national regulators, competition law and oversight mechanisms, should be examined in cooperation with competition authorities, civil society[198] and journalists. Local journalism should be properly funded.[199]

Move data governance to the centre of the debate

This debate is even more urgent with international tech companies expanding in new markets. For instance, in October 2018, in the US new downloads for Chinese ByteDance's TikTok app surpassed those of Facebook, Instagram, YouTube and Snapchat.[200] China is also chairing the International Telecommunication Union (ITU) until 2022, enhancing its leverage in setting global internet standards. The US and the EU have to strike a really difficult balance between protecting (if not enhancing) citizens' data privacy on one hand and adopting innovation enabling policies on the other. The Big Data & Digital Clearinghouse[201] established by the European Data Protection Supervisor indicates the EU is taking a multi-stakeholder approach. GDPR, although not perfect,[202] has raised EU public awareness of the importance of personal data protections. The G20 Osaka Leaders' Declaration also highlighted the important link between data and trust.[203]

Common long-term recommendations

Reform political campaigning and electoral law

Both the US and EU member states should conduct reviews of the ethics of political campaigning, what is legitimate and illegitimate influence, and lobbying reform to avoid state capture by Big Tech. Digital intermediaries have already advised political campaigns.[204] Investigation of the links between domestic actors and agents of foreign influence needs to be conducted. Statements from politicians could be fact-checked as well to improve the level of political discourse and reinstate trust.[205]

[198] The Media Reform Coalition has been doing extensive research on that front, https://mediareform.org.uk.

[199] The Cairncross Review in the UK, also recommended as much, via the Local Reporting Service, under the management of a proposed new body, the Institute for Public Interest News.

[200] Perez, S. (2018), 'TikTok surpassed Facebook, Instagram, Snapchat & YouTube in downloads last month', Tech Crunch, November 2018, https://techcrunch.com/2018/11/02/tiktok-surpassed-facebook-instagram-snapchat-youtube-in-downloads-last-month (accessed 13 Mar. 2019).

[201] European Data Protection Supervisor (n.d.)*, Big Data & Clearinghouse*, https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en (accessed 5 Aug. 2019).

[202] As demonstrated by the fact that four days after GDPR came into force some US publishers struggled to comply and cut off access from European readers altogether, while Romania was also criticized for attempting to use GDPR to force investigative journalists to reveal sources. Issues like browser 'tracking walls' that do not provide an opt-out persist. For more see Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C. and Helberger, N. (2017), 'Tracking Walls, Take-It- Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', *European Data Protection Law Review*, 3(3), pp353- 368. https://doi.org/10.21552/edpl/2017/3/9.

[203] G20 (2019), G20 Osaka Leaders' Declaration, https://g20.org/en/documents/final_g20_osaka_leaders_declaration.html (accessed 11 Jul. 2019).

[204] Mcgregor, S. and Kreiss, D. (2018), 'Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle', *Political Communication*, 35:2.

[205] UK's Full Fact has done real-time fact-checking of PMQs using custom-made tool Live. Using machine learning it has also created Trends, a tool allowing fact-checkers to monitor live propaganda and disinformation.

Invest in political security resilience

Disenfranchisement renders citizens more vulnerable to manipulation, so both US and EU states should put political engagement at the forefront of their efforts. Data and AI should be employed to meaningfully inform and engage with citizens,[206] by using Natural Language Processing for example to translate and coordinate debate across different countries and quickly process ideas, similar to the way that CitizenLab did with the Youth4Climate movement.[207]

Tailor-made media and digital literacy programmes

Each digital literacy initiative will demand clearly defined objectives grounded on thoroughly researched conclusions about the information individuals need to make informed decisions in regard to both legacy and digital media. Individuals of different age, background, and nationality may need a different set of skills as well as a different training approach,[208] which is why a national and context-specific approach to the issue is more appropriate.

Digital literacy programmes should target not just young students but all age groups, as well as politicians themselves. Initiatives should also entail enhancing public and policymakers' awareness of how data is collected, processed and managed, as well as the affordances and even false promises of emerging technologies such AI, deepfakes, 'neuropolitical' consulting,[209] and others. Following the example of Big Tobacco companies being ordered to pay for anti-smoking advertising, some suggested a similar model can be applied to the digital domain, by compelling tech giants to raise awareness and invest substantially into digital literacy programmes.[210]

Embrace technological innovation as a tool not a goal

Apart from its deployment in spotting disinformation campaigns, AI can facilitate the rapid exchange of information between the US and the EU, as well as international stakeholders. The US and the EU should invest resources in research into how emerging technologies can empower citizens and democracies. Governmental departments across the board should appoint AI experts to advise on how emerging technologies can enhance institutional capacity and contribute to societal resilience.

Convene an International Digital Assembly

The Tech Accord[211] and the Digital Peace Campaign[212] focus on cybersecurity but the call for global engagement in terms of setting up cyber norms relates to the issue of disinformation too. The health of democratic discourse depends on it. The US and the EU could bridge the

[206] The European Parliament's resolution on a comprehensive European policy on artificial intelligence highlighted this point too. See European Parliament (2019), *A comprehensive European industrial policy on artificial intelligence and robotics*, 12 February 2019, http://europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0081+0+DOC+XML+V0//EN&language=EN (accessed 5 Aug. 2019).

[207] Cuau, C. (2019), 'Applying artificial intelligence to citizen participation: the Youth4Climate case study', CitizenLab, https://www.citizenlab.co/blog/civic-engagement/youth-for-climate-case-study (accessed 12 Jul. 2019).

[208] DROG, a Dutch platform created by a team of academics and media experts gamified educational sessions on 'fake news' for example: https://aboutbadnews.com.

[209] Svoboda, E. (2018), 'The "neuropolitics" consultants who hack voters' brains', MIT Technology Review, 16 August 2018, https://www.technologyreview.com/s/611808/the-neuropolitics-consultants-who-hack-voters-brains (accessed 14. Mar 2019).

[210] Recommendation suggested during one of the EU–US Young Leaders Seminar break-out sessions.

[211] Cyber Tech Accord, https://cybertechaccord.org.

[212] Digital Peace Now, https://digitalpeace.microsoft.com.

work of Hybrid CoE, RRM, TCEI, the Internet Governance Forum (IGF) and the High-Level Panel on Digital Cooperation. As the latter stated, the current digital cooperation architecture is complex but not necessarily efficient. The panel's suggestion of the 'IGF Plus' model[213] for cooperation merits further attention. In the context of the ITU, the US and the EU should take the lead in establishing a long-term, open, international and interdisciplinary forum where developers, civil society, journalists, researchers, and policymakers can develop a code of ethics in terms of tech development[214] and harness the affordances of technological innovation to support and promote democracy. Evidently, the work of the UN's Group of Governmental Experts[215] and the Open-Ended Working Group[216] on cyber norms should also inform the EU–US cooperation on the issue of disinformation. The two allies should lead in setting a roadmap with the ITU towards convening an International Digital Assembly that would address the really pressing issues of international digital governance, such as information pollution, manipulation, and data governance. The cooperation frameworks recommended by the High-Level Panel on Digital Cooperation, which the ITU committed to refine, could be used in this process.

[213] UN Secretary-General's High-level Panel on Digital Cooperation (2019), *The Age of Digital Interdependence*, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf (accessed 21 Aug. 2019).
[214] OpenAI decided to initially withhold and subsequently release a constrained version of the GPT-2 text-generating AI system to the public, for fears of exacerbating the disinformation problem for example.
[215] Notably, in 2015, the first incarnation of the GGE agreed that the UN Charter and respect for human rights and freedom of expression apply to cyberspace, but in 2017 talks broke down. The General Assembly's first committee adopted the two separate resolutions on the actions of states in cyberspace in November 2018.
[216] OEWG's December 2018 resolution indicated 'false or distorted news' and 'hostile propaganda' are likely to be discussed. The deliberations of the two UN groups are bound to have long-term consequences for the free flow of information online, cyber sovereignty and freedom of expression. A useful timeline of OEWG and GGE processes can be found here: http://unidir.org/files/medias/pdfs/overview-of-the-group-of-governmental-experts-and-open-ended-working-group-processes-eng-0-786.pdf.

7. Conclusion

The US is home to 15 of the world's 20 most valuable tech firms, but as *The Economist* suggested,[217] Europe's weaker representation in the Big Tech league may be one of its main advantages, as it allows it to take a more objective stance in regulation. Disinformation poses a threat to democracies on both sides of the Atlantic. For far too long digital intermediaries' behaviour has displayed the traits of absentee ownership, a disengagement characteristic of monopolistic enterprises that operate far removed from distant communities around the world that have to bear the brunt of their externalities. That's why it is incumbent upon the EU and the US as allies representing democratic values and possessing the technological expertise, to join forces and lead the debate. There is nothing inevitable about the current course.

[217] *The Economist* (2019), 'Why big tech should fear Europe', 23 March 2019, https://www.economist.com/leaders/2019/03/23/why-big-tech-should-fear-europe (accessed 28 Mar. 2019).

About the Author

Sophia Ignatidou is an Academy Stavros Niarchos Foundation Fellow at the International Security Department of Chatham House. She researches artificial intelligence, disinformation, political campaigning, propaganda and surveillance. Before joining Chatham House in 2018, she worked as a freelance journalist and sub-editor for the *Guardian*, *The Sunday Times* and CNN, among others. Sophia holds an MA in Journalism from Goldsmiths, University of London, as well as an MA/PGDip in International Studies and Diplomacy from the School of Oriental and African Studies.

Acknowledgments

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the author and can in no way be taken to reflect the views of the European Union.

Chatham House is part of a consortium, coordinated by B&S Europe, implementing the EU Policy & Outreach Partnership in the United States.

The author would like to thank Charlotte Altenhoener-Dion, Kamel Ajji, Jennifer Daskal, Anastasia Denisova, Brendan Fischer, Elliot Higgins, Erica Lutes, Raegan MacDonald, Alexios Mantzarlis, Martin Moore, Paul Nemitz, Nikos Sarris, Jon Steinberg, Tina Zournatzi, as well as US, EU and NATO officials who assisted in the production of this research paper with information on background or non-attributed comments.

Thanks are due to Peter Fatelnig, Timothy Rivera, Maria Belovas and the rest of the team at the EU Delegation in the US for their comments on earlier drafts of this paper, the two anonymous peer reviewers, as well as Dr Patricia Lewis, Calum Inverarity and colleagues at Chatham House and the International Security Department for their valuable assistance.

Independent thinking since 1920

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

ISBN 978 1 78413 357 3

This publication is printed on FSC-certified paper.

FSC

Typeset by Soapbox, www.soapbox.co.uk

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223