

**CENTRE FOR MEDIA TRANSITION**

Regulatory approaches to misinformation and disinformation in the Asia–Pacific region

Background paper, 23 February 2022

Prepared for the Solomon Islands Law Reform Commission

## About the Centre for Media Transition

The Centre (CMT) was established in 2017 as an applied research unit based at the University of Technology Sydney (UTS). It is an interdisciplinary initiative of the Faculty of Arts and Social Sciences and the Faculty of Law, sitting at the intersection of media, journalism, technology, ethics, regulation and business.

Working with industry, academia, government and others, the CMT aims to understand media transition and digital disruption, with a view to recommending legal reform and other measures that promote the public interest. In addition, the CMT aims to assist news media to adapt for a digital environment, including by identifying potentially sustainable business models, develop suitable ethical and regulatory frameworks for a fast-changing digital ecosystem, foster quality journalism, and develop a diverse media environment that embraces local/regional, international and transnational issues and debate.

This paper was prepared by:

* Dr Michael Davis, Research Fellow, Centre for Media Transition

**CONTACT**

Centre for Media Transition  
Faculty of Law, University of Technology Sydney  
Building 2, Level 15   
UTS City Campus, Broadway  
PO Box 123, Broadway NSW 2007

cmt@uts.edu.au  
+61 2 9514 9669

[cmt.uts.edu.au](mailto:CMT@uts.edu.au)

## Introduction

Recent years have seen clear movement towards the regulation of online misinformation and disinformation. The first substantial effort to regulate came in the EU, following growing evidence of Russian disinformation campaigns, the rise of monetised fake news during the US 2016 election, and the European elections that same year. The EU Code on Disinformation was launched in 2018.

Moves to regulate have since gathered pace in other jurisdictions, with the pandemic-related surge in misinformation driving many regulatory efforts, alongside increasing evidence of foreign interference and influence in local politics. Such efforts include the Australian Code of Practice on Disinformation and Misinformation (ACPDM), launched in February 2021, the ongoing consideration of the Online Safety Bill in the UK Parliament and the launch of a strengthened EU code in June 2022. Other countries have also introduced or are considering legislation.

Regulatory approaches differ markedly, and efforts to address mis- and disinformation generally sit alongside existing media law. Several jurisdictions in the Asia–Pacific region have laws that regulate misinformation in traditional, offline media.

The purpose of this paper is to provide an overview of regulatory approaches to misinformation and disinformation, with a focus on the Asia–Pacific and, for comparison, on recent developments in Europe and the Americas. While all efforts have been made to ensure accuracy, the paper is not intended to be exhaustive.

### Definitions

Prior to the introduction of the [European approach to tackling online disinformation](https://digital-strategy.ec.europa.eu/en/library/communication-tackling-online-disinformation-european-approach) in 2018, there was no common conceptual framework for defining various types of information disorder, with a variety of terms in common use, including fake or false news, misinformation, disinformation, propaganda, influence operations, information warfare, to name several.

Under the auspices of the Council of Europe, Clare Wardle and Hossein Derakhshan[[1]](#footnote-1) developed a conceptual framework that would go on to underpin the European approach, including the 2018 European Code of Practice on Disinformation. This introduced the term ‘information disorder’ to cover a trio of related phenomena: misinformation, disinformation and malinformation.

* Misinformation is false or misleading information that is not intended to harm or deceive.
* Disinformation is false or misleading information that is intended to harm or deceive.
* Malinformation is true information that is spread with the intention to harm.

The distinctions between these phenomena are best illustrated by the following Venn diagram:[[2]](#footnote-2)

**INFORMATION DISORDER**

**Misinformation**

**Malinformation**

**Disinformation**

**FALSE**

**INTENTIONAL**

While it has both practical and conceptual limitations, this framework provides relatively clear terminology that has informed policy and regulatory developments around the world and in many cases entered media and popular discourse.

### Regulatory approaches and trends

Regulation of information disorder, like all government oversight of media and public speech, is a politically fraught area of policy. In democratic countries, the balance tends towards a hands-off approach for fear of encroaching on foundational principles of media freedom and freedom of expression. Self-regulatory and co-regulatory approaches are often favoured over black-letter law or direct regulation. In most jurisdictions, it is not illegal merely to propagate false information.

For the same reason, the recent moves towards digital-platform regulation in this area have been largely aimed at increasing industry accountability and transparency through industry codes of conduct rather than setting out explicit rules relating to, for example, content moderation. Where there are restrictions or positive obligations on platform conduct, developing regulation has focused on the question of harm rather than of truth or falsity.

The importance of balancing liberal democratic principles with objectives of reducing harms arising from misinformation and disinformation is in large part what makes information disorder what is sometimes called a ‘wicked’ problem. A wicked problem is one whose complexity is such that it cannot be solved but only mitigated, with all attempts at a solution being either politically or socially untenable or merely producing further problems to solve.[[3]](#footnote-3) Even leaving these principles aside barely reduces the complexity of the problem. This can be seen in the case of archetypically illegal content such as child pornography, which remains intractable despite concerns for personal liberty playing no role.

In some jurisdictions, where liberal democratic institutions are weaker, there is less compunction about limiting citizen speech or press freedom. This can make room for direct regulatory approaches. At the same time, jurisdictional issues arise with digital platforms that are typically run by multinational companies, and perceptions of arbitrariness over the enforcement of speech regulation can undermine trust in regulatory authority.

## Comparative regulation

### The European Union

#### Background

The voluntary, self-regulatory EU Code of Practice on Disinformation was released in October 2018 with major platforms Google, Facebook, Twitter and Mozilla signing up, and later, Microsoft and Tiktok. Several advertising industry groups also joined.

The 2018 code was restricted to disinformation, with misinformation excluded ostensibly to protect freedom of expression.

After a lengthy consultation, a revised code was released in July 2022 to address substantial criticisms of the 2018 code. These included that it lacked concrete commitments and mechanisms for measuring signatory performance against the code. This was borne out by signatories’ transparency reports, which were criticised for being very high level and lacking in performance data.[[4]](#footnote-4)

While the 2018 code fell short of the European Commission’s (EC) ambitions, it was a first step towards industry regulation to address online information disorder and provided a model for subsequent efforts including the Australian code.

#### Shift from self-regulation to co-regulation

In December 2020 the European Commission released its European Democracy Action Plan, outlining an intention to move towards a co- regulatory framework to address disinformation.[[5]](#footnote-5)

The Digital Services Act, which came into force on 16 November 2022, includes a co-regulatory scheme for ‘very large’ online platforms (those reaching more than 10% of the EU population—i.e. currently around 45 million people) that would enforce compliance with industry codes of conduct, including the EU disinformation code. The scheme would require annual independent audits and allow fines to be imposed for breaches.

As part of the Democracy Action Plan the EU has also proposed legislation to improve the transparency of political advertising on digital platforms. As well as requiring greater transparency, the proposal would limit the use of personal data to target political advertising at EU citizens.

#### The revised code

Industry released a revised code on 16 June 2022. The strengthened code sets much higher standards for comprehensiveness, accountability and transparency than the 2018 code. The scope of the code is broader, covering misinformation, information influence operations and foreign interference in the information space as elements of ‘disinformation’, as well as disinformation more narrowly conceived.

The code included commitments to introduce measures to address financial incentives to spread disinformation, increasing transparency of political advertising, and developing technological means to prioritise authentic and authoritative information.

Transparency commitments are much more detailed than in the 2018 code, with each commitment specifying qualitative and, where appropriate, quantitative KPIs to improve consistency and comparability of platform reporting.

### The United Kingdom

A bill to address online harms is currently under consideration by the UK parliament. This follows the 2019 release of the Online Harms White Paper. The Online Safety Bill takes a different approach to the self-regulatory schemes introduced in the EU and Australia, establishing a series of statutory duties of care for online platforms towards their users. These cover the gamut of online harms. Those particularly relevant to information disorder include duties to perform risk assessments relating to service design and operation, to include features to increase user control over harmful content, to use proportionate processes to ensure the importance of free political expression and journalistic expression is taken into account, and to publish transparency reports on their activities.

The bill also requires Ofcom, the UK communications and media regulator, to develop codes of practice for digital platforms to describe measures recommended for the purpose of complying with their statutory duties. Ofcom would also be granted a suite of enforcement options including information-gathering powers and the issuing of penalties and service-restriction orders.

The bill is currently under consideration by a committee of the House of Lords.

### United States

Much of the recent regulatory focus in the United States has focused on section 230 of the Communications Decency Act (47 U.S.C. § 230), which provides immunity from liability for third-party content to providers and users of interactive computer services. This includes immunity for distributing or making third-party content available online (47 U.S.C. § 230(c) (1)). It also includes immunity for moderating or restricting access to “objectionable” content, irrespective of whether the content is protected speech under the first amendment (47 U.S.C. § 230(c)(2)).

In effect, section 230(c)(2) means that digital platforms and websites can implement their own content-moderation policies and cannot in most cases be required to remove or moderate user-generated content. There are exceptions for material that violates copyright or federal sex-trafficking laws.

Calls to reform section 230 have come from both those seeking more-robust content moderation and those seeking to prevent platforms from removing or moderating content. In 2020 the US Department of Justice undertook a review of section 230 in response to an executive order from then- president Donald Trump. No legislative changes resulted from the review and the executive order was repealed by President Joe Biden on 21 May 2021.

At the state level, some US jurisdictions, including Texas and Florida, are considering laws to limit the ability of digital platforms to moderate user content.[[6]](#footnote-6)

In 2016 the US enacted legislation to address foreign interference and disinformation, but this was to establish government capability and is not directed at digital platforms.

### Canada

Canada has been undertaking consultation on a proposed online harms bill since a 2020 review of the country’s communication laws. Following public consultation in 2021, an advisory group was convened in 2022 to provide expert advice on legislative and regulatory design. The group advised the government in June 2022 to consider including disinformation in legislation on online safety, while being sure not to undermine fundamental rights enshrined in the Canadian Charter of Rights and Freedoms. The overall approach recommended by the group is to implement a risk-based framework underpinned by a formal duty for platforms to act responsibly.

## Asia–Pacific regulation

### Australia

#### Background

In December 2019, the Australian government asked major digital platforms to develop a voluntary, self-regulatory code of practice to address growing concerns about disinformation and the quality of online news. The independent media and communications regulator, the Australian Communications and Media Authority (ACMA) was appointed to oversee the development of the code and to report to government on its effectiveness.

In February 2021, following public consultation on a draft code, industry group DIGI released the Australian Code of Practice on Disinformation and Misinformation. Initial signatories were Google, Meta, Microsoft, Redbubble, Tiktok and Twitter, with Adobe and Apple joining soon after.

Consultation aimed at revising the code began in June 2022, and a revised code was launched in December 2022. This followed ACMA’s initial report to government on the code, which was released in March 2022. The report made a number of criticisms of the code. These included: a scope that was too narrow to effectively address all the harms arising from misinformation; inadequate reporting and transparency requirements; and inadequate frameworks for collaboration and ensuring consistency in risk assessment.

#### The code

Scope: The code includes misinformation but excludes some types of content (professional news, political advertising) and services (private messaging) associated with the dissemination of misinformation and disinformation. As a voluntary code, it is open to digital platforms to sign up to the code as they see fit.

The code includes commitments to address misinformation and disinformation on signatories’ online services; to counter financial incentives to propagate disinformation; to address inauthentic activity such as bots or sock-puppet accounts; to increase transparency of political and issues-based advertising; to provide users with tools to make informed choices about online content; and to support research and public awareness.

Enforcement: Some months after launching the code, DIGI introduced a code governance framework with independent input into both code oversight and evaluation of annual platform transparency reports. A complaints mechanism allows the public to lodge complaints where it is thought a platform is failing to comply with its code commitments.

#### Shift from self-regulation to co-regulation

In February 2023, the minister for communications announced that the government would introduce legislation to grant ACMA powers relating to disinformation and misinformation. These will include information-gathering powers, and powers to register and enforce industry codes, or to make standards where codes prove inadequate. It would also have a range of enforcement powers that are yet to be canvassed. This legislation will, if passed, essentially shift the scheme from self- to co-regulation, in harmony with existing broadcasting regulation.

Importantly, however, the minister has indicated that ACMA’s powers will be directed at addressing evidence of systemic problems, and will not extend to assessing the truth or falsity of individual statements or ‘items of content’. This differs from ACMA’s role in broadcasting, where it can assess a broadcaster’s compliance in particular cases with accuracy provisions in industry codes of practice.

Australia has no federal laws addressing truth in political advertising, though two internal jurisdictions (South Australia and the ACT) do have such laws. While there are no explicit protections for freedom of speech, the High Court has found that the Australian Constitution contains a limited, implied freedom of political communication.

### New Zealand

In New Zealand, non-profit online safety organisation Netsafe has led development of the voluntary Aotearoa New Zealand Code of Practice for Online Safety and Harms. The code was released on 25 July 2022 and will be administered by industry group NZTech. Signatories are Meta, Google, TikTok, Twitch and Twitter. The code aims to address a range of online harms, including disinformation and misinformation, by increasing platform accountability and transparency. It takes an outcomes-based, self-regulatory approach similar to the Australian code.

The New Zealand government commenced the Content Regulatory Review in June 2021 to examine harmful content as well as broader media reform. It is currently examining options for regulatory reform, with consultation on a new framework expected in mid-2023.

### Indonesia

Indonesia takes a more-robust approach to misinformation and disinformation than the countries previously discussed. In Indonesia, the spreading of false information or news that intentionally causes public disorder is illegal under the criminal code and those convicted can face prison sentences up to ten years. Spreading false information or news that causes unrest, or uncertain, exaggerated or incomplete information or news carries lower sentences. The use of the criminal code for policing misinformation has attracted significant criticism.[[7]](#footnote-7) The code is currently under review.

### Singapore

Singapore also has a robust approach.The Protection from Online Falsehoods and Manipulation Act (POFMA) was introduced in 2019 (Republic of Singapore, 2019). Under the Act, any minister can declare information to be “false or misleading” and force its publisher to apply a correction notice or remove the material if they believe the material to be against the public interest. Individuals face fines of up to S$50,000 and/or jail terms of up to five years. Non-individuals (such as internet companies) face up to S$1million in fines plus S$100,000 per day of non-compliance. International human rights groups have criticised POFMA as a threat to free speech. POFMA has been considered as a model for tackling online misinformation in other countries, such as Nigeria.[[8]](#footnote-8)

### Fiji

Fiji’s Online Safety Act was introduced in 2018 ostensibly to protect citizens from harms such as revenge porn and cyber-harassment. Although its wording is broad, the act addresses harms only to individuals. Nonetheless, the law raised concerns that it would be a back door to censorship in a country where the government has historically exercised some control over both state and private media.

The Media Industry Development Decree, introduced in 2010, established the Media Industry Development Authority to regulate traditional media organisations (i.e. not online public expression). Enforcement powers include fines and jail sentences for breaches of regulations prohibitions against material deemed to be against the public interest or order, against the national interest, or which creates communal discord. These provisions have attracted substantial criticism both inside and outside Fiji. The decree also sets out a code of ethics for media organisations that, aside from its obligatory nature, parallels best-practice codes seen in countries such as Australia.

### Papua New Guinea

Papua New Guinea has consitutional protections for freedom of speech, press, worship, movement and association. Since the onset of the Covid-10 pandemic, the PNG government has considered social-media regulation and has previously suggested that Facebook should be banned.

As with the introduction of the Media Industry Development Decree in Fiji, the PNG government has emphasised the need for the media to focus on national development and sought to improve media standards through stronger legislation. As in Fiji, critics have labelled this a guise for government media control.

On 5 February 2023, the PNG government proposed a new National Media Development Policy, which would impose licensing on journalists and media organisations and establish the hitherto self-regulatory PNG Media Council under legislation.

### Vanuatu

In 2021, the Vanuatu Government introduced the Cybercrime Act, ostensibly to combat cyberbullying, stalking and digital hate crimes. Enforcement measures are strong, but it carves out protections for free speech, the public good, and privacy (but not media) and requires judicial review of warrant applications.

The application of the legislation has been criticised, however, with the broad provisions allegedly being used to arrest and intimidate critics of the government.[[9]](#footnote-9)

1. C Wardle & H Derakhshan, *Information disorder: Toward an interdisciplinary framework for research and policymaking*, Council of Europe, 27 September 2017. [↑](#footnote-ref-1)
2. Based on ibid., p .20. [↑](#footnote-ref-2)
3. M Montgomery, *Disinformation as a wicked problem: Why we need co-regulatory frameworks,* Brookings Institution, 20 August 2020, <https://www.brookings.edu/research/disinformation-as-a-wicked-problem-why-we-need-co-regulatory-frameworks/> [↑](#footnote-ref-3)
4. J Pamment, *The EU Code of Practice on Disinforma- tion: Briefing note for the new EU Commission.*, Partnership for Countering Influence Operations: Policy Perspectives Series, Carnegie Endowment for International Peace. <https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187> [↑](#footnote-ref-4)
5. European Commission. *European Democracy Action Plan*, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN> [↑](#footnote-ref-5)
6. Knight First Amendment Institute. Netchoice, LLC v. Paxto, 2022. <https://knightcolumbia.org/cases/netchoice-llc-v-paxton?mc_cid=4b40d9f463> [↑](#footnote-ref-6)
7. Carson, A. (2021). *Fighting fake news: A study of online misinformation regulation in the Asia Pacific.* LaTrobe University. <https://www.latrobe.edu.au/__data/assets/pdf_file/0019/1203553/carson-fake-news.pdf> [↑](#footnote-ref-7)
8. Ibid. [↑](#footnote-ref-8)
9. Civicus. ‘Freedom of expression at risk as cybercrime legislation used to prosecute online critics in Vanuatu’ in *Civicus Monitor*, 14 June 2022. <https://monitor.civicus.org/updates/2022/06/14/freedom-expression-risk-cybercrime-legislation-used-prosecute-online-critics-vanuatu/> [↑](#footnote-ref-9)