Centre for
Digital Wellbeing

International Regulation of Social Media

December 2021

Table of Contents

Introduction

The role of social media and the influence and power of big tech companies has increasingly come under public scrutiny. There is mounting evidence about the negative effects of social media on mental health and wellbeing, particularly among young people, as well as significant concern about the role of social media platforms in spreading disinformation and misinformation, undermining trust in institutions and threatening social cohesion.

In this context, there is a growing recognition of the need for effective regulation of social media platforms in order to ensure the development and use of this technology is human-centred. Global discussion have centred on how countries can protect their citizens from various online threats. At the time of writing, the Australian Government has recognised these challenges, establishing a parliamentary inquiry into social media and online safety, which will "examine the practices of these companies—and whether more needs to be done".[1] This inquiry is a welcome and important step in establishing an Australian regulatory framework that draws on international best practice and experience.

The purpose of this review is to identify what approaches other countries have taken to regulate social media platforms and understand the context in which those regulations have been implemented. In doing so, this paper will identify experiences that Australian policymakers can learn from and draw upon in developing Australia's regulatory framework. It will form the foundation of recommendations best suited to an Australian context.

About us

The Centre for Digital Wellbeing is a policy research centre focusing on social media's impact on mental health and wellbeing, safety and social cohesion in the Australian community. The Centre seeks to collate research and increase awareness within Australia's policy domain on the effects of social media and to provide advice to government on policy and regulatory responses, including international best practice. The Centre has an Advisory Council comprising a network of health, mental health, digital technology and social policy experts who inform the Centre's work direction and policy development.

[1] Australian Government, Prime Minister of Australia, *Parliamentary committee to put big tech under the microscope* (1 December 2021) https://www.pm.gov.au/media/parliamentary-committee-put-big-tech-under-microscope

Background

Social media has fundamentally shifted the way Australians maintain connections, consume content, and share information. In recent years, the number of Australians using social media has increased significantly. As of March 2019, over 17 million Australians aged over 14 years used Facebook, representing an increase of nearly 4.2 million users since 2015.[2] Other platforms such as Instagram, TikTok, WeChat, YouTube, Pinterest, and Twitter also experienced significant growth in that period.[3] Social media platforms have seen further increases in usage during the COVID-19 pandemic, with more than one in three Australians increasing their use of social networking apps following the introduction of COVID-19 restrictions.[4] While there are many benefits of digitisation, there is increasing evidence that social media, gaming, and excessive screen time can severely impact our mental health and wellbeing, heighten the risk of online abuse and harassment, deepen societal divisions, and challenge social cohesion.[5]

Despite social networking platforms providing age restrictions, more children are online than ever before. A recent U.S. study found that for children aged 10-12, 49% of parents report the use of social media in the first six months of 2021. For children aged 7-9, 32% of parents report their child using social media.[6] In the same survey, parents reported finding it challenging to monitor children's behaviour online.

The impact of social media on mental health, safety, and social cohesion

Social media can aid increase connectedness and social support and build skills appropriate for the digital age. However, increased use of social media also carries risks, especially for children and adolescents. Social media can be incredibly addictive, with platforms intentionally designed to maximise the time users spend on them, for example through the use of algorithms to display content users will find engaging based on previous behaviour online. Like gambling and gaming, users can become captivated and obsessed, spending more time than anticipated on the platforms.

Research on the impact of social media on mental health and wellbeing is far from conclusive. However, growing evidence indicates that social media leads to social

[2] Roy Morgan, 'Facebook on top but Instagram and Pinterest growing fastest' (17 May 2019) http://www.roymorgan.com/findings/7979-social-media-trends-march-2019-201905170731.
[3] Ibid.
[4] Australian Communications and Media Authority, 'COVID restrictions helped increase digital communication use for older Australians' (22 April 2021) https://www.acma.gov.au/articles/2021-04/covid-restrictions-helped-increase-digital-communication-use-older-australians.
[5] John A. Naslund, Ameya Bondre, John Torous, & Kelly A. Aschbrenner, 'Social Media and Mental Health: Benefits, Risks and Opportunities for Research and Practice' (2020) 5 *Journal of Technology in Behavioral Science,* 245-257; Elly Robinson, 'Parental involvement in preventing and responding to cyberbullying' (2013) 92 *Family Matters*, 68-76; Joshua A Tucker, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, & Brendan Nyhan 'Social Media, Political Polarization, and Political Disinformation: A review of the Scientific Literature' (2018) *SSRN*.
[6] Mott Poll Report. 'Sharing too soon? Children and social media apps' (2018) 39 (4) *C.S. Mott Children's Hospital University of Michigan.*

isolation, stress, depression, and anxiety. Specifically, adolescents are more vulnerable to the consequences of social media use.[7]

In recent years social media has also emerged as a mechanism to perpetrate abuse and harassment, including cyberbullying and the promotion of violence and self-harm, age-inappropriate content, and gender-based violence. Social media platforms have started responding to concerns raised by individuals and organisations, implementing measures such as artificial intelligence to identify and block fake accounts, and providing access to safety tools. However, these measures remain limited, and social media platforms' overall self-regulation is weak and ineffective.

Social media can also deepen divisions and challenge social cohesion, including through the spread of misinformation and disinformation and the creation of echo chambers. The platforms are built to encourage and optimise content that generates clicks and is shared.[8] It therefore preferences viral content that is more sensational and more emotive.[9] As disinformation often acts on emotive plays and sensational claims, the content created is more likely to go viral and be shared, hence making it more difficult to contain. Anti-vaccine misinformation during the pandemic is a recent example of how easily false content can spread and the damaging effects that can have.

Social media has become a place where incorrect information spreads quickly. It has changed our traditional consumption of news and information. Over 12.7 million Australians (60.8 per cent) now cite the Internet as their primary source of news, including nearly 7.9 million Australians (37.7 per cent) who nominate social media as their primary source.[10] Traditionally, centralised news has been perceived as vetted and curated information and facts. In contrast, the decentralisation of information on social media has led to an erosion of trust in information and institutions and reduces overall trust in vetted fact-based channels.[11]

Further, with the use of algorithms, social media platforms expose their users to similar content they have previously engaged in. This creates echo chambers, where users are repeatedly exposed to similar views and opinions with minimal exposure to opposing views about current affairs. Echo chambers can make people insular, less curious, and less open-minded towards different ideas, which can fuel animosity towards 'the other'. The spread of disinformation, misinformation, and inflammatory content can have severe consequences for social cohesion.

Additionally, social media has opened new opportunities for foreign actors to undermine Australia's institutions. Social media provides an easy and accessible avenue for

---

[7] Jenna Palermo Christofferson, 'How is Social Networking Sites Effecting Teen's Social and Emotional Development: A Systemic Review' (2016) *Social Work Master's Clinical Research Papers*.
[8] Claire Wardle and Hossein Derakhshan, Council of Europe Report, *Information Disorder: Toward an interdisciplinary framework for research and policy making* (2017) https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html
[9] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (June 2019) 342-3
[10] Roy Morgan. 'It's official: Internet is Australia's main source of news; TV remains most trusted', (21 August 2020), http://www.roymorgan.com/findings/8492-main-sources-news-trust-june-2020-202008170619.
[11] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (June 2019) Chapter 6.

malicious actors to interfere in the democratic process by communicating directly with citizens and spreading disinformation to erode social cohesion. To combat disinformation online, users must first learn to recognise false information online, highlighting the need for further education and awareness.

The need for a regulatory response

Governments around the world have in recent years begun considering what regulatory response is required to mitigate the negative effects of social media. At the same time as recognising the challenges posed by social media, it is also important to recognise its benefits including its capacity to facilitate connections and communications across borders and give voice to those who may have traditionally been excluded from public debate. Any regulation needs to ensure that these benefits are maintained.

This paper provides an overview of the different regulatory frameworks adopted internationally, with a view to informing Australian policymakers about current trends and debates and options for regulation in Australia.

Australian Regulatory Response

Australia's regulatory response to social media to date has primarily focused on cyberbullying, terrorist and extremist content, and the media marketplace. Less consideration has been given to impacts on mental health (specifically relating to children, teenagers, and vulnerable groups) and the platforms' addictive properties. Further, while there is growing awareness of social media's role in spreading misinformation and disinformation, particularly in the context of COVID-19, and the corresponding negative effects on social cohesion, there has been a limited policy response to date. Communications Minister Paul Fletcher recently suggested Australia's defamation laws needed to ensure social media companies faced the same rules as traditional media. Deputy Prime Minister Barnaby Joyce has stated it is "essential" the Government pushes tech companies to clamp down on misinformation, noting Australia should take the US's lead. Prime Minister Scott Morrison has echoed Joyce's sentiment, urging tech companies to take more responsibility for content published on their platforms.[12]

Responding to social media's threat to social cohesion and impact on mental health should be a policy priority of government. To date, Australia has taken a piecemeal and reactive approach to the regulation of harmful online practices.[13] A better coordinated and proactive approach across sectors is needed to ensure social media platforms are appropriately and adequately regulated in Australia to minimise their negative effects.

Cyberbullying and Online Content

The *Enhancing Online Safety Act 2015* (Cth) establishes a two-tiered scheme for social media services to remove cyberbullying material targeted towards Australian children in response to cyberbullying on social media platforms.[14] Tier 1 social media platforms, including Twitter, TikTok, and Snapchat, participate in the scheme voluntarily. If a complaint is made to these platforms about cyberbullying material and the material is not removed within a specific period (currently 48 hours), the eSafety Commissioner may issue a request to have the material removed from the service. The Minister of Communications declares Tier 2 social media services following a recommendation by the eSafety Commissioner. Facebook, Instagram, and YouTube have been declared to be Tier 2 social media services. Tier 2 social media services may be subject to civil penalties and legally binding notices if they do not comply with requests to remove cyberbullying material.

The *Online Safety Act 2021* (Cth) builds on the existing regulatory framework established in the *Enhancing Online Safety Act* and will take effect on 23 January 2022. The new Act

[12] Stephanie Bory,' Social media a 'coward's palace', says Prime Minister, as he promises more action to hold online abusers responsible', (7 October 2021), *ABC News* https://www.abc.net.au/news/2021-10-07/prime-minister-defends-dutton-twitter-defamation-action/100522002
[13] Katharine Gelber, ' A better way to regulate online hate speech: require social media companies to bear a duty of care to users' (14 July 2021), *The Conversation* https://theconversation.com/a-better-way-to-regulate-online-hate-speech-require-social-media-companies-to-bear-a-duty-of-care-to-users-163808
[14] *Enhancing Online Safety Act 2015*; eSafety Commissioner, *Working with social media,* Australian Government.https://www.esafety.gov.au/about-us/consultation-cooperation/working-with-social-media.

introduces additional compliance obligations, including an online content scheme for removing specific material and a complaints-based removal notice scheme. The reform broadens the scheme to capture harms occurring on services other than social media.[15] A new set of industry codes are expected to be developed within 12 months of Royal Assent to guide industry compliance with their new obligations and to promote the adoption of responsible processes for dealing with online content and safety issues. The desired approach would see the codes developed by industry and then reviewed and endorsed by the eSafety Commissioner. The Commissioner has the authority to impose industry-wide standards if the codes cannot be agreed or do not meet the desired safety outcomes.[16]

The eSafety Commissioner has released general guidelines on social media use for parents, children, and young people. There is no recommended time limit for screen time; instead, the guidelines identify warning signs, such as reduced personal hygiene or becoming withdrawn from friends and family, that suggest online activity is becoming problematic for children and young people.[17]

Extremist content

In response to the Christchurch terror attack on 15 March 2019 where the perpetrator live-streamed footage of the event on social media platforms, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth)[18] was passed, requiring Internet, content, and hosting providers to report abhorrent violent conduct occurring in Australia on their services to the Australian Federal Police.[19] Failure to report violent material may result in fines of up to $888,000 for corporations,[20] and failure to remove the material from their services may result in fines of up to $11.1 million or 10 per cent of annual turnover, whichever is higher.[21]

Australia also signed the Christchurch Call, a voluntary commitment from governments and online service-providers aimed at addressing terrorist and extremist content online, established by the New Zealand and French Governments.[22] Government signatories have committed to considering appropriate action to prevent the use of online services to disseminate terrorist and violent extremist content through actions such as the development of industry standards or voluntary frameworks, as well as regulatory or policy measures that are consistent with international human rights law and the principle of a free, open and secure internet. Online service providers have committed to

[15] *Online Safety Act 2021* (Cth)
[16] eSafety Commissioner, *Online Safety Act 2021 Factsheet,* Australian Government. https://www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf
[17] eSafety Commissioner, *Time online.* Australian Government. https://www.esafety.gov.au/parents/big-issues/time-online.
[18] Attorney-General's Department, *Abhorrent violent material.* Australian Government. https://www.ag.gov.au/crime/abhorrent-violent-material.
[19] *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, s474.33
[20] *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019,* s474.33
[21] *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019,* s474.34
[22] Christchurch Call, *The Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online,* (2019). https://www.christchurchcall.com/christchurch-call.pdf.

implementing measures to prevent the upload of this content, with the Christchurch Call supported by social media platforms including Facebook and Twitter.[23]

Media

Earlier this year, Australia introduced a mandatory code of conduct, the *News Media and Digital Platforms Mandatory Bargaining Code*,[24] to address bargaining power imbalances between digital platforms, such as Google and Facebook, and Australian news media businesses. The Code enables eligible news businesses to bargain individually or collectively with digital platforms over payment for the inclusion of news on their platforms. The Code established a negotiation framework for news businesses and digital platforms to reach binding agreements and provides for an independent arbiter to determine the remuneration if parties cannot reach an agreement. While the Code was supported by both major parties in the Australian Parliament,[25] it was met with significant opposition by Facebook and Google. In response to the development of the legislation, in February 2021 Facebook temporarily blocked Australian users from viewing and sharing news on its platform, even blocking information and government pages, including health and emergency services.[26] The draft legislation was amended (and subsequently passed in parliament in February 2021) to include a mediation period to allow digital platforms and news businesses to attempt to reach agreement before entering into arbitration, and to consider platforms' existing agreements with publishers before deciding on the application of the Code.[27]

Blocking illegal online services

The *Telecommunications Act 1997* (Cth) allows Australian Government agencies to block illegal online services.[28] Following a review, the Department of Communications and the Arts published guidelines in 2017 on the use of the provision that entails "good practice measures" to be followed, including obtaining authorisation before disrupting online services, and limiting disruptions to instances of serious offenses or national security threats.

---

[23] Christchurch Call, *The Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online,* (2019) https://www.christchurchcall.com/christchurch-call.pdf
[24] *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021*
[25] Lisa Valentin, 'Landmark media code set to become law with Labor's backing', (16 February 2021), *The Sydney Morning Herald,* https://www.smh.com.au/politics/federal/landmark-media-code-set-to-become-law-with-labor-s-backing-20210216-p572wv.html
[26] Reuters, 'Facebook news ban stops Australians from sharing or viewing Australian and international news content', (18 February 2021), *ABC News,* https://www.abc.net.au/news/2021-02-18/facebook-to-restrict-sharing-or-viewing-news-in-australia/13166208; Amanda Meade, Josh Taylor & Daniel Hurst, 'Facebook reverses Australia news ban after government makes media code amendments', (23 February 2021), *The Guardian* https://www.theguardian.com/media/2021/feb/23/facebook-reverses-australia-news-ban-after-government-makes-media-code-amendments
[27] Josh Frydenberg & Paul Fletcher, *News Media and Digital Platforms Mandatory Bargaining Code*. (8 December 2020) https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/news-media-and-digital-platforms-mandatory-bargaining#:~:text=The%20News%20Media%20and%20Digital,public%20interest%20journalism%20in%20Australia
[28] *Telecommunications Act 1997,* s313(3)

Privacy

In October 2021, the Australian Government released an Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill (*Online Privacy Bill*)[29] for submissions and feedback by 6 December 2021. The Bill proposes amendments to the *Privacy Act 1988* (Cth), including establishing a framework to develop, implement and enforce a binding online privacy code to regulate large online platforms, social media platforms, and data brokers. The introduction of an Online Privacy Code is part of the response to the ACCC's Digital Platforms Inquiry Report,[30] which made extensive recommendations to strengthen privacy protections for individuals and improve transparency and accountability in data handling practices. The Bill would prevent social media platforms from accessing a child's data without a parent or guardian's permission and require companies to make all reasonable attempts to verify the age of users. The Bill would introduce stricter penalties and enforcement powers to enable the Office of the Australian Information Commissioner to resolve matters more effectively.

Disinformation and misinformation

In December 2019, as part of its response to the ACCC's Digital Platforms Inquiry Report, the Australian Government asked the digital industry to develop a voluntary code of conduct for disinformation and news quality.[31] The *Australian Code of Practice on Disinformation and Misinformation* was released in February 2021. It was drafted by Digital Industry Group Inc (DiGi), a non-profit industry association advocating for the digital industry in Australia. The voluntary code commits a diverse set of technology companies, including Facebook, Twitter, and Google, to reducing the risk of online misinformation causing harm to Australians. The signatories committed to safeguards to protect Australians and must publicly report their efforts in response to disinformation and misinformation. The Australian Communications and Media Authority reports on the efficacy of the code. The code has been criticised for its self-regulatory and opt-in approach, which may hinder its effectiveness.[32]

Defamation

On 25 October 2021, Nationals MP Anne Webster introduced a private member's Bill (the *Social Media (Basic Expectations and Defamation) Bill 2021*), which would enable the

[29] Attorney-General's Department, *Online Privacy Bill Exposure Draft*, Australian Government https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/
[30] Australian Competition and Consumer Commission, *Digital platforms inquiry - final report* (2019) https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
[31] Australian Government, *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (2019) https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf
[32] DIGI, *Disinformation code*, https://digi.org.au/disinformation-code/; Asha Barbaschow, 'Facebook, Google, Microsoft, TikTok, and Twitter adopt Aussie misinformation code', (22 February 2021), *ZDNet* https://www.zdnet.com/article/facebook-google-microsoft-tiktok-and-twitter-adopt-aussie-misinformation-code/; Josh Taylor, 'What is the Australian government doing to crack down on big tech, and why?', (30 October 2021), *The Guardian* https://www.theguardian.com/australia-news/2021/oct/30/what-is-the-australian-government-doing-to-crack-down-on-big-tech-and-why

Communications Minister to set basic expectations of social media service providers regarding the hosting of defamatory material on social media platforms. The proposed legislation would ensure that service providers are liable for defamatory material hosted on their platforms and not removed within a reasonable timeframe after notice from the eSafety Commissioner.[33] It remains unclear whether the government will adopt the Bill.[34]

On 28 November 2021, Prime Minister Scott Morrison and Attorney-General Michaelia Cash announced proposed new legislation which would include the introduction of new court powers to force social media platforms to unmask anonymous online trolls, with the aim of better protecting Australians online. The reforms, described by the Government as 'world-leading', will ensure social media companies are considered publishers and can be held liable for defamatory comments posted on their platforms. and the legislation is expected to be introduced into parliament in early 2022.[35] While reserving the Opposition's position, the Federal Opposition leader Anthony Albanese questioned how effective the imposition of domestic controls would be on a global industry and whether they could easily be avoided, for example by the use of foreign IP-addresses.[36]

Foreign Interference

Other legislation relevant to foreign interference includes the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020*[37] and the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*.[38]

[33] *Social Media (Basic Expectations and Defamation) Bill 2021*
[34] Josh Taylor, 'What is the Australian government doing to crack down on big tech, and why?', (30 October 2021), *The Guardian* https://www.theguardian.com/australia-news/2021/oct/30/what-is-the-australian-government-doing-to-crack-down-on-big-tech-and-why; Paul Karp, ' Social media giants face $10m fines for privacy breaches under proposed government reform', (25 October 2021), *The Guardian* https://www.theguardian.com/australia-news/2021/oct/25/social-media-giants-face-10m-fines-for-privacy-breaches-under-proposed-government-reform
[35] Australian Government, Prime Minister of Australia, *Combatting online trolls and strengthening defamation laws,* (28 November 2021) https://www.pm.gov.au/media/combatting-online-trolls-and-strengthening-defamation-laws
[36] Tom Lowrey, 'Social media companies could be forced to give out names and contact details under new anti-troll laws', (28 November 2021), *ABC News* https://www.abc.net.au/news/2021-11-28/social-media-laws-online-trolls/100657004
[37] Establishes a new legal framework to access overseas communication data for law enforcement and national security purposes, facilitating access to encrypted communications provided by non-Australian companies
[38] Grants the Australian Federal Police and Australian Criminal Intelligence Commission (ACIC) the ability to request new types of warrants to investigate and disrupt "serious" crime.

International Regulatory Responses

The United States

A surge in false, misleading and inflammatory content surrounding the November 2020 United States elections led to the violent attack on the U.S. Capitol on 6 January 2021. Following the storming of the Capitol, the U.S. Congress held a congressional hearing on 25 March 2021 interrogating the CEOs of Facebook, Google and Twitter about how their social media platforms spread extremism and misinformation, and the role of these platforms in the attack.[39] Executives from Facebook, YouTube and Twitter testified before a Senate Judiciary subcommittee on 27 April 2021 on the ways their platforms' algorithms influence users. Senators from both political sides criticised the negative effects of the advertising-supported business models and questioned the serving of harmful misinformation on the platforms.[40]

In mid-September 2021, the Wall Street Journal published a series of articles, commonly referred to as the 'Facebook Files', based on internal Facebook documents, released by a whistle-blower. The series included reports on internal studies, demonstrating that Facebook was aware of the negative impact of Instagram on teenage users, how the platform prioritises profit over public safety, and how its design features amplify hate, political unrest and misinformation.[41] On 5 October 2021, Frances Haugen came forward as the anonymous Facebook whistle-blower who released the internal documents.[42] Following the widespread media attention, she was invited to testify before the Senate Committee on Commerce, Science and Transportation about how the social network knowingly harms people (especially teenagers) with toxic content and how the company is failing to adequately protect against threats emerging from foreign entities including Russia, China and Iran.[43]

Social media has been at the forefront of Congressional and Senate hearings and oversight efforts over the past few years, including an October 2019 hearing on content

---

[39] US Congress, *Hearing on "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation"*, (2021) https://www.congress.gov/event/117th-congress/house-event/111407; House Committee on Energy and Commerce, *Hearing on "Disinformation Nation: Social media's role in promoting extremism and misinformation"*, (2021) https://energycommerce.house.gov/committee-activity/hearings/hearing-on-disinformation-nation-social-medias-role-in-promoting

[40] US Senate Hearing, *Algorithms and Amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds* https://www.judiciary.senate.gov/meetings/algorithms-and-amplification-how-social-media-platforms-design-choices-shape-our-discourse-and-our-minds

[41] Reed Albergotti, 'Frances Haugen took thousands of Facebook documents: This is how she did it', (26 October 2021), *The Washington Post* https://www.washingtonpost.com/technology/2021/10/26/frances-haugen-facebook-whistleblower-documents/; Wall Street Journal Investigation, 'The Facebook Files', *The Wall Street Journal*, wsj.com/articles/the-facebook-files-11631713039

[42] Daniel E. Slotnik, 'Whistle-Blower Unites Democrats and Republicans in Calling for Regulation of Facebook', (5 October 2021), *The New York Times* https://www.nytimes.com/live/2021/10/05/technology/facebook-whistleblower-frances-haugen

[43]US Senate Committee on Commerce, Science & Transportation, *Hearings* on "*Protecting Kids Online: Testimony from a Facebook Whistleblower,"* (5 October 2021) https://www.commerce.senate.gov/2021/10/protecting%20kids%20online:%20testimony%20from%20a%20facebook%20whistleblower

moderation[44] and a June 2020 hearing on the rise of disinformation and extremism online.[45] These are part of a broader policy discussion for reform currently taking place within the United States.[46]

Discussion on regulating social media platforms has largely centred on the First Amendment to the U.S. Constitution which prohibits censorship by the government, and on proposed amendments to Section 230 of the *Communications Decency Act*[47] which provides that an internet provider (such as a social media platform) cannot be treated as the publisher or speaker of third-party content. Section 230 gives social media platforms broad protection from liability for defamatory content, and broad scope to moderate discussions and remove or not remove posts.[48]

Section 230(c)(1) provides "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".[49] Section 230(c)(2) provides "Good Samaritan" protection from civil liability for operators of interactive computer services who remove or moderate third-party material they deem obscene or offensive, including constitutionally protected speech. [50]

Both Republicans and Democrats have advocated for the repeal of Section 230. As President, Donald Trump asserted online platforms were editing his and other right-wing sources' content, and they should no longer be protected from proceedings charging them with discrimination.[51] Conversely, President Joseph Biden has argued for the repeal of Section 230 on the basis that online platforms should be held responsible for disseminating false or misleading content.[52] Concerns have been raised regarding implications of reform on the First Amendment, for example that Section 230 encourages the moderation of content, and that the First Amendment protects social media platforms from hate speech liability.[53]

---

[44] House on Energy & Commerce, *Hearing on "fostering a healthier internet to protect consumers"* (16 October 2019) https://energycommerce.house.gov/committee-activity/hearings/hearing-on-fostering-a-healthier-internet-to-protect-consumers

[45] House on Energy & Commerce, *Joint hearing on "A country in crisis: How disinformation online is dividing the nation"* (24 June 2020) https://energycommerce.house.gov/committee-activity/hearings/joint-hearing-on-a-country-in-crisis-how-disinformation-online-is

[46] Gerrit De Vynck, Cat Zakrzewski & Elizabeth Dwoskin, *'Big tech CEOs face lawmakers in House hearing on social media's role in extremism, misinformation'*, (10 April 2021), *The Washington Post* https://www.washingtonpost.com/technology/2021/03/25/facebook-google-twitter-house-hearing-live-updates/

[47] 47 U.S.C. s230 https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim)

[48] Section 230 was developed in response to lawsuits against Internet service providers in the early 1990s that resulted in different interpretations of whether the service providers should be treated as publishers or, alternatively, as distributors of content created by its users. It was enacted as part of the Communications Decency Act, and the Act was challenged and ruled by the Supreme Court in *Reno v. American Civil Liberties Union* (1997) to be unconstitutional. However, Section 230 was determined to be severable from the rest of the legislation and remained.

[49] 47 U.S.C. s230 https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim)

[50] 47 U.S.C. s230 https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim)

[51] Abram Brown, 'What is section 230 - and why does Trump want to change it?' (28 May 2020), *Forbes* https://www.forbes.com/sites/abrambrown/2020/05/28/what-is-section-230-and-why-does-trump-want-to-change-it/?sh=7b540c33389d

[52] Sinan Aral, *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health—And How We Must Adapt.* Currency, New York, 2020.

[53] Ellen Goodman & Ryan Whittington, 'Section 230 of the Communications Decency Act and the Future of Online Speech', (9 August 2019), *The German Marshall Fun of the United States* https://www.gmfus.org/news/section-230-communications-decency-act-and-future-online-speech.

There have been a number of proposed reforms to regulate social media platforms and while there appears to be wide-ranging support for reforming Section 230, there is little agreement among political leaders about how this should occur. Unlike Australia where the introduction of legislation is tightly controlled by the government and the party system and Members of Parliament and Senators vote along party lines, the U.S. political system allows any member of the House of Representatives or Senate to propose legislation, with or without party support. Consequently, while many reforms have been proposed, they have not gained enough momentum and consensus to be implemented.

There have been numerous proposed reforms to Section 230, including many introduced in the 117th congressional session (2020-2021), several of which have been outlined below. These proposed Bills look to reform social media through amendments to Section 230 in four key ways: by repealing section 230 in whole, limiting the scope of Section 230, imposing new obligations or altering the 'Good Samaritan' part of Section 230.[54] While there are unique aspects to the regulatory debate and legislative reform in the US, it plays a leading role in setting the global policy agenda around social media, particularly given that the key technology companies are headquarted there. Accordingly, it is important to monitor and understand their proposals.

Regulating Online Platforms

Following the Facebook Files revelations, two major new Bills were put forward targeting big tech and social media. The most recent Bill put forward by Energy and Commerce Chair Frank Pallone and leading House Democrats[55], the *Justice Against Malicious Algorithms Act*[56] would amend Section 230 to remove absolute immunity in certain instances, specifically when an online platform knowingly or recklessly uses an algorithm to recommend harmful content that contributes to physical or severe emotional injury.[57] The Bill targets algorithms that materially contribute to a physical or severe emotional injury to a person. However, the proposed reform only applies to algorithms or search features that rely on personalisation.

The *Platform Accountability and Consumer Transparency Act (PACT Act)* is a bipartisan bill introduced to Congress in March 2021, aimed at imposing new obligations on internet companies. The PACT Act was originally introduced in the 2019-2020 Congressional session. The updated version of the Bill seeks to make content moderation for social

[54] Meghan Enand et al, 'All the ways congress wants to change section 230' (23 March 2021), *Slate* https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html
[55] Including Energy and Commerce Committee Chairman Frank Pallone, Jr. (D-NJ), Communications and Technology Subcommittee Chairman Mike Doyle (D-PA), Consumer Protection and Commerce Subcommittee Chair Jan Schakowsky (D-IL), and Health Subcommittee Chair Anna Eshoo (D-CA)
[56] *Justice Against Malicious Algorithms Act*, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/101421%20EC%20Section%20230%20Text.pdf
[57] House Committee on Energy & Commerce, *E&C Leaders announce legislation to reform Section 230* https://energycommerce.house.gov/newsroom/press-releases/ec-leaders-announce-legislation-to-reform-section-230

media platforms more transparent and increase consumer protections.[58] The PACT Act requires platforms to issue public statements on their policies regarding moderation, demonisation and the removal of user content, in addition to publishing transparency reports summarising their actions and statistics. The PACT Act additionally gives State Attorneys General the authority to bring legal action against platforms that violate federal civil law.[59] The Bill has been referred to the Senate Committee on Commerce, Science, and Transportation.[60]

The proposed *Safeguarding Against Fraud, Exploitation, Threats, Extremism and Consumer Harms Act (SAFE TECH Act)* was introduced in May 2021 and limits the scope of section 230 immunity. The SAFE TECH Act removes the legal protections for platform providers in situations where they have accepted payment to either make the speech available or have created or funded the speech.[61] The Bill also creates new exceptions to the liability protections in cases involving civil rights laws, antitrust laws, stalking, harassment or intimidation laws, international human rights laws and wrongful death action.[62] The objective of the SAFE TECH Act is to hold social media companies accountable for enabling cyber-stalking, targeted harassment, and discrimination.[63] The bill was referred to the Subcommittee on Communications and Technology in May 2021.[64]

The *Protecting Americans from Dangerous Algorithms Act,* introduced in March 2021, similarly removes liability immunity for a platform, focusing on the algorithmic promotion of harmful, radicalising content interfering with civil rights.[65] Under the proposed legislation, companies may still use Section 230 as a defence in cases if they distribute

---

[58] U.S. Senator for Hawai'i Brian Schatz (17 March 2021). *Schatz, Thune Reintroduce Legislation To Update Section 230, Strengthen Rules, Transparency on Online Content Moderation, Hold Internet Companies Accountable For Moderation Practices*. https://www.schatz.senate.gov/news/press-releases/schatz-thune-reintroduce-legislation-to-update-section-230-strengthen-rules-transparency-on-online-content-moderation-hold-internet-companies-accountable-for-moderation-practices.

[59] Frank Konkel, 'Bipartisan Bill Would Hold Tech Companies Responsible for Moderating Content', (17 March 2021), *Nextgov*. https://www.nextgov.com/policy/2021/03/bipartisan-bill-would-hold-tech-companies-responsible-moderating-content/172739/; Ashley Johnson & Daniel Castro, 'PACT Act Would Increase Platform Transparency, But Undercut Intermediary Liability', (7 August 2020), *Information Technology & Innovation Foundation* https://itif.org/publications/2020/08/07/pact-act-would-increase-platform-transparency-undercut-intermediary

[60] *PACT Act*, s797 https://www.congress.gov/bill/117th-congress/senate-bill/797/text?q=%7B%22search%22%3A%5B%22PACT+Act%22%2C%22PACT%22%2C%22Act%22%5D%7D&r=5&s=1

[61] Mark R. Warner, US Senator from the Commonwealth of Virginia, (5 February 2021), *Warner, Hirono, Klobuchar Announce the SAFE TECH Act to Reform Section 230*. https://www.warner.senate.gov/public/index.cfm/2021/2/warner-hirono-klobuchar-announce-the-safe-tech-act-to-reform-section-230.

[62] Taylor Hatmaker, 'The SAFE TECH ACT offers Section 230 reform, but the law's defenders warn of major side effects' (6 February 2021), *TechCrunch*. https://techcrunch.com/2021/02/05/safe-tech-act-section-230-warner/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAK_1kWPdJZrtSdGq4U1bPw3cTXtx7mSHfZtpkVUbdVRUBvyIrITpop-GtBDjd9xYur9rKcIH_zXPMfjuSE72yaHNJdtXxPhztFH0X1JEWhHoyxP2aIepdEMUAqT5eBuiKOdVLBXiO1pOj8ESvgRhMhbjAfZJu2vvQ05KCeZv8_Lf.

[63] Mark R. Warner, US Senator from the Commonwealth of Virginia, *Warner, Hirono, Klobuchar Announce the SAFE TECH Act to Reform Section 230* , (5 February 2021) https://www.warner.senate.gov/public/index.cfm/2021/2/warner-hirono-klobuchar-announce-the-safe-tech-act-to-reform-section-230.

[64] *SAFE TECH Act* https://www.congress.gov/bill/117th-congress/house-bill/3421/actions?r=3&s=3

[65] *Protecting Americans from Dangerous Algorithms Act* https://www.congress.gov/bill/117th-congress/house-bill/2154/text?q=%7B%22search%22%3A%5B%22Malinowski%22%5D%7D&r=2&s=3; Congressman Tom Malinowski, Representing the 7th District of New Jersey, *Reps. Malinowski and Eshoo reintroduce bill to hold tech platforms accountable for algorithmic promotion of extremism* (24 March 2021) https://malinowski.house.gov/media/press-releases/reps-malinowski-and-eshoo-reintroduce-bill-hold-tech-platforms-accountable.

content using methods that are "obvious, understandable, and transparent" to a reasonable user. [66] The Bill was referred to the Subcommittee on Communications and Technology in March 2021.

Other examples of legislation under consideration include Republican Senator Rick Scott's *Safe Social Media Act*, introduced in May 2021, which would require the Federal Trade Commission, in coordination with the Centers for Disease Control, to conduct a study on social media use among American teenagers and children including the use of personal information in algorithms, the mental health effects and the long-term impact of extended usage.[67] The *Abandoning Online Censorship (AOC) Act* was introduced in February 2021 and would repeal section 230.[68] The *Health Misinformation Act of 2021* was introduced in July 2021 and would create an exception to liability protections for platforms using algorithms to promote health misinformation, and would take effect for the remainder of the public health emergency.[69] The *Disincentivizing Internet Service Censorship of Online Users and Restrictions on Speech and Expression Act (DISCOURSE)* was introduced in June 2021 and would amend the Good Samaritan provision so that platforms would only receive liability protections when content that is extremist, obscene or unlawful was moderated. The Bill would also add a clause making it more difficult to be protected under section 230 when content is moderated so that it "burdens" religious exercise.[70]

The *Protect Speech Act*, introduced in June 2021 would narrow a platform's ability to use Section 230 as a defence for content removal.[71] The *21st Century Foundation for the Right to Express and Engage in Speech Act (21st Century FREE Speech Act*) would repeal section 230, and replace it with a reclassification of platforms as common carriers, required to provide their services to everyone, imposing additional responsibilities to platforms. Liability protections would only apply to platforms removing content in accordance with their content moderation policies, and the bill would also establish a private right of action.[72] The *Stop Shielding Culpable Platforms Act*, introduced in March 2021 would amend Section 230 to note it does not prevent a provider or user of a platform from being treated as the distributor of information provided by a third party.[73] The *See Something, Say Something Online Act of 2021,* introduced in January 2021 would require platforms to report suspicious transmissions they detect, and platforms would have to take reasonable steps to prevent and address these transmissions. Section 230 would could not be used as a defence if the provider should have been reasonably aware of the suspicious

[66] *Protecting Americans from Dangerous Algorithms Act* https://www.congress.gov/bill/117th-congress/house-bill/2154/text?q=%7B%22search%22%3A%5B%22Malinowski%22%5D%7D&r=2&s=3
[67] A Bill to require the Federal Trade Commission to conduct a study regarding social media use by teenagers, S. 1630, 117th Congress. (2021). https://www.congress.gov/bill/117th-congress/senate-bill/1630/text?r=4&s=1.
[68] *AOC Act* https://www.congress.gov/bill/117th-congress/house-bill/874/text?q=%7B%22search%22%3A%5B%22section+230%22%5D%7D&r=1&s=3
[69] *AOC Act* https://www.congress.gov/bill/117th-congress/house-bill/874/text?q=%7B%22search%22%3A%5B%22section+230%22%5D%7D&r=1&s=3
[70] *DISCOURSE Act*, s2228 https://www.congress.gov/bill/117th-congress/senate-bill/2228
[71] *Protect Speech Act* https://www.congress.gov/bill/117th-congress/house-bill/3827/text?q=%7B%22search%22%3A%5B%22protect+speech%22%5D%7D&r=1&s=2
[72] *Century FREE Speech Act*, s1384 https://www.congress.gov/bill/117th-congress/senate-bill/1384?s=9&r=2
[73] *Stop Shielding Culpable Platforms Act* https://www.congress.gov/bill/117th-congress/house-bill/2000/text?q=%7B%22search%22%3A%5B%22jim+banks%22%5D%7D&r=4&s=5

transmission.[74] The *Curbing Abuse and Saving Expression in Technology (CASE-IT) Act*, introduced in January 2021 would prevent a platform from using Section 230 as a defence for one year if the company creates, posts, materially contributes to, or induces another person to contribute to illegal online content.[75] The *Protecting Constitutional Rights From Online Platform Censorship Act*, introduced in January 2021 would remove the Good Samaritan provision and make it unlawful for any internet platform to restrict access or availability to content.[76]

While there appears to be some level of bipartisan consensus that there is an issue, the number and breadth of proposed legislation demonstrates the difficulty in agreeing on a regulatory solution.

Antitrust

The *American Innovation and Choice Online Act*,[77] put forward by a bipartisan group of Senators is an antitrust measure, is another high profile Bill recently proposed. This Bill does not look at Section 230; instead, it would prevent U.S. technology giants from giving an advantage to their own products over those of competitors. This comes after a various high-profile hearings in which the Senate Judiciary Subcommittee on Competition Policy, Antitrust and Consumer Rights investigated the conduct of big tech companies including Apple and Google.[78] The Bill would help restore competition online by establishing 'commonsense' rules for dominant digital platforms to prevent them from abusing their market power to harm competition, online businesses and consumers and from reducing incentives to innovate. The proposed Act outlines clear rules to protect competition, and gives enforcers strong and flexible tools to deter violations and hold platforms to account.[79] The *American Innovation and Choice Online Act* follows on from the proposed House of Representatives Bill, the *American Choice and Innovation Online Act* which was introduced on 11 June 2021, and ordered to be amended by the House on 24 June 2021.[80]

While the *American Innovation and Choice Online Act* is one of the most widely supported bills on antitrust measures, there are other similar proposed reforms, several of which are listed below. The House of Representatives Antitrust Subcommittee has proposed the *Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act*, which would require covered platforms to "maintain a set of transparent, third-party-

[74] *See Something, Say Something Online Act of 2021*, s27 https://www.congress.gov/bill/117th-congress/senate-bill/27/text?q=%7B%22search%22%3A%5B%22see+something+say+something%22%5D%7D&r=1&s=1
[75] *CASE-IT Act* https://www.congress.gov/bill/117th-congress/house-bill/285/text?q=%7B%22search%22%3A%5B%22section+230%22%5D%7D&r=2&s=3
[76] *Protecting Constitutional Rights from Online Platform Censorship Act* https://www.congress.gov/bill/117th-congress/house-bill/83/text?q=%7B%22search%22%3A%5B%22section+230%22%5D%7D&r=3&s=2
[77] *American Innovation and Choice Online Act* https://www.klobuchar.senate.gov/public/_cache/files/7/d/7d176f5c-c84b-4207-8d96-77469fe1db44/903C851389B04EA66A4D2133A3EA18CF.sil21b56.pdf
[78] Michael W. Scarborough & M Kevin Castello, 'Senate Zeros in on Big Tech with Latest Antitrust Reform Bill' (2021) 11 (334) *National Law Review* https://www.natlawreview.com/article/senate-zeros-big-tech-latest-antitrust-reform-bill
[79] US Senator Amy Klobuchar, *Support Builds for Bipartisan Legislation From Klobuchar, Grassley, and Colleagues to Rein in Big Tech* (18 October 2021) https://www.klobuchar.senate.gov/public/index.cfm/2021/10/support-builds-for-bipartisan-legislation-from-klobuchar-grassley-and-colleagues-to-rein-in-big-tech
[80] *American Choice and Innovation Online Act* https://www.congress.gov/bill/117th-congress/house-bill/3816/actions

accessible interfaces . . . to enable the secure transfer of data to a user",[81] and the *Ending Platform Monopolies Act*, which would prohibit technology platforms with at least 50,000,000 active monthly U.S. users and a market capitalisation of over $600 billion from selling products or services that they own and control.[82]

Protecting Children

U.S. Democratic Representative Kathy Castor introduced an updated *Protecting the Information of our Vulnerable Children and Youth Act (Kids PRIVCY Act*) on 29 July 2021 to strengthen the *Children's Online Privacy Protection Act (COPPA*). The Bill expands privacy protections for children and teenagers, and incorporates key elements of the U.K.'s Age-Appropriate Design Code. This includes banning companies from providing targeted advertisements to children and teenagers, requiring opt-in consent for individuals under 18, creating a right to access, correct and delete personal information, expanding coverage of companies, and strengthening enforcement.[83]

European Union

The European Union (EU) is comprised of 27 sovereign and independent countries (and their citizens), known as Member States, who have pooled some of their 'sovereignty', delegating some of their decision-making powers to shared institutions such as the European Council, the European Parliament and the European Commission. Generally, the European Commission proposes new laws, the European Parliament and European Council adopt them, and then Member States and the European Commission then implement them. Regulations passed are applicable and binding in all Member States directly, and while they do not have to passed into national law by Member States, national laws may need to be amended to avoid conflict with the regulation.[84]

The European Union is striving to be global role model for the digital economy and internationally promote its digital standards. As such a large and influential market, their regulation of social media contributes to the setting of global norms. The legislation proposed by the EU will have significant impacts on European democracy, and how they are able to balance the market, state, civil society and speech.[85] The EU and its member

[81] *ACCESS ACT* https://cicilline.house.gov/sites/cicilline.house.gov/files/documents/ACCESS%20Act%20-%20Bill%20Text%20%281%29.pdf
[82] *The Ending Platform Monopolies Act* https://cicilline.house.gov/sites/cicilline.house.gov/files/documents/Ending%20Platform%20Monopolies%20-%20Bill%20Text.pdf
[83] U.S. Representative Kathy Castor, (29 July 2021), *Rep. Castor Reintroduces Landmark Kids PRIVCY Act to Strengthen COPPA, Keep Children Safe Online* https://www.congress.gov/bill/117th-congress/house-bill/4801?r=12&s=1 https://castor.house.gov/news/documentsingle.aspx?DocumentID=403677; https://www.congress.gov/bill/117th-congress/house-bill/4801?r=12&s=1
[84] https://eeas.europa.eu/archives/delegations/singapore/documents/more_info/eu_publications/how_the_european_union_works_en.pdf
[85] Damian Tambini, 'Media Policy in 2021. As the EU takes on the tech giants, will the UK' (12 January 2021) *London School of Economics* https://blogs.lse.ac.uk/medialse/2021/01/12/media-policy-in-2021-as-the-eu-takes-on-the-tech-giants-will-the-uk/

states are pursuing regulation in various areas, including artificial intelligence, digital markets and services, connectivity, cybersecurity, data and digital identity.[86]

The European Commission's approach focuses on digital transformation, making technology work for people and fostering a cohesive democratic society through investment in digital skills. Europe's overarching digital strategy, *Shaping Europe's Digital Future,*[87] released on 19 February 2020, invests in digital skills for all Europeans and protects against cyber threats. The Strategy focuses on ensuring that technology – in particular artificial intelligence – is developed in a way that respects individuals rights, and maintains their trust. The digital strategy targets a fair and competitive digital economy, and an open, democratic and sustainable society.[88]

Digital Services and Markets

The European approach to regulating the digital environment centres around the *Digital Markets Act*[89] and *Digital Services Act,*[90] which were both proposed on 15 December 2020. These Acts are currently proposals. In order for them to become binding on EU member states, they require approval by the European Council and the European Parliament. This is expected to take 18 months from when they were proposed by the European Commission. These Acts aim to provide users with access to a wide range of safe products and services online. Upon implementation, these Acts would impose an EU-wide obligation on Member States to ensure that digital services connecting consumers to goods, services and content also protect user's fundamental rights. The regulations would be binding in their entirety and directly applicable in all Member States, as harmonisation and cooperation cannot be achieved by Member States acting in silos.

The *Digital Markets Act* is based on the understanding that social media and digital platforms have strong network effects, particularly as increased use by business and end-users (the consumers of the goods and services) drives further demand. In mediating the connection between businesses and end-users, platforms have the potential to create lock-in effects (making the user dependent on them for products and services, unable to use another service without substantial switching costs) and a significant level of dependence of both businesses and users. In turn, this enhances the bargaining power of the platforms, creates unequal relationships between market actors, and impedes innovation.

[86] European Commission, *Priorities 2019-2024, A Europe fit for Digital Age* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en
[87] European Commission, *Shaping Europe's Digital Future* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en
[88] European Commission, *Shaping Europe's Digital Future* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en
[89] Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN
[90] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services

The *Digital Markets Act* proposes that the collection of large amounts of data from end-users by digital market gatekeepers should be regulated and transparent to protect the privacy interests of end-users. The Act requires data sharing across platforms to be a voluntary choice by end-users rather than the only available and accessible option. Further, social media and other digital platforms would be required to offer end-users the ability to opt out of processes that require access through a gateway controlled by a single gatekeeper. Under the Act, platforms would be restricted in their the deep profiling of end-users – where large volumes of information about a user are combined. Where profiling processes are in play, users would need to be informed of the profiling's purpose and impact. Service providers would need to demonstrate the steps taken to ensure user awareness of the use of profiling, and their consent. Platforms will not be able to combine personal data from core platform services with any other service offered by the gatekeeper unless user consent is provided.[91]

Other measures may complement this Act; for example, a proposal by the Committee on Economic and Monetary Affairs has called for banning platforms from displaying micro-targeted advertisements that rely on deep profiling.[92]

The *Digital Services Act* seeks to improve users' online safety, and better protect their fundamental rights and online anonymity where possible.[93] This proposal tackles core operations of platforms, namely how information is prioritised and presented on its online interface. Significant online platforms (with more than 45 million end-users, or an equivalent of 10% of the European Union population)[94] would be required to ensure recipients are appropriately informed of the information presented to them. The Act defines the responsibilities of digital services providers, specifically online platforms, social media, and online marketplaces. Further, it outlines obligations and procedures to tackle illegal content and disinformation, and offers the opportunity to challenge content moderation decisions. The proposal introduces safeguards protecting fundamental rights, allowing citizens to freely express themselves while maintaining rights to effective remedies, non-discrimination, the rights of the child, and personal data and privacy protection.[95] Platforms would be required to ensure recipients of online advertisements know what information has been used to personalise advertising content, and platforms will have to obtain user consent prior to processing data for targeted advertising.

[91] Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN
[92] European Parliament resolution of 18 June 2020 on competition policy – annual report 2019 (2019/2131(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2020-0158_EN.html
[93] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services
[94] Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN
[95] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services

These regulated platforms would also have to ensure public access to repositories of advertisements displayed on their online interfaces, to facilitate supervision and research into emerging risks brought about by the distribution of advertising online. These risks include illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality.[96]

The Act would allow for protocols in response to extraordinary situations affecting public security or public health. In such a crisis, the Commission would initiate the drafting of a protocol to coordinate a rapid, collective, and cross-border response in the online environment.[5] Further, the Commission encourages these platforms to participate in the drafting, testing and application of crisis protocols. This may include displaying prominent information on the crisis provided by Member States authorities on the Union level, initiating or adjusting cooperation between online platforms, facilitating a faster response to removing access to illegal or harmful content, and termination of services providing such content to their recipients. The Commission is aware of a possible conflict between the protection of human rights and freedom of expression and hence seeks collaboration in the drafting and implementation of appropriate protocols.[97]

Platforms would be required to respond without delay and inform the issuing authority of the actions taken when an order is made against a specific item of illegal content. The Digital Services Coordinator is required to transmit the order to all other Digital Services Coordinators. Member States will be required to appoint a Digital Services Coordinator (DSC), an authority to supervise, investigate, and enforce the regulation in the Member State. The DSCs have powers to require information from providers, carry-out on-site inspections, ask any staff member or representative of the providers for explanations regarding investigation cases. They are also required to publish annual reports on their activities. DSC's can impose fines and penalties for failure to comply with the regulation.[98] DSCs from each member State will form the European Board of Directors.[99]

The European Union has also developed an initiative, EU4Digital, to extend the Digital Single Market to the Eastern Partnership (which includes Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, and Ukraine). EU4Digital promotes key digital economy and society concerns in line with EU norms and practices.[100] It supports the reduction of roaming tariffs, developing high-speed broadband to boost economies and expand e-

[96] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services
[97] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services
[98] Penalties shall not exceed 6% of the annual income or turnover of the provider for the failure to comply with regulations, and no more than 1% of the annual profit or turnover if the provider is providing misleading information to the coordinators.
[99] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services
[100] EU4Digital Website, https://eufordigital.eu/

services, coordinated cyber-security, and harmonizing digital frameworks in areas ranging from logistics to health, skills, and jobs creation in the digital industry.[101]

Concern has been voiced regarding the effect of the proposed legislation on digital services and digital markets. Specifically, there is concern that it could allow repressive governments to suppress speech.[102] Amnesty International welcomed the *Digital Services Act*, although stated that it does not go far enough to protect people's human rights.[103] Their position is that companies should not be granted more responsibility regarding the adjudication of the legality of the content and should not bear liability for failure to remove it if they are not aware of its presence. Amnesty calls for stricter limits in the targeting of online advertisements and that deep-profiling should be an opt-in option rather than an opt-out.[104]

Civil societies around the globe formed *Digital Services Act Human Rights Alliance* in May 2021, calling on the EU to focus on the protection of human rights.[105] Recognising that the European Union approach will have global influence, they call for some changes to the *Digital Services Act*. Their recommendations include not legally imposing automated content moderation tools and to focus on protecting human rights, especially on very large online platforms. In their joint statement, they state that decreasing the response time for removal requests will result in more pressure on small platforms and the removal of legitimate content.[106] They also urge legislators to prevent public authorities from becoming trusted flaggers (entities approved by the EU as having expertise and competence in identifying illegal content) and that the conditions for instituting trusted flagger status should not be determined solely by private platforms.[107]

Digital Education

The European Union has drafted the *Digital Education Action Plan 2021-2027* to support the sustainable and effective modernisation of education and training systems. The plan has two key priorities, to foster the development of a high-performing digital education

[101] EU4Digital Website, https://eufordigital.eu/
[102] See, eg, European plans to regulate internet will have major impacts on civic space at home and abroad' (10 May 2021), *OpenGlobalRights*, https://www.openglobalrights.org/european-plans-to-regulate-internet-will-have-major-impacts-on-civic-space-at-home-and-abroad/
[103] Amnesty International, *Amnesty International Position of the proposals for a Digital Services Act and a Digital Markets Act* (2020) https://www.amnesty.eu/news/amnesty-international-position-on-the-proposals-for-a-digital-services-act-and-a-digital-markets-act/
[104] Amnesty International, *Position Paper on the Proposal for a Digital Services Act and Digital Markets Act* (2021) https://www.amnesty.eu/wp-content/uploads/2021/04/Amnesty-International-Position-Paper-Digital-Services-Act-Package_March2021_Updated.pdf
[105] Acces Now, *Digital Services Act: Bad decisions can lead to global consequences* (22 October 2021) https://www.scoop.co.nz/stories/WO2110/S00210/digital-services-act-bad-decisions-can-lead-to-global-consequences.htm
[106] Digital Services Act Human Rights Alliance, *Joint Statement of the Digital Services Act Human Rights Alliance* (21 October 2021) https://www.eff.org/files/2021/10/21/digital_services_act_human_rights_alliance_statement_upd.pdf
[107] Ibid.

eco-system (priority 1), and to enhance digital skills and competencies for digital transformation (priority 2).[108]

The plan encompasses a variety of actions which target key challenges of the digital era, including:

- Creating the *European Digital Content Framework* by 2023, with an understanding of the underlying 'supply side' and 'demand side' issues relating to digital education content in response to the problems algorithms pose for educational resources (Action 3);
- Creating common guidelines for teachers and educators to foster digital literacy and tackle disinformation through education and training, with a planned finalisation date of September 2022 (Action 7);
- Developing a European Digital Skills Certificate (EDSC), which will enhance the transparency and mutual recognition of digital skills certification by governments, employers, and other stakeholders across Europe (Action 9). The EDSC is expected to be fully operational 2023;
- Improving the provision of digital skills in education and training, to empower Europeans with basic and advanced digital skills (Action 10). The aim is for at least 65% of Europeans to have at least basic digital skills by 2025, with the proposal to be finalised by the end of 2022;
- Collecting cross-national data on student digital skills and reducing the share of low-achieving 13-14 year olds in computer and information literacy to below 15% by 2030 (Action 11);
- Providing Digital Opportunity Traineeships, to provide higher education students the opportunity to gain professional experience in digital fields demanded by the labour market (Action 12).[109]

The EU Commission has also funded the Digital Wellbeing Educators Project, which focuses on increasing lecturers and teachers' capacity to integrate the promotion of students digital wellbeing into education.[110] The project helps students critically assess the media they consume and create, to become responsible and confident digital citizens.[111] The project provides resources to introduce practical strategies on digital competency. Participating institutions, universities, and colleges have strengthened their commitment to support their staff and students digital wellbeing. Further, an App has been developed with short courses on digital wellbeing for students. Feedback on the App noted its assistance in assessing social media usage and improving critical thinking skills.[112]

---

[108] European Commission, *Digital Education Action Plan 2021-2027* https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[109] European Commission, *Digital Education Action Plan 2021-2027* https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[110] European Commission, *Digital Wellbeing Educators Project* https://ec.europa.eu/programmes/erasmus-plus/projects/eplus-project-details/#project/2018-1-UK01-KA203-048214
[111] European Commission, *Joint Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, Action Plan Against Disinformation* (2018) https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf
[112] European Commission, *Digital Wellbeing Educators Project* https://ec.europa.eu/programmes/erasmus-plus/projects/eplus-project-details/#project/2018-1-UK01-KA203-048214

Disinformation

In 2018 the EU Commission issued an Action Plan Against Disinformation (the Plan) in response to the threat of online disinformation, specifically by Russia. The Plan outlines the EU's coordinated response to disinformation, and is based on the cooperation of EU institutions, Member States, civil society, and the private sector.[113]

The Plan aims to improve EU capabilities to detect, analyse and expose disinformation by: using data mining; and increasing the number of analysts; and investing in relevant analytical tools. Further, the plan centres on strengthening joint responses to disinformation through the creation of the *Rapid Alert System* which provides alerts on disinformation in real-time. This system would improve information-sharing and awareness among the Member States. The plan also raises awareness and increases the level of digital literacy of platform users, through campaigns including the European Week of Media Literacy. These campaigns encourage independent quality journalism, promote media freedom, and support pluralism.

The European External Action Service (the EU's diplomatic wing), created the East StratCom Task Force to support the plan. The Task Force's mandate is to expose disinformation in countries within and neighbouring the EU, the three priority regions being to the EU's East, South, and Western Balkans.

The Plan mobilises the private sector to tackle disinformation through the Code of Practice. This Code is the first time globally that industry has voluntarily agreed to self-regulatory standards to combat disinformation.[114] Signatories to the Code committed to respond to disinformation, invest in detection technologies, and address verifiable false or misleading information.[115] Initial signatories included Facebook, Google, Twitter, and Mozilla.[116] The platforms have agreed to invest in products, technologies and programs to assist users make informed decisions when they encounter online news that might be false; invest in technological means to prioritise relevant, authentic and authoritative information in search and feed features; and invest in features making diverse perspectives about public interest topics easier to locate.[117] The implementation assessment on the Code was generally positive, and indicated that the Code had set the foundation for further activities. While the Code has improved awareness on disinformation, and led to the implementation of policies by platforms to increase

[113] European Commission, *Joint Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, Action Plan Against Disinformation* (2018) https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf
[114] European Commission, *Code of Practice on Disinformation* https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[115] European Commission, *Code of Practice on Disinformation* https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[116] European Commission, *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions Tackling online disinformation: a European Approach* (2018) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN
[117] European Commission, *Joint Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, Action Plan Against Disinformation* (2018) https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

collaboration with researchers and fact-checkers, the voluntary nature of the Code and lack of sufficient communication between Signatories and researchers poses issues for enforceability and effectiveness.[118]

A multi-disciplinary committee, the Social Observatory for Disinformation and Social Media Analysis (SOMA) has been established to support the plan.[119] Through SOMA, fact-checkers collaborate with tech specialists, data collection experts, and applied machine learning to exploit existing verification platforms and provide experts with necessary resources and tools to fight disinformation. SOMA is negotiating with major social media networks to access their content and data. SOMA also conducts investigations into disinformation narratives in the European Union.[120]

The Plan is complemented by other EU efforts to regulate online platforms. In 2021, the European Council implemented a regulation to address the online dissemination of terrorist content. This regulation gives the competent authority of each Member State the power to issue an order to hosting service providers to remove terrorist content or disable access to terrorist content in all Member States. The hosting provider must remove content or disable access in all member States within one hour of receipt of the removal order.[121]

EU Member States

In parallel with the EU actions, Member States have taken legislative and non-legislative measures to tackle disinformation and social media concerns more broadly.[122]

Germany

The *Network Enforcement Act* (NetzDG) was implemented in 2017, to combat hate speech and misleading information on social media. While the legislation did not enforce new requirements for social media platforms, it imposed large fines for noncompliance with existing legal obligations. Under NetzDG, platforms are required to respond to complaints of unlawful content and determine whether the content is illegal in accordance with the German Criminal Code. If illegal, the content must be removed within 24 hours, or in some cases, within seven days. Illegal content may include the incitement of violence or hatred against national, religious, ethnic, or racial groups. Penalties for non-compliance include fines of up to €50 million ($79 million AUD) per violation. On 28 June 2021, NetzDG was

[118] Iva Plasilova et al., 'Study for the assessment of the implementation of the Code of Practice on Disinformation', (2020), *European Commission* https://digital-strategy.ec.europa.eu/en/library/study-assessment-implementation-code-practice-disinformation
[119] European Commission, *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions Tackling online disinformation: a European Approach* (2018) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN
[120] SOMA, https://www.disinfobservatory.org/
[121] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2021.172.01.0079.01.ENG
[122] Iva Plasilova et al., 'Study for the assessment of the implementation of the Code of Practice on Disinformation', (2020), *European Commission* https://digital-strategy.ec.europa.eu/en/library/study-assessment-implementation-code-practice-disinformation

amended, to increase the content and comparability of social media providers' transparency reports and improve the user-friendliness of reporting channels for complaints. The amendment introduced an appeals procedure for measures taken by the social network platform.[123]

Austria

The *Communications Platforms Act* came into force in 2021, in response to an increase in hate speech, harassment, and the spreading of false information on online platforms. Under the legislation, providers (domestic and foreign providers of for-profit communication platforms that have more than 100,000 users in Austria or revenues exceeding EUR 500,000) are required to establish effective and transparent procedures for reporting and deleting. Deletion must occur within 24 hours if the illegality is "obvious to a legal layman", or within 7 days if a detailed examination is necessary. Platforms are required to store deleted postings for at least ten weeks for any possible prosecution. Providers are required to submit an annual review on illegal content handling, or a quarterly review for platforms exceeding one million registered users. If non-compliant with the legislation, fines of up to EUR 10 million can be imposed on the platform, and fines of up to EUR 1 million can be imposed on members of the managing board.[124]

The EU Commission noted the Act may impede the freedom to provide services and may lead to unnecessary additional costs and administrative burdens. The EU Commission also questioned why Austria implemented its own legislation while the Digital Services Act is being formulated. Nevertheless, the Austrian government's position is that the urgency of the issue required immediate implementation of national measures, before EU wide regulations are implemented.[125]

Sweden

Sweden has sought to increase the misinformation literacy of its citizens, with the Civil Contingencies Agency (MSB) releasing the *Countering Information Influence Activities: A Handbook for Communicators* in 2018. The publication provides communicators working in public administration with resources in the event of an actual or anticipated disinformation influence campaign.[126] The Swedish Minister for Digital Development Anders Ygeman noted in early 2020 that he wanted to introduce legislation to increase accountability for social media platforms in removing offensive content.[127] Additionally,

[123] *Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)* https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=AD99C47B2608D

[124] European Commission, *Draft Federal Act on measures to protect users on communication platforms (Communication Platforms Act)* https://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2020&num=544

[125] Gabriela Staber, *Communication platforms face new obligations and high fines in Austria* https://www.lexology.com/library/detail.aspx?g=fcf46df4-4694-4f10-b11b-67564a824470

[126] Swedish Civil Contingencies Agency: *Countering information influence activities: A handbook for* communicators (2018) https://www.msb.se/RibData/Filer/pdf/28698.pdf

[127] Fanny Svärd, 'Government wants to legislate against illegal content in social media', (18 February 2020), *Radio Sverige* https://sverigesradio.se/artikel/7410502

Sweden has also advocated for a tougher stance in the EU against platforms such as Google and Facebook and fraudulent and illegal material posted on their platforms.[128]

Spain

The Spanish Government's policy – *Spain Digital 2025* – includes nearly 50 measures to promote the country's digital transformation process over 5 years, aligned to the EU Digital Strategy. *Spain Digital 2025* targets digital connectivity, cybersecurity and strengthening the digital skills of the general public.[129] In July 2021, the Spanish Government adopted the *Charter on Digital Rights*, fulfilling a mandate in *Spain Digital 2025,* to reinforce and extend citizens' rights, generate certainty in the new digital age and increase people's confidence in the face of the disruption that technology represents. The Charter includes rights on freedom, the right to identity in the digital environment, data protection, pseudonymisation, the right to not be traced and profiled, the right to cybersecurity and to digital inheritance.[130]

Denmark

Denmark's primary focus on social media is on ensuring clear guidelines around product advertisement on platforms. As businesses are relying more on "influencers" and "bloggers" to sell their products online, clear and transparent advertising has become a priority.[131] Section 4 of the *Danish Marketing Practices Act* dictates that advertising through social media should be clearly distinguishable, to ensure target groups recognise content as an advertisement and are able to judge the content accordingly.[132]

In March 2021, Danish lawmakers proposed legislation to make tech giants, such as Facebook and Google, pay Danish media for using content on their platforms.[133] The legislation was implemented in June 2021 and builds on an EU directive giving individual media outlets the right to agree deals with tech giants.[134] The legislation was inspired by the Australian *News Media and Digital Platforms Mandatory Bargaining Code*.

Denmark has also adopted an EU Code of Practice on Disinformation that applies to Denmark as an EU Member State. Further, since 2018 the Danish Government has

[128] TricksFast, 'Ygeman: Indecent of Google and Facebook for not stopping posts', (12 January 2020), *TricksFast* https://tricksfast.com/sweden/ygeman-indecent-of-google-and-facebook-for-not-stopping-posts/
[129] Government of Span, *Digital Spain 2025* https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210204_Digital_Spain_2025.pdf
[130] Carta Derechos Digitales https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf ; Government of Spain, 'The Government adopts the Digital Rights Charter to articulate a reference framework to guarantee citizens' rights in the new digital age' (14 July 2021) https://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2021/20210713_rights-charter.aspx
[131] *Danish Marketing Practices Act* s 4. 'Covert advertising'. https://www.consumerombudsman.dk/marketing-practices-act/covert-advertising/
[132] *Danish Marketing Practices Act* s 4. 'Covert advertising'. https://www.consumerombudsman.dk/marketing-practices-act/covert-advertising/
[133] Ritzau, 'Denmark proposes new law to make Facebook pay for news and music', (26 March 2021), *The Local* https://www.thelocal.dk/20210326/denmark-proposes-new-law-to-make-facebook-pay-for-news-and-music/
[134] European Parliament, *Agreement reached on digital copyright rules,* (13 February 2019), https://www.europarl.europa.eu/news/en/press-room/20190212IPR26152/agreement-reached-on-digital-copyright-rules

increased media literacy among government and defence employees to combat disinformation.[135] Digital literacy and technology is also built into early years educational settings. Most kindergartens use digital technologies in their pedagogical practices as well.[136] Screen time and the use of digital technologies continue to be a paradox as parents are torn between their inclination to limit their child's screen use and to ensure children are digitally literate.[137]

France

Legislation was passed in December 2018 cracking down on the dissemination of false information. The law allows election candidates to sue for the removal of contested news reports during election periods, and requires social media platforms to disclose the source of funding for sponsored content. The legislation imposes a quick-response judicial review of potentially "manipulative" information shared during electoral periods.[138] Online platforms are required to establish a mechanism for users to flag false information in an easily accessible and visible way. The legislation also outlines that French public schools should teach children how to navigate online information. Critics have noted that it could jeopardise democracy and censor the press.[139]

Other Member States

Other member states have implemented a range of measures to tackle disinformation, including:

- Lithuania: implemented the *Law on Provision on Information to the Public,* making it illegal to spread disinformation and enabling the Radio and Television Commission to block channels spreading disinformation.[140] Lithuania has also implemented European Initiatives such as "Debunk.eu", that unites the media, society and the state to fight against disinformation;[141]
- Greece: established the website Ellinica Hoaxes in 2013 to debunk disinformation items;[142]

[135] Council of Europe, *Mapping of Media Literacy Practices and Actions in EU-28,* (2016), https://rm.coe.int/1680783500.
[136] Media & Learning, 'Early Years Education and Digital media in Denmark', (1 October 2020), https://media-and-learning.eu/type/featured-articles/early-years-education-and-digital-media-in-denmark/
[137] Media & Learning, 'Early Years Education and Digital media in Denmark', (1 October 2020), https://media-and-learning.eu/type/featured-articles/early-years-education-and-digital-media-in-denmark/
[138] Politico, 'French Parliament passes law against 'fake news'', (4 July 2018), *Politico* https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/
[139] Michael-Ross Fiorentino, 'France passes controversial 'fake news' law', (22 November 2018), *EuroNews* https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law
[140] Republic of Lithuania, Law on Provision of Information to the Public https://www.legislationline.org/download/id/5542/file/Lithaunia_law_provision_information_public_am2006_en.pdf
[141] https://debunk.eu
[142] Iva Plasilova et al., 'Study for the assessment of the implementation of the Code of Practice on Disinformation', (2020), *European Commission* https://digital-strategy.ec.europa.eu/en/library/study-assessment-implementation-code-practice-disinformation

- Sweden: In collaboration with researchers from Lund University, the Swedish Civil Contingencies Agency published a handbook describing different techniques used by malicious actors and the methods they can use to spread disinformation;[143]
- Latvia: implemented school workshops educating teachers and students how to differentiate fact from fiction;[144]
- Luxemburg: the BEE SECURE initiative includes *"Share Respect – Stop Online Hate Speech"*, within which files about false online information are published. The initiative also includes advice to parents on coping with their children's media consumption;[145]
- Cyprus: designed and implemented media literacy programs to educate high school students on how to recognise disinformation;
- Finland: invested in strengthening media literacy through partnerships between the schools and fact-checker agencies;[146]
- The Netherlands: launched a public awareness campaign aimed at informing people about disinformation.

Norway

In June 2021, in response to increasing concerns around the impact of social media on the Norwegian population's mental health and body image insecurity, the Norwegian Government passed legislation requiring content creators to disclose when they have retouched or added a filter to photos.[147]

United Kingdom

In the UK, there is increasing concern about online activity and harmful content. Technology firms have been accused of not addressing online abuse, with soccer clubs and other sporting authorities boycotting social media platforms in April 2021 to shine a spotlight on the increasing problem.[148] British schoolgirl Molly Russell's suicide in 2017

[143] Iva Plasilova et al., 'Study for the assessment of the implementation of the Code of Practice on Disinformation', (2020), *European Commission* https://digital-strategy.ec.europa.eu/en/library/study-assessment-implementation-code-practice-disinformation
[144] Latvian Academy of Culture, *Professional Development Conference for teachers* https://lka.edu.lv/en/international-cooperation/international-projects/nordplus-projects/film-and-media-education/professional-development-conference-teachers/?edit_off
[145] Iva Plasilova et al., 'Study for the assessment of the implementation of the Code of Practice on Disinformation', (2020), *European Commission* https://digital-strategy.ec.europa.eu/en/library/study-assessment-implementation-code-practice-disinformation
[146] Iva Plasilova et al., 'Study for the assessment of the implementation of the Code of Practice on Disinformation', (2020), *European Commission* https://digital-strategy.ec.europa.eu/en/library/study-assessment-implementation-code-practice-disinformation
[147] Vedtak til lov om endringer i markedsføringsloven mv. (merking av retusjert reklame) (Legislation amending the Swedish Marketing Practices Act) https://www.stortinget.no/globalassets/pdf/lovvedtak/2020-2021/vedtak-202021-146.pdf
[148] Michael Holden, 'UK unveils law to fine social media firms which fail to remove online abuse', (12 May 2021), *Reuters* https://www.reuters.com/technology/uk-unveils-law-fine-social-media-firms-which-fail-remove-online-abuse-2021-05-11/

after viewing graphic self-harm images on Instagram ignited the calls for regulation.[149] There have also been calls to enact 'David's law' to clamp down on social media abuse of public figures and end anonymity online after the murder of M.P. Sir David Amess in October 2021,[150] which followed on from significant online threats and abuse directed towards politicians in recent years,[151] including the murder of MP Jo Cox in 2016.[152] The proposed reforms to the regulation of social media and online safety take a similar approach to the European Union's proposals, looking simultaneously at human welfare and free speech, treating social media platforms as public environments, not as publishers.[153]

Online Harms and Online Safety

The UK Government released an *Online Harms White Paper* (the Paper) in April 2019, claiming that the existing patchwork of regulation and voluntary initiatives had not gone far or fast enough to keep online users safe. The Paper proposed a single regulatory framework to tackle the issue, which centres on a duty of care for internet companies, including social media platforms. Compliance with duty of care obligations was to be overseen and enforced by an independent regulator.[154] The Paper received a varied reaction, including concerns that harms were insufficiently defined and it may threaten freedom of expression.[155] The UK Government consulted on the White Paper, and subsequently a draft *Online Safety Bill* was included in the Queen's speech of 11 May 2021, and published the following day. A Joint Committee has been established to consider the draft legislation, with a report deadline of 10 December 2021.[156]

The draft Bill would impose duties of care on providers of online content-sharing platforms and search services, to address illegal content on their services. This illegal content includes terrorism offences, child sexual exploitation and abuse offences, offences directed at an individual as the victim, and offences set out in secondary legislation.[157] Companies within the scope of the legislation would need to take "robust action to tackle illegal abuse, including swift and effective action against hate crimes, harassment and threats directed at individuals and keep their promises to users about

[149] BBC News, 'Molly Russell social media material 'too difficult to look at', (26 September 2020), https://www.bbc.com/news/uk-england-london-54307976
[150] Jessica Elgot, 'PM urged to enact 'David's law' against social media abuse after Amess's death', (19 October 2021), *The Guardian* https://www.theguardian.com/uk-news/2021/oct/18/pm-urged-to-enact-davids-law-against-social-media-abuse-after-amesss-death
[151] Jennifer Scott, ' Can Online Safety Bill tackle social media abuse of MPs?', (20 October 2021), *BBC News* https://www.bbc.com/news/uk-politics-58958244
[152] BBC News, 'Labour MP Jo Cox 'murdered for political cause'', (14 November 2016), *BBC News* https://www.bbc.com/news/uk-37978582
[153] Parmy Olsen, 'The appeal of British efforts to keep social media under watch', (3 November 2021), *Mint* https://www.livemint.com/opinion/columns/the-appeal-of-british-efforts-to-keep-social-media-under-watch-11635872121309.html
[154] UK Government. (2020). *Fact sheet — Online Harms Full Government Response.* https://researchbriefings.files.parliament.uk/documents/CBP-8743/CBP-8743.pdf
[155] Claudine Tinsman, ' Will the government's online safety laws for social media come at the cost of free speech?', (24 December 2020), *The Conversation* https://theconversation.com/will-the-governments-online-safety-laws-for-social-media-come-at-the-cost-of-free-speech-152352
[156] UK Government. (2020). *Fact sheet — Online Harms Full Government Response.* https://researchbriefings.files.parliament.uk/documents/CBP-8743/CBP-8743.pdf
[157] Clause 41(3)(c) of the *Online Harms Bill*

their standards". The definition of harm would be that which may cause significant adverse physical or psychological impact on individuals.[158]

Ofcom, the UK's independent communications regulator would be appointed as the online harms regulator, their remit broadening to include setting codes of practice, establishing a transparency, trust and accountability framework, and requiring all in-scope companies to have effective and accessible mechanisms for users to report concerns. Ofcom's powers would include the ability to fine companies up to £18 million or 10% of annual global turnover (whichever is higher) and have the power to block access to sites if they are non-compliant. However, social media platforms will set their own definitions of risk assessment, which may lend itself to less diligent reporting.[159]

The proposed legislation has been heavily critiqued by civil liberties organisations, however it was welcomed by children's safety organisations.[160] Critique centres on freedom of expression and privacy concerns, including private messaging, legal but harmful content and journalistic material.[161]

Counter Terrorism

The *Counter-Terrorism and Border Security Act 2019* amended the *Terrorism Act 2000* in response to attacks in London and Manchester in 2017, including provisions related to online activity for individuals.[162] The legislation states it is an offense to view terrorist material over the Internet,[163] and individuals face up to 15 years in prison for viewing or accessing material that is useful or likely to be useful in preparing or committing a terrorist act, even if there is no demonstrated intent to commit such acts.[164] The legislation includes exceptions for journalists and academics accessing materials in the course of their work.[165] Critique of the legislation centres on threats to freedom of expression.

[158] Part 1 contains definitions of the services to which the Bill would apply.
Part 2 sets out the duties of care that would apply to providers of user-to-user and search services – i.e. duties to undertake risk assessments, and duties with regards to content that is illegal, harmful to children and harmful to adults; Part 4 sets out Ofcom's powers and duties, including duties to carry out risk assessments and to maintain a register of categories of services. Part 4 also establishes Ofcom's functions and powers with respect to the use of technology in relation to terrorism content and child sexual exploitation and abuse content, information-gathering, enforcement, research, and media literacy; Part 5 provides for the grounds and avenues for appeals against Ofcom's decisions, and for designated bodies to make super complaints.
[159] UK Government. (2020). *Fact sheet — Online Harms Full Government Response.* https://researchbriefings.files.parliament.uk/documents/CBP-8743/CBP-8743.pdf
[160] Alex Hern, 'Online safety bill 'a recipe for censorship', say campaigners', (13 May 2021), *The Guardian* https://www.theguardian.com/media/2021/may/12/uk-to-require-social-media-to-protect-democratically-important-content
[161] John Woodhouse, 'Regulating online harms', (12 August 2021), *House of Commons Library* https://researchbriefings.files.parliament.uk/documents/CBP-8743/CBP-8743.pdf; Heather Burns, 'Online harms plans threaten the future of freedom of expression', (15 December 2020), *Open Rights Group* https://www.openrightsgroup.org/blog/online-harms-freedom-of-expression-remains-under-threat/
[162] *Counter-Terrorism and Border Security Act 2019* https://bills.parliament.uk/bills/2255
[163] Amends s58 of the *Terrorism Act 2000*
[164] Chapter 2 – Punishment and management of terrorist offenders. S7-11 Sentencing
[165] Freedom House, *United Kingdom* https://freedomhouse.org/country/united-kingdom/freedom-net/2021

Prosecution of Digital Offences

The Crown Prosecution Service publishes guidelines for the prosecution of crimes committed by social media users.[166] The guidelines inform decisions on whether criminal charges should be pursued against individual social media users for a range of offences. These guidelines were updated in 2014 to include digital harassment offences committed under the *Sexual Offences Act 2003*. The guidelines were updated in 2016 to include more abusive online behaviours, including online harassment, trolling, threats, disclosure of sexual images without consent, grooming, stalking online, and online mobbing.[167] There have been recent calls for closer monitoring.

Cyberbullying

Cyberbullying is not explicitly covered by UK regulation, however, there are several acts under which it may be deemed a criminal offence. Under section 127 *Communications Act 2003,* it is an offence to send via any electronic communication network a message deemed grossly offensive or of an indecent or menacing manner.[168] Under section 1 of the *Malicious Communications Act 1988*[169] it is an offence to send communication that is indecent or grossly offensive, for the purpose of causing distress to the recipient. The Act encompasses threats and information which are false.

New Zealand

The evolution of social media has resulted in increasing potential for exposure to harmful content, explicitly evident by the livestreaming of the Christchurch terror attack. The existing New Zealand regulatory system was designed around analogue publication such as books and free-to-air TV, and does not have the capacity to respond to digital media types, including content made available online.[170] Further, the Christchurch Call, the international effort to curb violent extremism and terrorist content spread through tech companies' algorithms, was initiated by NZ Prime Minister Jacinda Ardern and French President Emmanuel Macron in May 2021.

Harmful Content

A comprehensive review of content regulation was announced by the Hon Jan Tinetti, Minister of Internal Affairs, on 10 June 2021, to design and create a modern, flexible and coherent regulatory framework to mitigate the harmful impacts of content. Content includes any publicly available communicated material (video, audio, images and text), regardless of how it is communicated. Specifically, harmful content ranges from child

[166] The Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/
[167] Crown Prosecution Service, *CPS publishes new social media guidance and launches Hate Crime consultation* (10 October 2016) https://web.archive.org/web/20161013201133/www.cps.gov.uk/news/latest_news/cps_publishes_new_social_media_guidance_and_launches_hate_crime_consultation/
[168] *Communications Act 2003* https://www.legislation.gov.uk/ukpga/2003/21/section/127
[169] *Malicious Communications Act 1988* https://www.legislation.gov.uk/ukpga/1988/27/section/1
[170] The Department of Internal Affairs, *The Content Regulatory System Review* https://www.dia.govt.nz/media-and-online-content-regulation

sexual exploitation material, adult content that children can access and violent extremist content.[171] The review has a broad scope, encompassing areas not covered by existing legislation such as misinformation and disinformation, in addition to broadcasting and advertising standards, the *Harmful Digital Communications Act*, the classification system and Chief Censor's office. The consultation is twofold, with targeted stakeholder engagement in mid-to-late 2021, and public consultation anticipated for early 2022.[172]

The *Harmful Digital Communications Act 2015* assists people dealing with serious or repeated harmful digital communications and provides 10 communication principles that guide how to communicate online. The Act covers any harmful digital communications which include racist, sexist and religiously intolerant comments, cyberbullying and comments about disabilities or sexual orientation.[173] Netsafe has responsibility to resolve reports on alleged breaches, however they are not an enforcement agency. The District Court handles cases of harmful digital communications that Netsafe has not been able to resolve. Criminal penalties include a fine of up to $50,000 for an individual or up to $200,000 for a body corporate, or up to two years jail for posting or sending a digital communication with intent to cause harm.[174]

Canada

Prime Minister Justin Trudeau secured a third election victory in September 2021 after calling a snap election, resulting in a minority government and necessitating a negotiated position with smaller parties to govern and pass legislation.[175] The dissolution of Parliament on 15 August 2021, which paved the way for the snap election, put a pause on several Bills to regulate social media platforms, that were considered both ambitious and controversial.[176] As the Government commences its third term, and as a minority government, the Canadian regulatory space will likely change.

---

[171] The Department of Internal Affairs, *The Content Regulatory System Review* https://www.dia.govt.nz/media-and-online-content-regulation; Hon Jan Tinetti, *Govt acts to protect NZers from harmful content* (10 June 2021) https://www.beehive.govt.nz/release/govt-acts-protect-nzers-harmful-content; Hon Jan Tinetti Proactive release of Cabinet material about the initiation of the media content regulatory review (2 July 2021) https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/Cabinet-material-about-the-initiation-of-the-media-content-regulatory-review.pdf

[172] The Department of Internal Affairs, *The Content Regulatory System Review* https://www.dia.govt.nz/media-and-online-content-regulation; Hon Jan Tinetti, *Govt acts to protect NZers from harmful content* (10 June 2021) https://www.beehive.govt.nz/release/govt-acts-protect-nzers-harmful-content; Hon Jan Tinetti Proactive release of Cabinet material about the initiation of the media content regulatory review (2 July 2021) https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/Cabinet-material-about-the-initiation-of-the-media-content-regulatory-review.pdf

[173] Harmful Digital Communications Act 2015 https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html; https://www.netsafe.org.nz/what-is-the-hdca/

[174] Netsafe, 'What is the NDCA?', (1 September 2021), *Netsafe* https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html; https://www.netsafe.org.nz/what-is-the-hdca/

[175] Leylan Cecco, 'Justin Trudeau secures a third victory in an election 'nobody wanted'', (22 September 2021), *The Guardian* https://www.theguardian.com/world/2021/sep/21/justin-trudeau-wins-third-election-victory

[176] Blayne Haggart & Natasha Tusikov, 'Resetting the Debate on Regulating Social Media: Part One', (8 September 2021), *Centre for International Governance Innovation* https://www.cigionline.org/articles/resetting-the-debate-on-regulating-social-media/

Proposed Legislation

The Canadian Government's proposed legislative and regulatory framework creates rules for how social media platforms and other online services must address harmful content.[177] The framework sets out: the entities subject to the new rules; the types of harmful content that would be regulated; new rules and obligations for regulated entities; and two new regulatory bodies and an Advisory Board to administer and oversee the new framework and enforce its rules and obligations.[178] The legislative framework would apply to online communication service providers, which is intended to capture major platforms such as Facebook, Twitter and YouTube, and exclude products and services such as fitness applications or travel review websites. Further, the legislation would target five categories of harmful content: terrorist content, content that incites violence, hate speech, non-consensual sharing of intimate images, and child sexual exploitation content.

While the definitions would draw on existing law, they would be modified to tailor them to a regulatory context. Obligations in the legislation would require regulated entities to do whatever is reasonable and within their power to monitor for harmful content on their platforms, including through automated systems based on algorithms. Once platform users flag content, regulated entities would have to respond by assessing whether it should be made inaccessible in Canada, and if the content meets the legislated definitions, the entity would have to make the content inaccessible within 24 hours.[179]

The Government presented a discussion guide summarising the approach and a technical paper proposing instructions to inform the legislation for public consultation. Consultation closed on 25 September 2021, and no further information on the "proposed approached" is yet available.

In addition, several proposed Bills were introduced in the 43rd Canadian Parliament, 2nd Session, which ended in August 2021, and were not passed before the election was called. They will need to be reintroduced by the new government, and it is likely they will be amended in some capacity.[180] Bill C-36 proposes amendments to several Canadian laws, including the *Canadian Human Rights Act* to make it a discriminatory practice to communicate (or cause the communication of) hate speech on the internet where the hate speech is likely to encourage the vilification of an individual or group of individuals on a prohibited ground of discrimination.[181] The Bill would make online hate speech punishable by a fine of up to $700,000 Canadian dollars, and imprisonment. The Bill was read in Parliament in June 2021 and has not yet been passed.[182] The Bill is intended to

[177] Government of Canada, *Consultation closed: The Government's proposed approach to address harmful content online* https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html
[178] Government of Canada, *Consultation closed: The Government's proposed approach to address harmful content online* https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html
[179] Government of Canada, *Discussion guide* https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html
[180] Bill C-36, An Act to amend the Criminal Code and the Canadian Human Rights Act https://openparliament.ca/bills/43-2/https://openparliament.ca/bills/43-2/C-36/; Bills for the 43rd Parliament, 2nd Session https://openparliament.ca/bills/43-2/
[181] Bill C-36 First Reading https://parl.ca/DocumentViewer/en/43-2/bill/C-36/first-reading#ID1RB
[182] Bill C-36, An Act to amend the Criminal Code and the Canadian Human Rights Act https://openparliament.ca/bills/43-2/C-36/

complement the proposed legislation on combatting online harms.[183] There have been concerns voiced regarding censorship and the government's authority to determine what is hate speech.[184]

Another proposed piece of legislation is Bill C-10, an Act to amend the *Broadcasting Act*. The Bill passed the House of Commons but did not receive Senate endorsement before the election was called. The proposed legislation would allow the federal government to regulate video content on social media the same way it regulates national broadcasting, through the Canadian Radio-television and Telecommunications Commission, protecting domestic cultural industries as Canadians turn to internet platforms for music and videos.[185] This would regulate social media platforms by requiring them to provide information, pay Canadian content contributions and put in place discoverability of Canadian content rules. This proposed legislation was controversial, as some considered that it would implement censorship of social media and control the content Canadians view.[186]

Bill C-11 would enact the *Consumer Privacy Protection Act*, which would update Canadian privacy legislation to address online activities, by protecting the personal information of individuals while recognising the need of organisations to collect, use or disclose personal information in the course of commercial activities.[187] This Bill was first read in November 2020, however did not reach committee study.[188]

Electoral Integrity

In the lead-up to the 2019 Canadian federal election,[189] the Canadian Government released the *Canada Declaration on Electoral Integrity Online*.[190] The non-binding declaration establishes a set of common commitments with online platforms to safeguard federal elections from malicious interference and build a healthier online

[183] Dale Smith, 'Here's what died on the order paper', (17 August 2021), *National Magazine* https://nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2021/here-s-what-died-on-the-order-paper
[184] Standing for Freedom Center Staff, 'Canada proposes another 'hate speech' law and this one is just as threatening to free speech', (28 June 2021), *Standing for Freedom* https://www.standingforfreedom.com/2021/06/28/canada-proposes-another-hate-speech-law-and-this-one-is-just-as-threatening-to-free-speech/
[185] Bill C-10, An Act to amend the Broadcasting Act and to make related and consequential amendments to other Acts https://parl.ca/DocumentViewer/en/43-2/bill/C-10/third-reading
[186] Dale Smith, 'Here's what died on the order paper', (17 August 2021), *National Magazine* https://nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2021/here-s-what-died-on-the-order-paper; Timothy Gindi, Marty Rabinovitch & Angela Papeo, 'Canada: Bill C-10: The Future of Regulated Canadian Content' (22 October 2021) *Mondaq* https://www.mondaq.com/canada/social-media/1118340/bill-c-10-the-future-of-regulated-canadian-content
[187] Bill C-11 First Reading https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading
[188] Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts https://www.parl.ca/LegisInfo/en/bill/43-2/C-11
[189] Further in the electoral space, *The Elections Modernization Act* (Bill C-76) received Royal Assent in December 2018. The legislation prohibits the use of foreign funds by third parties for partisan advertising and activities. It heightens transparency measures and clarifies offences related to false statements and foreign interference. https://www.canada.ca/en/democratic-institutions/news/2019/01/combatting-foreign-interference.html
[190] Government of Canada, *Canada Declaration on Electoral Integrity Online (2021)* https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/declaration-electoral-integrity.html.

ecosystem. The declaration contains initiatives aimed at enhancing integrity, transparency and authenticity which include assisting users to better understand the sources of information they are viewing; removing fake accounts and inauthentic content on their platforms; and ensuring transparency for regulated political advertising.[191] The declaration was updated on 11 August 2021 to include a clearer focus on inauthentic behaviour online, providing further protection of free expression. Facebook, Google, Microsoft, Twitter and TikTok have endorsed the Declaration.[192]

China

China has one of the world's most restrictive media environments, utilising censorship to regulate and control information online, in the news and on social media. Chinese authorities blocked platforms including Facebook, Twitter and Google in July 2009 following riots in Xinjiang, to restrict communication among independence activists.[193] Commonly referred to as the 'Great Firewall', various methods are utilised to control online expression, including blocking websites, filtering keywords and censoring social media. In 2014 the Cyberspace Administration of China was established as the main body to censor the internet in China.[194]

At the same time, China has the world's largest social media market, with an estimated 927 million users in 2020.[195] While many foreign social media companies are prohibited, Chinese companies are flourishing and include platforms such as Weibo, WeChat and Baidu.[196] Further, despite the ban, there are several ways to access blocked platforms in China, through virtual private networks (VPN) and proxy websites.[197]

Chinese platforms have evolved significantly into 'super apps', to encompass more of what people do online. For example, WeChat facilitates life online, and allows you to message friends, see updates in their feed, as well as take out loans, shop and arrange food delivery. It is anticipated that the major social networks such as Facebook will become super apps and will become increasingly important ways for people to stay connected, bank, shop and entertain themselves.[198]

---

[191] Joan Bryden, 'Several tech giants sign onto Canadian declaration on electoral integrity', (27 May 2019), *Global News Canada* https://globalnews.ca/news/5323084/tech-giants-electoral-integrity/.
[192] Government of Canada, *The Government of Canada updates the Canada Declaration on Electoral Integrity Online* (2021) https://www.canada.ca/en/democratic-institutions/news/2021/08/the-government-of-canada-updatesthe-canada-declaration-on-electoral-integrity-online.html
[193] Techcrucnh, 'China blocks access to Twitter, Facebook after riots', (7 July 2009), *Techcrunch* https://techcrunch.com/2009/07/07/china-blocks-access-to-twitter-facebook-after-riots/
[194] KPMG China, *Overview of China's Cybersecurity Law* (2017) https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf
[195] Statista, *Number of social network users in China from 2017 to 2020 with a forecast until 2016* (2021) https://www.statista.com/statistics/277586/number-of-social-network-users-in-china/
[196] Christina Lu, 'China's social media explosion' (11 November 2021), *Foreign Policy* https://foreignpolicy.com/2021/11/11/china-social-media-tech-linkedin-wechat-censorship-privacy-regulation/
[197] Sam Gaskin, 'A guide to digital security for reporters in Asia', (4 October 2019), *Asia Media Centre* https://www.asiamediacentre.org.nz/features/a-guide-to-digital-security-for-reporters-in-asia/
[198] Alex Health, 'The rise of the super app', (1 November 2021), *The Verge* https://www.theverge.com/22738395/social-media-super-app-facebook-wechat-shopping

Data protection and privacy

The rhetoric within China is that the prohibition of platforms such as Facebook, Twitter, and YouTube is critical to the protection of citizen's user data, as these platforms aggregate vast amounts of data on their users, which is stored and used. An archived article from MingPao News claims that Facebook is used as a channel for Western Intelligence services to subvert other countries' regimes.[199] Yin Yungong, the Director of News at the Chinese Academy of Social Services, has stated that while Chinese citizens love to engage in politics and discussions, there are issues on banned platforms (such as cyberbullying), from which Chinese citizens are being protected. Discussion also centres on how Facebook, Twitter, and Google threaten China's interests and Chinese customers' interests, with Facebook and Twitter considered especially dangerous as they have capacity to disseminate disinformation fast. Facebook's participation in spreading information on the Arab Spring has been used as a critical argument.[200]

Under China's new *Personal Information Protection Law*, which was announced in August 2021, and came into force on 1 November 2021, users are afforded greater protections from tech companies. The law contains provisions requiring any organisation or individual handling Chinese citizens' personal data to obtain prior consent and minimise data collection.[201] The Chinese Government is expected to maintain broad access to the data. The framework comes in response to frustration in the government and Chinese society over online fraud, data theft and data collection by domestic technology giants. Previously, loose rules on data access allowed companies to develop new products and technology quickly, while simultaneously also stimulating a black market for consumer data. The new legislation unifies previously piecemeal law on personal information and protection, in addition to addressing increasingly pertinent issues such as the proliferation of facial recognition, and algorithmic discrimination.[202]

Social media addiction in children

TikTok (DouYin in China) has implemented rules regarding access to the app for children under 15 years old in response to gaming and media addiction in young people. Children can only use DouYin for 40 minutes a day, between 6 am to 10 pm. The content available is carefully curated, and consists of science experiments, museums and gallery

[199] MingPao News, *Chinese Academy of Social Sciences: Facebook becomes a destructive tool* (translated from '社科院：Facebook成顛覆工'), (8 July 2010), https://web.archive.org/web/20100711170314/http://hk.news.yahoo.com/article/100707/4/j1ol.html

[200] Tang QiWei, 'Chinese officials made it clear that Facebook will not be allowed to enter Chinese market' (translated from '中国官员明确表态不允许FACEBOOK进入中国市场'), (12 September 2014), *Radio Free Asia*, https://www.rfa.org/mandarin/yataibaodao/meiti/vt-09122014132912.html

[201] Christina Lu, 'China's social media explosion' (11 November 2021), *Foreign Policy* https://foreignpolicy.com/2021/11/11/china-social-media-tech-linkedin-wechat-censorship-privacy-regulation/

[202] Eva Xiao, 'China passes one on the world's strictest data-privacy laws', (20 August 2021), *The Wall street Journal* https://www.wsj.com/articles/china-passes-one-of-the-worlds-strictest-data-privacy-laws-11629429138; Li Yuan, 'Personal-privacy concerns grup China', (31 August 2016), *The Wall Street Journal* https://www.wsj.com/articles/personal-privacy-concerns-grip-china-1472665341?mod=article_inline

exhibitions, and historical knowledge of China.[203] While proof of age is not required upon registration, parents are advised to help children register their age in the app.

Singapore

Singapore's approach to social media regulation can be characterised as cautious and paternalistic.[204] It has been criticised for curbing free speech and stifling political dissent.[205] To better understand the Singapore context, the People's Action Party (PAP) has lead Singapore's parliamentary system since independence in the 1960s. The government allows for some political pluralism; however, it limits freedoms of expression, assembly, and association and restrains the growth of credible opposition parties.[206]

Protection from Online Falsehoods

In response to the spread of deliberate online falsehoods, the *Protection from Online Falsehoods and Manipulation Act* (POFMA), known colloquially as Fake News Law, was passed in the Singapore Parliament on 8 May 2019, and came into effect on 2 October 2019.[207] POFMA's purpose is to prevent the communication of false statements and enable measures to counteract effects of this communication, to suppress the financing and promotion of online locations communicating these statements and to enable measures to detect and control this behaviour.[208] Under the legislation, falsehoods are defined as statements of fact that are false or misleading,[209] and these are determined by POFMA ministers. These false statements are considered particularly serious to the public interest if they are prejudicial to the security and bilateral relations of Singapore or if they incite feelings of hatred between different groups.[210] Individuals in breach of POFMA can be liable for fines up to $50,000 Singapore dollars and/or imprisonment of up to 5 years, and companies can be liable for up to $1 million Singapore dollars.[211]

---

[203] TengXun Net, 'DouYin pushes the strictest youth protection rules in history. Daily usage limited to 40 minutes' (translated from'抖音推史上最严青少年保护措施 每天只能用40分钟'), (19 September 2021), *TengXun Net* https://new.qq.com/rain/a/20210919a0ckqc00)

[204] Jing Yi Tay, 'No news is good news, but "fake news" is bad news: A comparative analysis of Singapore's and Australia's measures to combat misinformation on social media', (2021) 33(2) *Singapore Academy of Law Journal*, 600–624

[205] Agence France-Presse, 'Singapore passes foreign interference law allowing authorities to block internet content', (5 October 2021), *The Guardian* https://www.theguardian.com/world/2021/oct/05/singapore-passes-foreign-interference-law-allowing-authorities-to-block-internet-content

[206] Freedom House, *Singapore* https://freedomhouse.org/country/singapore/freedom-net/2021

[207] *Protection from Online Falsehoods and Manipulation Act* 2019 https://sso.agc.gov.sg/Act/POFMA2019?TransactionDate=20191001235959; Tan Zhi Han, 'Protection from Online Falsehoods and Manipulation Act (POFMA): Regulating Fake News to Maintain Public Trust in Singapore' *Honrad Adenauer Stiftung* https://www.kas.de/documents/288143/11133938/Panorama_Trust_TanZhiHan.pdf/898f786c-229e-b2c6-a4d3-1b1e22128035?t=1608692256696

[208] *Protection from Online Falsehoods and Manipulation Act* 2019, s5

[209] *Protection from Online Falsehoods and Manipulation Act 2019*, s2(2)(b)

[210] *Protection from Online Falsehoods and Manipulation Act 2019*, s4

[211] Taylor Vinters, *5 things you need to know about Singapore's controversial new fake news law* https://www.taylorvinters.com/article/5-things-you-need-to-know-about-singapores-controversial-new-fake-news-law; Tech Law for Everyone, *POFMA: Singapore's anti-fake news law* https://www.scl.org/articles/10541-pofma-singapore-s-anti-fake-news-law; *Protection from Online Falsehoods and Manipulation Act* https://www.mlaw.gov.sg/files/news/others/POFMABrochure.pdf

Critiques of this approach centre on how the law gives authorities excessive and broad powers to crack down on dissenting political views, with the first POFMA actions issued against individuals affiliated with the opposition political party.[212] This legislation is significant to the greater region, as the Asian headquarters of Facebook and Twitter are both located in Singapore.[213] Other countries, such as Sri Lanka, have implemented similar laws to control misleading and false statements online.[214]

Foreign Interference

The *Foreign Interference (Countermeasures) Act* (FICA) was passed in the Singapore Parliament on 4 October 2021, and seeks to prevent, detect and disrupt the use of hostile information campaigns and local proxies by foreign entities intending to interfere in domestic politics.[215] FICA allows authorities to compel internet, social media service platforms and website operators to provide user information,[216] block content,[217] and remove applications if the information is harmful and is suspected as being carried out by foreign actors. People deemed "politically significant persons" under the law will have to comply with strict rules relating to donations[218] and declare their links to foreign affiliations.[219] Instead of a court, an independent tribunal chaired by a judge will hear appeals against government minister's decisions.[220] The legislation does not apply to citizens airing their political opinions (unless they are agents of a foreign principal as defined in the Act), and it does not apply to foreign individuals and publications commenting and reporting on Singapore politics, even if the comments may be critical of the government.[221]

Critics note that because the law is vague and broadly worded it could be used to silence government critics. It also followed just weeks after independent media site The Online Citizen (a site for alternative political views) was shut down over alleged failures to identify its funding sources. This raised concerns that Singapore authorities are strengthening efforts to enforce greater state control over its citizens.[222]

---

[212] Amnesty International, *Singapore: Social media companies forced to cooperate with abusive fake news law* (19 February 2020) https://www.amnesty.org/en/latest/news/2020/02/singapore-social-media-abusive-fake-news-law/; https://sso.agc.gov.sg/Acts-Supp/18-2019
[213] Ashley Westerman, 'Fake News' Law Goes Into Effect In Singapore, Worrying Free Speech Advocates', (2 October 2019), *NPR* https://www.npr.org/2019/10/02/766399689/fake-news-law-goes-into-effect-in-singapore-worrying-free-speech-advocates.
[214] Shreetesh Angwalkar, 'Sri Lanka Implements Singapore Style Law to Control Fake News', (23 April 2021), *Spherex* https://www.spherex.com/regulation/sri-lanka-implements-singapore-style-law-to-control-fake-news
[215] *Foreign Interference (Countermeasures) Act 2021* https://www.parliament.gov.sg/docs/default-source/default-document-library/foreign-interference-(countermeasures)-bill-24-2021.pdf
[216] *Foreign Interference (Countermeasures) Act*, s108
[217] *Foreign Interference (Countermeasures) Act*, s33
[218] *Foreign Interference (Countermeasures) Act,* Part 5, Division 3
[219] *Foreign Interference (Countermeasures) Act,* Part 6, Division 1
[220] *Foreign Interference (Countermeasures) Act,* Part 8, Division 2
[221] Philip J. Heijmas, 'Singapore Proposes Law Combating Foreign Interference Online', (13 September 2021), https://time.com/6097362/singapore-online-foreign-interference-bill/; PR Week Staff, 'Singapore's new foreign interference law could impact social media, publishers', (6 October 2021), *PR Week* https://www.prweek.com/article/1729525/singapores-new-foreign-interference-law-impact-social-media-publishers
[222] Amnesty International, *Singapore: Foreign interference law is a tool for crushing dissent*

India

India is the largest market of users of Facebook and WhatsApp.[223] India has become increasingly less accommodating toward big tech companies, driven by a rise in India's homegrown platforms such as Reliance Jio, a rapid spread of misinformation on platforms, and the government's desire to have a greater level of control over social media.[224] In July 2018, villagers in a rural Indian town beat five strangers to death over a rumour circulated on WhatsApp that the men had kidnapped children.[225] On 29 June 2020 India banned 59 apps developed by Chinese firms, including TikTok, over concerns that these apps were engaging in activities that threatened the "national security and defence of India, which ultimately impinges upon the sovereignty and integrity of India".[226] In February 2021, India ordered Twitter to remove more than 1100 accounts and posts it alleged spread misinformation about farmers protesting agricultural reforms. The Indian government rebuked Twitter for not fully complying with the government order.[227]

These are some of the events that have led to sweeping reforms to hold social media companies, streaming platforms and digital news publishers to account under direct government oversight. The legally enforceable *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021* targets misinformation and hate speech. The rules require social media companies to establish a grievance redressal mechanism, obliges platforms to remove content within 36 hours of receiving a legal order, and requires them to disable any post depicting an individual in a sexual act or conduct. Critics note that these rules were introduced and implemented without public consultation and may lead to outright censorship. Further, the rules may undermine user

(5 October 2021) https://www.amnesty.org/en/latest/news/2021/10/singapore-foreign-interference-law-dissent/ ; Human Rights Watch, *Singapore: Withdraw Foreign Interference (Countermeasures) Bill* https://www.hrw.org/news/2021/10/13/singapore-withdraw-foreign-interference-countermeasures-bill ; Agence France-Presse, "Chilling': Singapore's 'fake news' law comes into effect' (2 October 2019), *The Guardian* https://www.theguardian.com/world/2019/oct/02/chilling-singapores-fake-news-law-comes-into-effect

[223] Sankalp Phartiyal & Aditya Kalra, 'India tightens regulatory grip on Facebook, WhatsApp with new rules' (25 February 2021), *Reuters* https://www.reuters.com/article/india-tech-regulation-idUSKBN2AP175

[224] Saheli Roy Choudhury, 'India wants to cut Big Tech down to size. Critics say the new rules may give the state too much power' (20 April 2021) *CNBC* https://www.cnbc.com/2021/04/20/indias-social-media-law-puts-big-techs-power-into-states-hands-critics-say.html; Sarah Frier, Naomi Nix & Sarah Kopit, 'How and why internet companies moderate speech online' (25 October 2-2021), *The Washington Post* https://www.washingtonpost.com/enterprise/how-and-why-internet-companies-moderate-speech-online/2021/10/21/e4c87baa-3293-11ec-8036-7db255bff176_story.html?utm_source=rss&utm_medium=referral&utm_campaign=wp_business

[225] Pranav Dixit & Ryan Mac, 'How WhatsApp destroyed a village' (9 September 2018), *Buzzfeed News* https://www.buzzfeednews.com/article/pranavdixit/whatsapp-destroyed-village-lynchings-rainpada-india

[226] Government of India, *Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order* (29 June 2020) https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206; Manish Singh, 'Facebook, Twitter, WhatsApp face tougher rules in India', (25 February 2021), *Techcrunch* https://techcrunch.com/2021/02/25/india-announces-sweeping-guidelines-for-social-media-on-demand-streaming-firms-and-digital-news-outlets/

[227] Saheli Roy Choudhury, ' India rebukes Twitter for not fully complying with government order to ban certain accounts', (11 February 2021), *CNBC* https://www.cnbc.com/2021/02/11/india-rebukes-twitter-for-not-fully-complying-with-government-order.html

rights such as end-to-end encryption, and some consider that the Indian Government does not have the capacity to effectively enforce the rules.[228]

[228] Saheli Roy Choudhury, 'India wants to cut Big Tech down to size. Critics say the new rules may give the state too much power', (20 April 2021), *CNBC* https://www.cnbc.com/2021/04/20/indias-social-media-law-puts-big-techs-power-into-states-hands-critics-say.html;

Conclusion

Across jurisdictions there is significant debate about the role of social media and how best to regulate it. Growing concern over the negative impact of social media engagement on individuals and on social cohesion has created a consensus on the need for better regulations. However approaches have differed and many regulatory frameworks are still under construction or in consultation phase.

This paper has provided an overview of the different approaches adopted by countries around the world and the different contexts in which these responses have been implemented. The diversity of approaches outlined can be used to inform consideration of what can be adapted and adopted for regulation in the Australian context.

Targeted, holistic and effective regulation is needed to counteract the negative effects of social media on mental health and wellbeing and its threats to social cohesion. The impact of algorithmic culture is profound, and the solutions must go beyond regulation and into social policy spheres. As we race towards web 3.0, new forms of encrypted communications, the creation of the metaverse and quantum computing, the ability of regulators to keep pace and ensure a balance between public safety and civil liberties will present enormous challenges.