FIGHTING FAKE NEWS

A STUDY OF ONLINE MISINFORMATION REGULATION IN THE ASIA PACIFIC

LA TROBE UNIVERSITY

Prepared and Written by

ANDREA CARSON
ASSOCIATE PROFESSOR (JOURNALISM)
DEPARTMENT OF POLITICS, MEDIA &
PHILOSOPHY, LA TROBE UNIVERSITY

with

LIAM FALLON

latrobe.edu.au

LA TROBE
UNIVERSITY

Table of contents

Tables, Figures and Boxes

Executive summary

Key findings and **conclusions**

The global spread of online misinformation has the potential to erode foundational elements of modern civilisation across much of the developed and developing world. Social cohesion, public health and safety, political stability and democracy are all under threat by the rapid and sometimes malicious dissemination of false information within and across national borders.

Online misinformation is an extremely complex and multi-layered problem that defies simple, one-size-fits all solutions; effective mitigation can only be achieved through multi-pronged strategies involving collaboration and cooperation between governments, digital platforms and community-based organisations.

Attempts to date by governments and global technology companies to tackle online misinformation and disinformation have been constrained by a multitude of challenges and policy shortcomings, not least being a lack of co-ordination and co-operation between key players.

Traditional media outlets can also contribute to the online misinformation problem through amplification of the existence of misinformation campaigns and should be included in strategies to mitigate it.

Popular terms such as misinformation, disinformation, fake news, false news and hoaxes are used loosely and interchangeably, leading to widespread confusion about their meanings, and adding to the already formidable challenge of trying to tackle the issue.

The extent of online misinformation is extremely difficult to gauge and to accurately measure, in part due to contested definitions about what is being measured.

Governments, global technology companies and other interested parties need to work together towards achieving a broadly agreed set of definitions of key terms surrounding online misinformation to enable coordinated and more effectively targeted strategies to be developed at local, national and global levels.

New laws in Indonesia and Singapore, ostensibly introduced to fight online misinformation and disinformation, are also alleged to have been misused by governments to crack down on political dissent and suppress freedom of expression and the media, further undermining already compromised democratic structures and institutions in Southeast Asia.

Advanced liberal democracies face a difficult challenge trying to balance the sometimes competing aims of pluralism, free expression and individual liberty against the need to protect citizens from online harms and to uphold the integrity of the electoral system.

Liberal democracies, including Australia, should be alert to the potential for any new anti-misinformation laws and regulations to be misused by governments to undermine freedom of speech and the media.

The European Union's 2018 Code of Practice on Disinformation, despite some shortcomings and ongoing issues, has gained attention as a benchmark for self-regulation of online content, and is influencing debate in Australia on the development of its proposed co-regulation framework.

Despite the uniquely difficult challenges faced in culturally-diverse jurisdictions like Indonesia, extensive work has been undertaken at grassroots and higher levels to mitigate online misinformation, with some success. However, the need for new approaches and initiatives is also apparent.

The global spread of online misinformation surrounding COVID-19 has exposed the broader potential of "information disorder'' on the internet to jeopardise public health and safety – particularly, but not exclusively, in less developed countries.

Background

The internet has revolutionised the way we live and connect with each other, bringing transformational economic and lifestyle benefits to much of the planet. But at what cost?

Increasingly, the rewards of the internet age are being shadowed by unintended consequences – not least the insidious spread of false and misleading information in the online sphere, with sometimes harmful consequences. This global problem can threaten essential elements of our modern civilisation, including social harmony, health and safety, the rule of law and democracy.

The focus of governments and law makers on the issue has been heightened since 2016, when evidence emerged about Russian operatives attempting to use online disinformation to interfere in the US presidential election campaign; and, also when the term "fake news" was popularised by then candidate Donald Trump. Of course there is nothing new about fake news; it has been around for centuries. What has changed in recent decades is how the internet has enabled the mass transmission of falsehoods to any part of the world at a rapid pace.

In the past five years, almost 20 countries have adopted new laws and regulations in attempts to tackle online misinformation and disinformation. Two of those countries, Indonesia and Singapore, are the focus of detailed examination in this report. Australia, meanwhile, is pursuing a voluntary co-regulation scheme involving the major digital platforms, scheduled to commence in 2021.

This independent research project, funded by Facebook Inc (based in Menlo Park), reflects the views of the authors and should not be taken to reflect the views of Facebook. Through the detailed examination of the experiences of Australia's near neighbours Singapore and Indonesia, and the European Union, the research aims to provide insights and points of comparison to assist the Australian Government, relevant authorities and digital platforms in their deliberations on managing the complex and fraught issue of online misinformation and its spread. The findings contain both valuable insights and warnings for policy makers in Australia and elsewhere.

Led by La Trobe University Associate Professor Andrea Carson, the research is based primarily on in-depth interviews conducted in the second half of 2020 with online experts and practitioners living in Indonesia and Singapore. Project participants included academics, technology industry experts, media executives, online journalists, editors and community-based activists in both countries. The report also incorporates other recent research into how the spread of online misinformation is being tackled in Europe and Australia.

Thematic **findings**

This study offers new insights summarised below and organised around three broad themes identified out of the in-depth interviews with experts in Singapore and Indonesia.

The themes are:

- What is online misinformation – and why is it a problem? (chapter 5)
- Tackling misinformation online and its challenges (chapter 6)
- Potential remedies (chapter 7)

Theme 1:
What is online misinformation – and why is it a problem?

Contested definitions

The lack of universally agreed definitions of terms such as online misinformation, disinformation and fake news presents significant obstacles to achieving consensus on how to tackle the problem. Even among experts who contributed to this project, significant diversity of opinion emerged over the meanings of misinformation and disinformation.

For the purposes of this report, we have adopted the following definitions for online misinformation and disinformation:

- **Online misinformation** is the spread of inaccurate or misleading content online.
- **Online disinformation** is the spread of inaccurate or misleading content online with conscious intent to mislead, deceive or otherwise cause harm.

In this way, this report characterises online disinformation as a substantial subset of the broad, overarching problem of misinformation. By our definition, misinformation can be spread with or without ill-intent, while disinformation necessarily involves ill-intent. We have adopted these definitions – and in particular a broad interpretation of misinformation – in part because it closely aligns with the usage of experts who participated in this project.

Our typology is not standardised. For example, First Draft, a global coalition of newsrooms, universities, online platforms and civil society groups, defines **misinformation** more narrowly: as verifiably false content that is spread *without the intention of causing harm*. The First Draft typology, while embraced by many, has its problems. Social media and technology platforms argue that a person's intention when posting information is too difficult to divine. They prefer to identify **misinformation** based on the veracity or accuracy of the *content*, and **disinformation** with reference both to the *actors* and *behaviours* of those who spread it, and to the content's propensity to cause harm.

Other complications emerge. The profusion of false content surrounding COVID-19, including bogus remedies, shows how misinformation, as defined by First Draft, can be spread without intention to cause harm and yet it also can engender real-word harm. Further, some online content that starts out being spread with ill-intent can be spread innocently by others and still cause harm.

Another complication surrounds the term fake news, which has evolved from a descriptor of factually incorrect news content to a phrase increasingly weaponised by some – most conspicuously populist-styled political leaders such as Trump – to try to delegitimise factual content in the mainstream news media. Loosely-defined terms such as fake news can also result in the conflation of very different and distinct problems – such as threats to electoral integrity, hate speech and cyber threats – which, in turn, can potentially lead to inappropriate one-size-fits-all remedies. Conversely, when governments and platforms adopt separate, or "siloed" approaches to misinformation and disinformation, problems can emerge when falsehoods fall into both categories, as can happen on issues such as COVID-19.

Scale and measurement of the problem

It is generally agreed that online misinformation is a greater problem in Indonesia than in Singapore. Indonesia's geographical, cultural, linguistic and religious diversity provides fertile ground for political polarisation, and considerable scope and motivation for spreading false information. Its varied literacy levels in a mass population also make it a challenging environment for online education against the proliferation of misinformation.

The extent of online misinformation is extremely difficult to gauge and to accurately measure, in part due to contested definitions about what is being measured. Moreover, misinformation transcends geographical borders as well as online and traditional platforms, and is often shared on encrypted platforms such as WhatsApp. This report finds some cause for optimism that greater levels of misinformation are being detected and acted on. But whether the gap has narrowed between the volumes of what is being spread and what is being acted on remains an open question.

Common forms of misinformation

The report finds the most commonly detected forms of online misinformation in Indonesia and Singapore relate to politics, public health and conspiracy theories. Online hate speech is a major global problem, but it is outside the scope of this study as its spread is most often regarded as disinformation. Observed motivations for spreading misinformation ranged from political and financial, to mischief-making.

Consequences of misinformation

The negative consequences of online misinformation can be many and varied, ranging from emotional and physical harm to individuals, to wider damage to communities through adverse health outcomes (such as from anti-vaccination campaigns) and undermining of democracy, particularly during election campaigns. Experts who participated in this project also identified a number of marginalised groups in Indonesia and Singapore they considered at high risk from online misinformation campaigns, including women (particularly in Indonesia), people identifying as LGBTI, journalists, human rights and anti-corruption activists, and minority ethnic groups. They also cited wider social consequences of online misinformation, including:

- Reduced public trust in news media and politics
- Low quality discourse in the online environment
- Reduced capacity of the general public to distinguish fact from fiction.

Theme 2: Tackling misinformation online and its challenges

Industry measures

Multinational technology companies such as Facebook, Google and Twitter have implemented a range of measures, at both local and global levels, to try to reduce harmful and "inauthentic" content on platforms. Given the essential differences between misinformation and disinformation, the platforms have tended to assign separate strategies, and in some cases separate teams, to each.

Disinformation is typically defined as the spread of false information with the intention of causing harm. However, given the inherent difficulty of discerning the intent of individuals who post false information, the platforms focus on other criteria – in particular the online actors and their behaviour patterns – when trying to identify and deal with suspected disinformation. By contrast, platform strategies to identify and manage misinformation (defined for the purposes of this report simply as the spread of inaccurate content) tend to focus on the veracity or otherwise of the content itself, rather than the behaviour of the poster. However, when problematic content falls into both categories – typically at varying times – platform responses may include

one or more different measures, with the choice of response depending on the type and severity of the suspected breach. Low-level breaches may lead to no more than the publication of terms and conditions of use with reference to a platform's published community standards. At the other end of the scale, flagrant and serious breaches can result in users being banned from the platform.

Facebook employs a broad three-pronged approach involving shutting down offending accounts; limiting distribution of problematic content; and providing cues to online users about the quality of the information they are consuming, with a view to boosting the media literacy of users. Within these broad categories, Facebook:

- Provides tools and campaigns to improve digital literacy
- Commissions third-party fact checking of suspect content
- Attaches false information warning labels to problematic content
- At times, require proof of user identity to improve account transparency
- Takes down harmful content, or technically limits its algorithmic spread
- Reduces services to users found to have breached the platform's community standards
- Provides resources and financial support to news media organisations in some countries.

Facebook and other platforms have also:

- Used artificial intelligence (AI) to detect and identify problematic online content
- Forged partnerships with community-based organisations that can detect and forewarn platforms of emerging misinformation campaigns. This has been particularly useful in Indonesia, where demographic diversity presents unique challenges
- Exchanged information with each other and with governments about known online misinformation threats
- Funded academic research (including this project) to expand their knowledge about online misinformation and possible remedies
- Provided mechanisms for the public to report online misinformation, and to alert platforms to other content that deviates from their community standards.

Government measures

The governments of Singapore and Indonesia have strongly focused on legislative measures in response to the quantum of online misinformation in the past decade, utilising existing laws and enacting new ones – with sometimes controversial outcomes. It is a fast-moving policy landscape with new laws passed even as this report was going to print.

The major legislative initiatives have been the 2019 Protection from Online Falsehoods and Manipulation Act (POFMA) in Singapore, and 2016 revisions to the Information and Electronic Transactions Law (ITE) in Indonesia. Singapore has also utilised existing broadcasting and sedition laws, while Indonesia has invoked its defamation and anti-pornography laws, and proposed controversial changes to its Criminal Code, which critics argue will give the Government too much power to suppress freedom of speech and expression. In December 2020, Indonesia passed its highly controversial Ministerial Regulation 5/2020, which amongst other things requires platforms to remove content "against the public order" within 4 hours, or face heavy penalties, including blocking of platforms. Indonesia's Communications and Informatics (KOMINFO) Ministry has also been active in the fight against alleged hoaxes and disinformation with its own fact checking exposés.

The governments of both Indonesia and Singapore have often clashed with civil society groups and major technology platforms over how to define and respond to contested online content. Platforms have at times refused requests or demands from governments to respond to disputed content in particular ways – notably when governments have sought the prompt removal of content before the platform says it has had time to assess it adequately. Such disagreements have occurred most frequently during election campaigns. In this environment, the newly passed Indonesian Ministerial Regulation 5/2020 will likely be a closely watched law by defenders of civil liberties.

Challenges for platforms

Despite their apparent progress in tackling some forms of online misinformation, technology platforms face formidable ongoing challenges. Participants in this project identified at least four major persisting impediments for the platforms:

- The spread and detection of false content between different platforms
- The geographic spread, and the ethnic, religious and linguistic diversity of Indonesia

- Government pressure to remove content at odds with the platforms' own assessments
- Content on encrypted platforms, which adds to the difficulty of detecting misinformation and alerting users to its spread.

A number of remedies have been suggested to counter the sharing of false content between different platforms. One approach would be to follow the example of the European Code of Practice on Disinformation, which prescribes regular meetings of a range of stakeholders. For Asia-Pacific countries, this would mean establishing and formalising closer cooperation between rival platforms, and forging ongoing relationships with community-based organisations to develop more systematic early alert systems for the emergence of misinformation campaigns.

Indonesia's demographic diversity and geographic spread present major obstacles on various fronts. For example, detection measures involving the use of artificial intelligence struggle against the multitude of languages in use across the Indonesian archipelago. And while media and digital literacy campaigns have some utility in countering the spread of misinformation, their success is constrained by disparate levels of education in very large populations.

Dealing with government demands and expectations relating to contested online content is more difficult to address. Platform experts who contributed to this project argued that:

- Deadlines set by governments to assess and remove misinformation tended to be too tight
- Governments were hopelessly conflicted when they purported to be both the arbiter of online misinformation and the enforcer of laws against misconduct
- The governments of Indonesia and Singapore had taken a binary approach to defining and identifying misinformation, putting them at odds with the platforms' global policies and Western values of trying to balance concerns about freedom of expression against the need for social responsibility and harm mitigation.

Critics of the legislative approaches of Indonesia and Singapore, which include significant jail terms and large fines for convicted offenders, say the laws have been used to suppress free speech and intimidate government opponents into self-censorship.

While different polities, the problems with legislative responses to online misinformation in Asian countries highlight some potential challenges for Australian legislators and policymakers

as they consider new approaches to the issue domestically. Not least among these challenges is how to balance the need for social responsibility and harm minimisation against freedom of expression and other fundamental values and rights held dear in advanced liberal democracies.

Challenges for governments

Globalisation – and the massive flow of internet content over national boundaries – places major practical limitations on the effectiveness of national laws to fight misinformation, particularly when there is disagreement between countries on what constitutes legitimate content. The international reach of online misinformation can render one country's legal jurisdiction relatively impotent in the absence of cooperation from other countries. And when disagreements emerge across national borders about content appropriateness, diplomatic issues can arise not just for governments, but for the platforms tasked with resolving them.

The tendency of the Indonesian and Singapore governments to prioritise law enforcement ahead of less punitive mechanisms to deal with online misinformation has also created major controversy and public distrust towards governments – particularly in light of accusations that anti-misinformation laws have been misused for political purposes.

Political misuse

Experts say the governments of Indonesia and Singapore have used misinformation laws to censor or silence a wide spectrum of critics. They say this has had detrimental implications for freedom of speech, media freedom and political pluralism, and democratic representation in both countries. The governments have been accused of using the laws to target their political opponents, as well as journalists, religious groups, political dissidents, human rights campaigners and other activists.

In Singapore, most of the controversy surrounds the 2019 Protection from Online Falsehoods and Manipulation Act (POFMA), which bestows extensive powers on the Government and its ministers to declare information to be false or misleading, and to force publishers to apply a correction notice or remove content. Some MPs have accused the ruling PAP of creating and using POFMA to serve its own political ends and, in the words of one, tighten a "dictatorial government's… hold onto absolute power". Some have also questioned how the Government could make fair judgements in cases

where it was the subject of alleged falsehoods, while others have highlighted the potential for POFMA to be used to intimidate independent media and government critics.

The Singapore Government has also been accused of using pre-existing laws, including the Defamation Act, to deter dissent under the guise of prosecuting online misinformation. According to the international organisation Human Rights Watch, the Defamation Act has been the Government's "most powerful non-criminal weapon" against its opponents. Its large penalties are claimed to have served as a government tool against speaking ill of the Government, with self-censoring widely observed and practised, and government-initiated defamation actions often succeeding.

In Indonesia, the Government's use of the Information and Electronic Transactions Law (ITE) to prosecute online misinformation has been characterised by critics as a threat to freedom of speech and media freedom. Hundreds of Indonesians have been prosecuted under the ITE law over online comments critical of the Government and President Jokowi in recent years. During Jokowi's first term (2014-2019), 241 individuals were "criminalised for criticising authority figures of the Jokowi administration," according to Usman Hamid relying on Amnesty International figures.[1] Meanwhile, academic Ross Tapsell found no evidence of anyone being prosecuted by the state for spreading falsehoods about Jokowi's opponent, Prabowo, during the 2019 presidential election campaign.[2] The Government also used the law against critics in West Papua, the scene of a long-running struggle for independence. In 2019, human rights lawyer and West Papua defender Veronica Koman was charged under the ITE law for allegedly spreading fake news that caused unrest in the region. And in August of that year, the Government used Article 40 of the ITE law to shut down internet access in West Papua.[3]

Theme 3: Potential remedies

Experts agree that effective mitigation of online misinformation requires a multi-pronged approach, with the active involvement of all interested groups – the digital platforms, governments and policymakers, academics, journalists, community organisations and the wider community of internet users. Further, the experts identified that existing measures and programs implemented by governments and technology platforms need to be supplemented on a number of important fronts. These include:

Common definitions

Agreement among key stakeholders on definitions of key terms – most importantly misinformation and disinformation – will be essential to ensuring that authorities dealing with online falsehoods are acting in concert and addressing the same problems. To date this has not occurred. Currently, the terms misinformation and disinformation can mean different things within and beyond national borders – including in the labelling of national legal codes. Even some experts who participated in this research project used the terms interchangeably.

Education

Digital education programs have been rolled out in Indonesia and Singapore. They include "train the trainer" programs for digital literacy educators, and mass advertising campaigns against false news designed to educate internet users to identify false information and avoid sharing it. But experts argue more needs to be done – and emphasise that education programs cannot succeed in the absence of efforts on other fronts to curb the spread of false and potentially harmful content.

Engagement and collaboration with all sectors

The project participants unanimously agreed that the involvement and cooperation of all interested parties – governments, policymakers, technology companies, academics, media groups, journalists and grass roots community-based organisations – was an essential precondition to effective action against a problem as complex and multi-layered as online misinformation.

Greater transparency

Platforms have been criticised for allegedly inadequate reporting of the scale of the problem of misinformation, and for not being more transparent about what they are doing to manage it. In their defence, platform experts point out the extreme difficulty of measuring a phenomenon that transcends national borders and often goes undetected, and for which there is no agreed definition and varying degrees of associated harm. Facebook undertakes twice yearly reporting of its global measures, and quarterly reporting of country-specific measures that were geoblocked because of local laws. This data is available on the platform's website. However, critics argue greater efforts are required to communicate to the public what is being done to tackle online misinformation.

Supporting public interest journalism

Among other factors, the rise of the major technology platforms – in particular Google and Facebook – has impacted the advertising business model of mainstream media companies and led to newsroom cutbacks and closures, as the ACCC reported.[4] At the same time, the platforms have provided financial support for quality journalism for many reasons, including because of its power to help internet users distinguish fact from falsehood. So ironically, while journalism has been a casualty of the mega-success of the technology platforms, Google and Facebook have recognised the importance of it with targeted initiatives such as the Journalism Project (Facebook) and the Google News Initiative, which provides journalists with data skills and online tools. Google's News Lab also collaborates with journalists and entrepreneurs to drive innovation in news. Facebook is piloting Facebook News in the USA to enable quality news outlet stories to reach bigger audiences. Elsewhere, Twitter donates to specific journalism projects such as the Committee to Protect Journalists and the International Women's Media Foundation. Most major platforms also provide journalism research funding to the academic community and support for digital media start-ups. While these initiatives will not restore employment of journalists to the levels of the pre-Facebook and Google era, they are an acknowledgement of the essential role of public interest journalism in functioning liberal democracies – and, by extension, in the fight against online misinformation and disinformation.

1   Usman Hamid, "Indonesia's Information Law has threatened free speech for more than a decade. This must stop," *The Conversation*, November 25, 2019, https://theconversation.com/indonesias-information-law-has-threatened-free-speech-for-more-than-a-decade-this-must-stop-127446
2   Ross Tapsell, "Indonesia's policing of hoax news increasingly politicised," *ISEAS*, no. 75 (2019), https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_75.pdf
3   Reuters, "Rights group, journalists press Indonesian govt to lift internet curb in restive Papua," Thomson Reuters Foundation, published August 23, 2019, https://news.trust.org//item/20190823055418-5iy2g/
4   Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final report* (Canberra: ACCC, 2019), 34, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

**FIGHTING
FAKE NEWS**

A Study of
Online Misinformation
Regulation in the
Asia Pacific

Overview

The internet is without question among the most transformational human inventions of recent centuries. In the space of just two decades, it has revolutionised the way we live and connect with each other, delivering previously unimaginable economic and lifestyle benefits. But as with many other monumental inventions, the internet has come with some harmful unintended side-effects. And among the most concerning of these has been its enabling of the spread of false information, or "fake news".

There is nothing new about fake news; it has been around for centuries. What has changed is that near-universal access to online technology has enabled the spread of false information on an unprecedented scale.

Governments, technology platforms and other stakeholders have become increasingly alert to the dangers of online misinformation and disinformation over the past decade – particularly in the time since Donald Trump popularised the term fake news during his 2016 US presidential election campaign. On many fronts, the spread of online falsehoods appears to be undermining foundational elements of modern civilisation – most notably social harmony, public health and safety, and political democracy – in many parts of the world.

In Indonesia and Singapore – two dynamic Southeast Asian nations that are the primary focus of this report – misinformation and disinformation have flooded the online space during recent national elections, adding to serious concerns about their degrees of liberal governance. The concerns have been compounded by accusations that the national governments of both countries have used anti-misinformation laws to target their political opponents and suppress free speech and freedom of the media.

Elsewhere, external state actors are increasingly using false online content to try to influence foreign election outcomes. Others are targeting vulnerable groups and individuals with hate speech. Online misinformation is also undermining global public health – most recently with the spread of falsehoods and conspiracy theories surrounding COVID-19. Fake news can also make money, an example being the Macedonian youth entrepreneurs who made millions in advertising revenue by using made-up political headlines as clickbait.[1]

Surveys in Australia find that most people are worried about fake news.[2] Some scholars fear an epistemic crisis with citizens unable to confidently separate fact from fiction.[3] Other studies show that political leaders who seek to delegitimise journalism as "fake news" could be undermining public trust in the mainstream news media, and leading people to rely on less trustworthy sources.

It is in this context that governments, technology platforms and other interested parties in all jurisdictions, including Australia, have been redoubling efforts to tackle this serious and challenging public policy issue.

Aim and report objectives

This independent research project, funded by Facebook Inc. (based in Menlo Park, US), aims to inform contemporary deliberations in Australia about tackling online misinformation and disinformation, including the proposed development of a voluntary code of technology industry practice in 2021. The research examines in depth how Singapore and Indonesia – two of Australia's closest Asia-Pacific neighbours – have tackled the problem, and compares and contrasts their responses to supra-national initiatives in the European Union. It is hoped the findings will help to guide the Australian Government, its media regulator and digital technology companies as they consider various possible measures to try to contain the spread of false information on digital platforms in the Australian context. To this end, the report:

- Provides an overview of how governments and digital platforms in Singapore, Indonesia and the European Commission have responded to the perceived threats of falsehoods on social media and other digital platforms
- Provides the examples of Singapore and Indonesia to examine the potential implications of legislative and other policy responses to online misinformation for political discourse and freedom of expression
- Documents detailed insights from key actors (journalists, academics and technology platform experts) about the major challenges arising from the spread of false information online, and the consequences for public debate
- Consolidates the findings into a timely publication that highlights the public policy and political challenges and responses to the spread of false information on digital platforms in the selected countries
- Identifies key considerations and challenges relevant to online platform governance in Australia.

---

1   https://www.wired.com/2017/02/veles-macedonia-fake-news/
2   Caroline Fisher, "Australia," in *Reuters Institute Digital News Report* 2019, eds. Nic Newman, Richard Fletcher, Antonis Kalogeropoulos and Rasmus Kleis Nielsen (Oxford: Reuters Institute for the Study of Journalism, 2019), 132-133, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/inline-files/DNR_2019_FINAL.pdf; Michael Barthel, Amy Mitchell and Jesse Holcomb, "Many Americans believe fake news is sowing confusion," Pew Research Centre, published December 15, 2016, https://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/
3   Paul Dahlgren, "Media, knowledge and trust: The deepening epistemic crisis of democracy," Journal of the European Institute for Communication and Culture 25, no. 1-2 (2018): 20-27, DOI: 10.1080/13183222.2018.1418819

Background and Australian context

In advanced liberal democracies like Australia, the reach and spread of online networks presents a conundrum for legislators and policymakers. On one hand, the state must try to protect the public against harm from false and potentially dangerous information. On the other hand, as a custodian of democracy, the state must seek to protect the rights of the people to freedom of expression and speech. Governments therefore face a difficult challenge trying to balance the sometimes competing aims of pluralism, free expression and individual liberty against the need to protect citizens from online harms and, in the case of democracy, to uphold the integrity of the electoral system.

The dilemma is highlighted by some worrying global trends. Freedom House and other global political and media indices paint an alarming picture of how democracy and pluralism have come "under assault"[4] in the online age, with the world experiencing 14 years of decline in political rights and civil liberties up to 2019.[5] Similarly, media freedom has reportedly been in decline for more than a decade – under both illiberal and liberal governments,[6] with some using the spectre of fake news to restrict online news content.

But there is also cause for optimism. Global technology platforms are investing heavily in efforts to verify online information, with measures ranging from sophisticated artificial intelligence detection, to manual fact checking on a large scale across both developed and developing jurisdictions. Yet it remains to be seen how far these measures go towards restoring public trust in public information and in established news organisations in an era blighted by the spread of misinformation.[7]

How governments have responded

In an overview of regulatory and other responses to online misinformation across the globe, academics James Meese and Edward Hurcombe identify three distinct approaches:

- Voluntary co-regulation initiatives "that do not involve mandated regulation or state oversight".[8] In these instances, government bodies encourage digital platforms to work with stakeholders to develop and implement a broad set of aims to tackle online misinformation, as is the case with the EU Commission. Australia is currently following this model.
- Direct legislative measures, such as those adopted in Singapore and Indonesia. Meese and Hurcombe say that generally governments adopting this approach have tended to circumvent consultation. Others claim such laws have been misused for political purposes, and tend to operate in jurisdictions already known for low levels of media and political freedoms.[9] The European liberal democracies of France and Germany have also opted for legislation, but with more checks and balances against misuse than Indonesia and Singapore. Even so, the German Government has been criticised for over-reach.[10]
- Non-regulatory activities such as the government funding of digital literacy campaigns (Indonesia and the EU) and factchecking operations (Indonesia).[11]

Australian response

In 2017, the Australian Government directed the Australian Competition and Consumer Commission (ACCC) to oversee a Digital Platforms Inquiry. The final report of the inquiry in 2019 contained detailed proposals to address disinformation and misinformation on online platforms operating in Australia (see chapter four). The report called for

"monitoring efforts of digital platforms to implement credibility signalling"[12], and for a voluntary digital platforms "code" to counter disinformation.[13] The report stated that the code should apply to complaints about disinformation that involved "serious public detriment"[14], and that it should be overseen by the Australian Media and Communications Authority (ACMA).

ACMA's subsequent position paper – *Misinformation and news quality on digital platforms in Australia: A position paper to guide code development* – was released in 2020. It said digital platforms to be covered by the code should include online search engines, social media platforms and other "digital content aggregation services with at least one million monthly active users in Australia".[15] Individual news media outlets were excluded from consideration for coverage by the code because they were "not considered key distributors of misinformation in Australia."[16] This was despite subsequent findings that traditional media outlets also contribute to the online misinformation problem in Australia.[17]

In response to the ACMA and ACCC initiatives, the platform providers, represented by the Digital Industry Group Inc. (DIGI), produced the *Australian code of practice on disinformation* for public consultation in October 2020 (see chapter four for details). The use of the word "disinformation" in the title is noteworthy in light of the previous use of "misinformation" in the title of ACMA's position paper. As discussed elsewhere in this report, ambiguity over the meanings of key terms including misinformation and disinformation has to some extent compounded the challenge of tackling the broad problem of online falsehoods.

This research report is intended to complement the public consultation process in the lead-up to the planned enactment of the voluntary code in 2021.

4   Sarah Repucci, "A Leaderless Struggle for Democracy: Democracy and Pluralism are under assault", *Freedom House,* 2020, https://freedomhouse.org/report/freedom-world/2020/leaderless-struggle-democracy

5   Ibid.

6   Freedom House, *Special Report 2018: Attacks on the Record - The State of Global Press Freedom, 2017-2018* (Freedom House, 2018), https://freedomhouse.org/report/special-report/2018/attacks-record

7   Andrea Carson, *Investigative Journalism, Democracy and the Digital Age* (New York: Routledge, 2020), *232.*

8   James Meese, J and Edward Hurcombe, Regulating Misinformation: Policy Brief (Melbourne, Analysis & Policy Observatory, RMIT University), https://apo.org.au/node/309357 p.3

9   Ric Neo "The Securitisation of Fake News in Singapore." *International Politics*, October 4, 2019. https://doi.org/10.1057/s41311-019-00198-4.

10   James Meese, J and Edward Hurcombe, Regulating Misinformation: Policy Brief (Melbourne, Analysis & Policy Observatory, RMIT University), https://apo.org.au/node/309357

11   Ibid.

12   ACMA defines credibility signalling as "flagging trusted sources and providing users with access to information on publishers and other sources" (Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia: A position paper to guide code development (Canberra: ACMA, 2020), 29,* https://www.acma.gov.au/sites/default/files/2020-06/Misinformation%20and%20news%20quality%20position%20paper.pdf

13   Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final report (Canberra: ACCC, 2019), 34,* https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

14   Australian Competition and Consumer Commission, *Digital Platforms Inquiry, 34.*

15   Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia: A position paper to guide code development*, 3.

16   Ibid., 22.

17   Axel Bruns, Stephen Harrington, and Edward Hurcombe, "'Corona? 5G? Or Both?': The dynamics of COVID-19/5G conspiracy theories on Facebook," *Media International Australia* 177, no. 1 (November 2020): 12–29, https://doi.org/10.1177/1329878X20946113

Method, scope and terminology

This research project centres on two case countries in the Asia Pacific region – Indonesia and Singapore – that have adopted a legislative approach to tackling online misinformation. The project also examines the alternative of voluntary co-regulation between governments and platforms adopted in European Union nations, on which Australian authorities have heavily drawn in their deliberations ahead of the proposed adoption of an Australian voluntary code.

Literature and policy review

The first step of the research process involved a detailed review of previous research examining countries that have taken a legislative approach to online misinformation, and others that have adopted voluntary co-regulation. The extensive literature review identified key themes that helped to inform the in-depth interviews conducted with 14 experts in the online sectors in Indonesia and Singapore. The interviewees included journalists, editors, media regulators, academics, digital platform experts, human rights activists and members of non-government organisations with practical knowledge of how false information online – and policy responses to it – impact citizens' daily lives and public discourse. The views of government representatives have been recorded in official documents and cited in background chapters.

Interviews

Plans for face-to-face meetings with experts in Indonesia and Singapore had to be abandoned in favour of online interviews after the COVID-19 pandemic precluded international travel. Each expert was interviewed for approximately one hour on the general nature of online information disorder in the digital age, and how it impacts on work and society, and government responses to it (see Appendix 4 for detail). Some interviewees participated on condition of anonymity due to their concerns about possible adverse repercussions.

Scope and terminologies

The original empirical findings of this study detailed in chapter five to seven focus on the legislative responses to online misinformation and disinformation in Indonesia and Singapore. The findings are intended to provide insights and a point of comparison for those involved in deliberations over future measures to tackle online misinformation in Australia.

A limitation that should already be apparent from this introduction is the lack of broad consensus on the meanings and applications of terms such as misinformation, disinformation, malinformation and fake news. Even experts who contributed to this project were not completely aligned or consistent in their use of these terms. This lack of consensus on definitions is acknowledged as a significant barrier to developing effective policies and measures to tackle the problem.

To try to mitigate confusion for readers of this report, we have adopted a simple and broad definition of **online misinformation:** the spread of inaccurate or misleading content online.

We define **disinformation**, by contrast, as the spread of inaccurate or misleading content online *with conscious intent to mislead, deceive or otherwise cause harm*. In this way, we consider online disinformation to be a substantial subset of the broad, overarching problem of misinformation. This is a similar position to the ACMA.

It must be emphasised that this typology is not an accepted standard; others use slightly or even widely differing definitions. We have adopted this typology for the sake of clarity and consistency. It also reflects broad usage of the term misinformation – to mean all types of false or misleading online content – by a majority of expert participants in this project.

Our broad definition of misinformation is in contrast to some popular definitions which hold that misinformation is confined to false and/or misleading content created *without the intention of causing harm*.[18] This provides a simple and clear counterpoint to disinformation when it is defined as false or misleading content spread *with* the intention of causing harm. However, as we show in this study, there are practical problems with both these definitions.

The narrower definition of misinformation can be problematic because in some instances, as the COVID-19 pandemic has shown, false content spread without ill-intent can also cause harm.[19] And while the idea of disinformation as false content spread with ill-intent is conceptually straight forward, in practice it can be difficult to establish or to prove the intentions of people posting content. For this reason, technology platforms focus on other criteria such as the *actors* who are spreading false information and *patterns of behaviour* when trying to identify and mitigate disinformation, and on the *veracity of the content* when identifying other types of misinformation.

In summary, when this report uses the word disinformation, it should be taken to mean spreading false or misleading content with *conscious intent to mislead, deceive or otherwise cause harm*. When we use the broader term misinformation, or quote others using that word, it refers to the spread of inaccurate or misleading content online that may or may not cause harm – depending on the context.

The report further acknowledges that both misinformation and disinformation are a part of what academic Claire Wardle and her colleagues call the broad problem of online "information disorder".[20] We also acknowledge and adopt the British Government's broad definition of the term fake news "as shorthand for both disinformation and misinformation".[21]

Chapter contents

Chapters one and **two** examine how the spread of online misinformation and disinformation has been approached by governments in Indonesia and Singapore, two of Southeast Asia's most prominent and dynamic nations. In each case we consider the unique local historical and cultural contexts in which this most global of 21st century issues is playing out. We examine the various laws (pre-existing and new), regulations and other tools they have deployed in the fight against misinformation – and how these measures have at times been as controversial as the problems they purport to tackle. The report gives particular attention to claims that governments in both countries have used anti-misinformation measures as weapons to silence their critics and suppress freedom of speech and the news media. By extension, we look at the

---

18   Claire Wardle, "The Need for Smarter Definitions and Practical, Timely Empirical Research on Information Disorder." *Digital Journalism*, 6, no. 8: 953.
19   Ibid.
20   Claire Wardle, "The Need for Smarter Definitions and Practical, Timely Empirical Research on Information Disorder."
21   DDCMS, *The Cairncross Review: A Sustainable Future for Journalism*, (London: Department for Digital, Culture, Media & Sport,12 February 2019), 103, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf

vexed questions of who decides what is and what is not misinformation, and what it all might mean for the governance of Indonesia and Singapore.

Chapter three provides a brief history and overview of the measures in place in the EU. It focuses on the development and performance of the EU's main measure, the EU-wide *Code of Practice on Disinformation*, established in 2018. It also examines other important initiatives and actions taken in Europe to manage the spread of misinformation and disinformation, including laws passed by individual EU Member States.

Chapter four looks in detail at Australia's experience of online misinformation, and how governments have responded to it. We trace the recent history of debates and development of proposed co-regulation, and draw comparisons, where relevant, with measures undertaken in other countries.

Chapters five, six and seven are the results chapters derived from the interviews. Each chapter reflects one of the three broad themes outlined in the Executive Summary. Together, they examine the challenges and responses to misinformation and disinformation in the Asia-Pacific region, drawing on expert local knowledge within Indonesia and Singapore.

Chapter five draws on interviewees' experiences and knowledge to explore the nature and scale of online misinformation in Indonesia and Singapore.

Chapter six examines existing measures in Indonesia and Singapore being used to address online misinformation, including legislative responses as well as initiatives of digital platform providers and non-government and media organisations. It also examines accusations of political misuse of the laws by governments in both countries, and the implications for their democratic status.

Chapter seven considers potential remedies to online misinformation from the experts' perspectives. High on the list is the need for common definitions, digital education programs, involvement of trusted partners from the non-government sector, support for quality journalism and academic research, and greater reporting transparency from the platforms.

Chapter eight brings together the earlier findings and salient lessons observed from different countries' responses to online misinformation. It provides final observations about how the Australian Government, policy makers, regulators and the digital platforms and their users could work cooperatively to tackle this insidious problem.
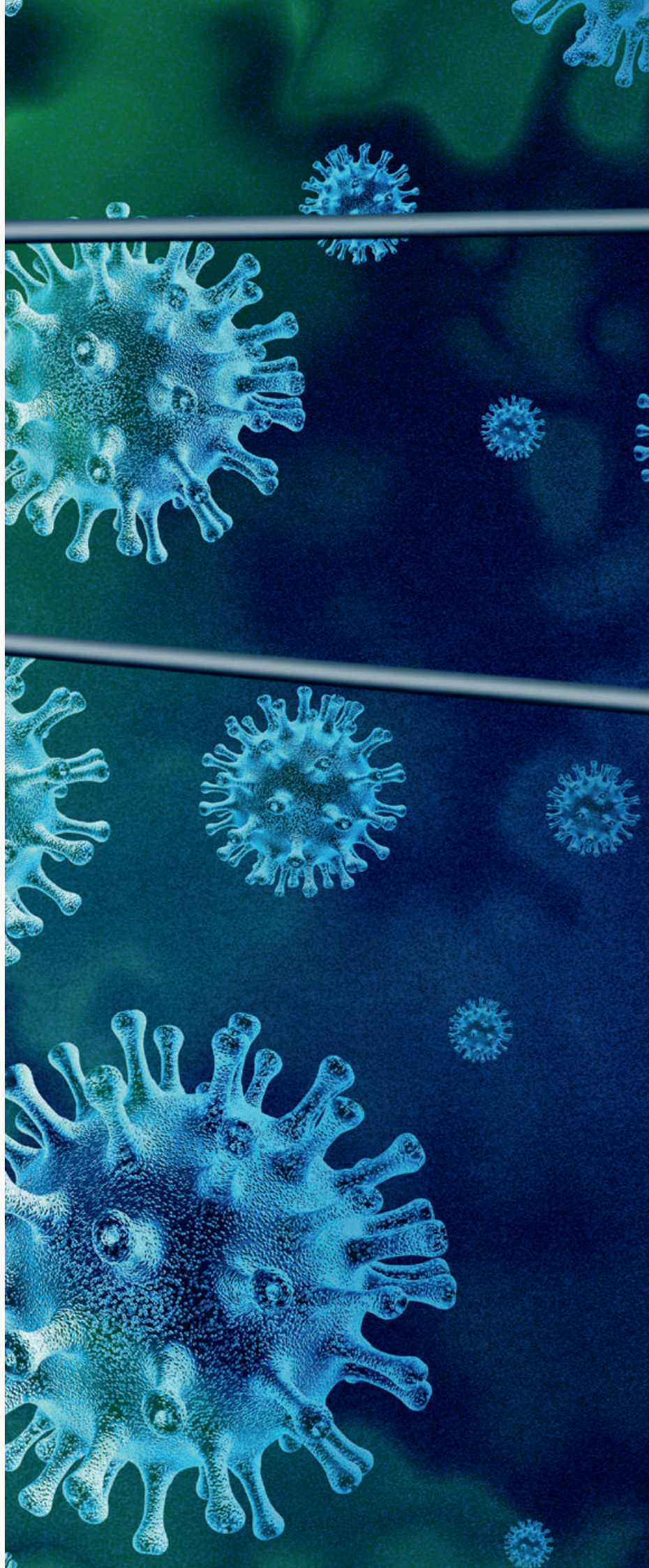
About the **Authors**

Dr Andrea Carson

is a political scientist and an Associate Professor in journalism in the Department of Politics, Media and Philosophy at La Trobe University in Melbourne, Australia. She has authored numerous articles on political communication, election campaigns and digital media and fake news. Her research focus is on quality information in the public sphere (fake news, media trust), political representation (women) and political communications. Her 2020 book examines the role of investigative journalism in democracies: *Investigative journalism, democracy and the digital age*. She researches the media's role in public policy agenda-setting using big data and was awarded Australian Research Council (2018-2021) funding as part of a team; and an ARC Linkage (2020-2024) studying female political representation in local government. She previously worked as a newspaper journalist and section editor at *The Age* in Melbourne from 1997-2001 and as a radio broadcaster (RRR) and radio and television producer (Australian Broadcasting Corporation) from 2001-2010.

Liam Fallon

is a researcher whose work at La Trobe University on research projects with Associate Professor Andrea Carson has covered political science, journalism, democracy and gender in politics. Liam is also a research assistant at Deakin University, where he has recently been working on a Victorian Government Department of Justice and Community Safety funded study on masculinity and violent extremism with Dr Joshua Roose. Liam's research interests include polarisation, truth and citizenship in democratic societies, public service media and cultural studies. He graduated from the University of Melbourne with a Bachelor of Arts (Honours) in 2016. He has previously worked in community broadcasting and the NGO sector.

CHAPTER 1

Indonesia's approach to online misinformation

Introduction

In this chapter and the following we examine how the spread of online misinformation and disinformation has been approached by governments in Indonesia and Singapore, two of Southeast Asia's most prominent and dynamic nations.

In each case we consider the unique local historical and cultural contexts in which this most global of twenty-first century issues is playing out. We examine the various laws (pre-existing and new), regulations and other tools they have deployed in the fight against misinformation – and how these measures have at times been as controversial as the problems they purport to tackle. We give particular attention to claims that governments in both countries have used anti-misinformation measures as weapons to silence their critics and suppress freedom of speech and the news media. By extension, we look at the vexed questions of who decides what is and what is not misinformation, and what it all might mean for the future of political rights and civil liberties in Indonesia and Singapore.

Background and context

Mass protests staged in Indonesia in September 2019 signalled deep and widespread public discontent with proposed changes to a law about the Corruption Eradication Commission; the changes to Indonesia's Criminal Code (KUHP) was one of several other grievances protestors expressed at the rallies.[1] Of particular concern are the KUHP Bill's ostensible attempts to curb the spread of online misinformation with provisions targeting "hoaxes," known locally as *hoaks,* Indonesia's term for fake news.

It also clamps down on defamation of the Government, which has raised fears of further limits on freedom of speech and the media. While the protests prompted President Joko Widodo to postpone a vote on the Bill, fears about its illiberal potential persist.

In this chapter, we track the history of Indonesia's approach to tackling online misinformation over the past decade, leading up to the proposed new Criminal Code. We look at how existing laws and regulations have been adapted and used by the Government to take on internet abusers – and, according to critics, to suppress dissent and free speech. The chapter also examines the unique cultural, ethnic and historical characteristics of Indonesia that help to explain the evolution of its approach to the issue. A timeline of the implementation of "fake news" laws and policies is tabled at the conclusion of the chapter (Table 1.1).

Ethnic and religious diversity

Suspicion about the Government's motives for wanting to amend the Criminal Code is informed partly by Indonesia's chequered history on freedom of speech. Successive regimes have employed varying levels of authoritarianism, including limits on free speech and the media, in their attempts to rule and hold together the highly diverse ethnic, religious and cultural groups that make up Indonesia's 270 million people. Javanese account for 40.1 per cent of the population, followed by Sundanese (15.5 per cent), Malay, Batak, Madurese and Betawi (each around 3 per cent) and dozens more.[2] Ethnic Chinese, though only 1.2 per cent of the population, have a disproportionately large presence and role in Indonesia's society and economy, which sometimes leads to tensions with majority groups.[3]

The disparate ethnic and language groups struggled collectively for independence from Dutch colonial rule in the 20th century.[4] In recent decades, however, in the absence of a shared colonial enemy, ethnic and regional differences have become more pronounced, keeping governments alert to potential and actual divisions.[5]

The existence of significant religious minorities also presents further challenges. While a large majority of Indonesians identify as Muslim, there are also significant numbers of Christians (9 per cent), Hindus (1.7 per cent), and others.[6] And within Islam, tensions exist between the large Sunni majority and smaller, mainly Shi'a communities.[7]

History and freedom

Historical narratives also influence contemporary Indonesian politics and its approach to tackling online information. The authoritarian, anti-democratic rule of President Suharto from the 1960s to the late 1990s – founded on anti-communist ideology and the national philosophy of "Pancasila,"[8] and marked by institutional corruption – continues to shape modern Indonesia. While direct presidential elections staged every five years since 2004 (indirect through parliament since the 1999 election) have been deemed free and fair by external adjudicators, fabricated claims of ballot fixing in the 2019 election[9] were a reminder that democracy in Indonesia remains fragile.

Feeding into this narrative of democratic vulnerability is evidence of declining civil freedoms. Indonesia scored just 61/100 (down from 65/100) in the latest Freedom House report, making it "partly free."[10] It was marked down on issues including rights for minorities, corruption, transparency, religious freedom (atheism is banned), judicial process, state violence, and legal, political and social equality.[11]

> Most established media groups, though technically independent of the Government, have strong partisan links to parties and politicians.[12]

Independent publications, such as the weekly magazine *Tempo*, are in the minority. And despite the proliferation of technologies enabling citizen-led journalism, much of this activity has been co-opted into the systems of established media conglomerates, ensuring continued concentration of media ownership.[13]

---

1   Eve Warburton, "Indonesia's pro-democracy protests cut across deep political cleavages", *New Mandala, October 3, 2019,* https://www.newmandala.org/indonesias-pro-democracy-protests/
2   Central Intelligence Agency, "The world factbook: Indonesia," accessed August 19, 2020, https://www.cia.gov/library/publications/the-world-factbook/geos/id.html
3   Sarah Turner and Pamela Allen, "Chinese Indonesians in a rapidly changing nation: Pressures of ethnicity and identity," *Asia Pacific Viewpoint* 48, no. 1 (2007): 112-127.
4   Christine Drake, *National Integration in Indonesia: Patterns and Policies* (Honolulu: University of Hawaii Press, 1989), 45.
5   Jacques Bertrand, *Nationalism and Ethnic Conflict in Indonesia* (Cambridge: Cambridge University Press, 2003) doi:10.1017/CBO978051155934; Richard Chauvel, and Ikrar Nusa Bhakti, *The Papua Conflict: Jakarta's Perceptions and Policies*, (Washington, D.C: East-West Center Washington, Policy Studies 5, 2004)
6   Oliver Wolter et al., "Indonesia: Religions," Britannica, last modified November 11, 2020, https://www.britannica.com/place/Indonesia/Services
7   Chiara Formichi. "Violence, sectarianism, and the politics or religion: Articulations of anti-Shi'a discourses in Indonesia," *Indonesia*, no.98, (2014): pp. 1-27.
8   Pancasila, literally meaning 'five principles', is the nation's core philosophy. It entails 'the belief in one God, just and civilized humanity, Indonesian unity, democracy under the wise guidance of representative consultations, and social justice for all the peoples of Indonesia' ("Pancasila,"Britannica. accessed August 20, 2020, https://www.britannica.com/topic/Pancasila).
9   After Joko Widodo was declared the winner of the 2019 Presidential election, his opponent, Prabowo Subianto, stated to the media that he and his team would not accept the result on grounds of alleged vote-rigging by Widodo.
10   "Freedom in the world 2020: Indonesia," Freedom House, accessed November 13, 2020, https://freedomhouse.org/country/indonesia/freedom-world/2020
11   Ibid.
12   Ross Tapsell, "Platform convergence in Indonesia: Challenges and opportunities for media freedom," *Convergence* 21, no. 2 (2014): 7-8.
13   Ibid., 13-14.

Indonesia is a major online player, accounting for the fourth and third largest number of internet and Facebook users globally.[14] But as online activity has soared in the past decade, Indonesia's internet freedom ratings, as measured by Freedom House, have declined[15] over issues including equality of access, transparency of internet restrictions, judicial protection, criminalisation of online acts, state surveillance, and extra-legal intimidation and violence.

Official attempts by the Indonesian Government to tackle online hoaxes have fuelled many of these concerns.

According to MAFINDO, a prominent community organisation dedicated to fighting online misinformation,[16] political content accounts for around 70 per cent of online hoaxes[17] – making efforts to combat it a contested and at times complicated endeavour.

The Government's approach to tackling misinformation

Multi-faceted strategy

The Government has employed a variety of tools, some of them direct and blunt, in its fight against alleged hoaxes. For example, it shut down internet access after riots over protests against racial discrimination in Papua that grew into broader calls for an independence referendum,[18] and in Jakarta during post-election riots in May 2019.[19] It has also empowered the National Police to arrest people alleged to have disseminated misinformation, while encouraging members of the public to report suspect online behaviour to authorities.[20] These efforts are aided by new technologies, such as artificial intelligence, that can identify inauthentic behaviour such as automated bot accounts on social media.[21] The Government has also implemented public education programs to increase media literacy,[22] engaged groups like MAFINDO to help identify hoaxes, and sought cooperation from social media companies to share their knowledge of hoaxes and ultimately have them removed.[23]

Conflicts of interest

Many critics have questioned the Government's motives and impartiality when it comes to deciding what is false information. Given that much of the content being scrutinised is political in nature and often anti-government in sentiment, the potential conflicts of interest are substantial – and readily apparent in the operations of the National Cyber and Encryption (BSSN) and State Intelligence Agencies, which report directly to the President. While these bodies may be necessary to tackle the problem, it raises the spectre of government manipulation to protect itself.[24]

Fighting religious and ethnic discrimination

Preserving religious and ethnic stability is a core element of Indonesia's approach to tackling online hoaxes. This is reflected in the criminalisation of information sharing that aims to incite hostility based on ethnic or religious divisions,[25] and blasphemy allegations.[26] Concerns about religious radicalism and political and ethnic tensions in some instances have led the Indonesian Government to pressure social media platforms to remove content.[27] People deemed to have contradicted "the beliefs or political ambitions'' of the Muslim majority online have also been targeted under Indonesian laws.[28] In one case a man who posted "God does not exist" and other comments deemed offensive to Muslims on Facebook was charged under the Criminal Code[29] and the

14   "Leading countries based on Facebook audience size as of July 2020," Statista, published July 24, 2020, https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-use
15   Usman Hamid, "Indonesia's Information Law has threatened free speech for more than a decade. This must stop," *The Conversation*, November 25, 2019, https://theconversation.com/indonesias-information-law-has-threatened-free-speech-for-more-than-a-decade-this-must-stop-127446; "Freedom on the net 2019: Indonesia," Freedom House, accessed November 13, 2020, https://freedomhouse.org/country/indonesia/freedom-net/2019
16   "About," MAFINDO, accessed August 10, 2020, https://www.mafindo.or.id/about
17   Santi Indra Astuti quoted in Cristina Tardaguila, "Fact-checkers are teaching Indonesian housewives how to stop misinformation," Poynter, published December 12, 2019, https://www.poynter.org/ifcn/2019/fact-checkers-are-teaching-indonesian-women-how-to-stop-misinformation/
18   Reuters, "Rights group, journalists press Indonesian govt to lift internet curb in restive Papua," Thomson Reuters Foundation, published August 23, 2019, https://news.trust.org//item/20190823055418-5iy2g/
19   Karina M. Tehusijarana, and Jessica Valentina, "Jakarta riot: Government temporarily limits access to social media, messaging apps," *The Jakarta Post*, May, 22 2019, https://www.thejakartapost.com/life/2019/05/22/jakarta-riot-government-temporarily-limits-access-to-social-media-messaging-apps.html
20   Ross Tapsell, "Indonesia's policing of hoax news increasingly politicised," *ISEAS*, no. 75 (2019), https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_75.pdf
21   Kate Lamb, "Muslim Cyber Army: a 'fake news' operation designed to derail Indonesia's leader," *The Guardian*, March 13, 2018, https://www.theguardian.com/world/2018/mar/13/muslim-cyber-army-a-fake-news-operation-designed-to-bring-down-indonesias-leader
22   See 'About Siberkreasi', Siberkreasi, accessed November, 13 2020, https://siberkreasi.id/tentang-siberkreasi/
23   Safrin La Batu, "Nine social media, messaging apps agree to combat fake news," *The Jakarta Post*, January 31, 2018, https://www.thejakartapost.com/news/2018/01/31/nine-social-media-messaging-apps-agree-to-combat-fake-news.html
24   Tapsell, "Indonesia's policing of hoax news increasingly politicised," 3.
25   "Law No. 11 of 2008 on Information and Electronic Transactions [UU ITE] (Indonesia), 2008 [revised 2016]" HUKUM Online, accessed November 13, 2020, Article 28(2), https://www.hukumonline.com/pusatdata/detail/lt584a7363785c8/node/lt56b97e5c627c5/uu-no-19-tahun-2016-perubahan-atas-undang-undang-nomor-11-tahun-2008-tentang-informasi-dan-transaksi-elektronik
26   "Draft Revised Criminal Code [RKUHP] (Indonesia), 2019," accessed November 13, 2020, Article 304, https://www.hukumonline.com/pusatdata/detail/17797/rancangan-undang-undang-2019#
27   Interview 7, interviewed by Andrea Carson, 19 August 2020.
28   Ismail Hasani, "The decreasing space for non-religious expression in Indonesia," in *Religion, Law and Intolerance in Indonesia*, ed. Tim Lindsey and Helen Pausacker (London and New York: Routledge, 2016), 202.
29   "Criminal Code [KUHP] (Indonesia), 1946," accessed November 13, 2020, Article 156, https://www.unodc.org/res/cld/document/idn/indonesian_penal_code_html/I.1_Criminal_Code.pdf

Information and Electronic Transactions law (ITE), the latter leading to 30 months' jail and a US$10,000 fine.[30]

Numerous groups and individuals, including journalists, have used misinformation to play on Indonesians' fears of Islamophobia.[31] Groups found to have intentionally inflamed religious tensions for such purposes include Saracen and the Muslim Cyber Army.[32]

> During post-election protests in 2019, many protestors said they were motivated by online news and widely shared private messages that falsely reported attacks on Mosques and other forms of religious discrimination.[33]

Content that seeks to frame individuals as sympathetic to communism (it is illegal under Indonesia's Criminal Code to communicate communist ideology[34]) has also been prominent. President Jokowi has been variously claimed to be ethnically Chinese, and to be leading a government involved in Chinese conspiracies to influence Indonesian affairs.[35] A doctored image was once posted purporting to show Jokowi at a communist rally in 1955 – six years before he was born.[36] However blatant, such falsehoods have been known to gain traction, and are commonly used by political players to try to discredit opponents and incite public unrest.[37]

Misinformation as a political weapon

Prominent political figures have been among those employing hoaxes to advance their political objectives. An investigation by *The Guardian* in 2018 found links between the Muslim Cyber Army and Indonesian opposition parties, as well as the Indonesian military.[38] During the 2019 presidential election, the campaign teams behind Jokowi and his rival Prabowo Subianto were found to be "funding sophisticated social media operations to spread propaganda and disinformation through fake accounts."[39] A Prabowo spokesperson later decried the behaviour, saying it creates "a climate where voters become ever-more polarised and find it difficult to ascertain what is true and what is fiction – which, in the end, can only damage our ability to hold rational discourse."[40] Patterns in the timing and targeting of hoax crackdowns have also prompted some to accuse the state of attempting to "strengthen controls on oppositional information" in the lead-up to elections.[41]

Laws and regulations

Indonesia has a number of laws that it exercises in its fight against misinformation. The key laws are detailed below, including plans to update and amend the 1945 Criminal Code, and the new Ministerial Regulation no. 5/2020 launched as this report was going to print.

Criminal Code

Indonesia's Criminal Code, or Kitab Undang-Undang Hukum Pidana (KUHP), has been in operation since 1945, when independence from the Netherlands was declared. The code is a modified version of the previous Dutch-imposed code,[42] and has remained largely unchanged for more than 70 years. Recent attempts to rewrite the code have prompted widespread consternation within Indonesia.

In its current form, under Article 14(1) of the KUHP, people charged with spreading false information or news that intentionally causes public disorder can face ten years in prison.[43] Under Article 14(2), publishing false information that may reasonably be considered to cause public unrest can result in up to three years' jail.[44] And under Article 15,

30   Ismail Hasani, "The decreasing space for non-religious expression in Indonesia."
31   Andreas Harsono, "Indonesia's journalists grapple with Islamism," Human Rights Watch, published August 21, 2019, https://www.hrw.org/news/2019/08/21/indonesias-journalists-grapple-islamism
32   Lamb, "Muslim Cyber Army: a 'fake news' operation designed to derail Indonesia's leader."
33   Quinton Temby, "Disinformation, violence, and anti-Chinese sentiment in Indonesia's 2019 elections," *ISEAS*, no. 67 (2019), https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_67.pdf
34   Ibid.
35   Amy Chew, "Chinese army uniforms" in Indonesia: Another hoax to discredit Beijing, Widodo," *South China Morning Post*, July 29, 2020, https://www.scmp.com/week-asia/politics/article/3095217/chinese-army-uniforms-indonesia-another-hoax-discredit-beijing
36   Kieren Aris and Rachel Fielden, "Tackling online disinformation in Indonesia through media literacy: The redirect method," (Paper presented at Fake News and Elections in Asia Conference, Bangkok, Thailand, July 10-12, 2019), 307. Accessed November 13, 2020, https://asiacentre.org/wp-content/uploads/2019/09/Fake-News-Conference-Proceeding.pdf
37   Temby, "Disinformation, violence, and anti-Chinese sentiment in Indonesia's 2019 elections."
38   Lamb, "Muslim Cyber Army: a 'fake news' operation designed to derail Indonesia's leader."
39   Fanny Potkin and Augustinus Beo Da Costa, "Fact-checkers vs. hoax peddlers: A fake news battle ahead of Indonesia's election," *Reuters*, April 11, 2019, https://www.reuters.com/article/us-indonesia-election-fakenews-insight/fact-checkers-vs-hoax-peddlers-a-fake-news-battle-ahead-of-indonesias-election-idUSKCN1RM2ZE
40   Irawan Ronodipuro quoted in Tse Yin Lee, "Analysis: How effective was Indonesia's war on fake news in its election?," BBC Monitoring, published May 16, 2019, https://monitoring.bbc.co.uk/product/c200tf1I
41   Tapsell, "Indonesia's policing of hoax news increasingly politicised," 4.
42   "RKUHP Explainer: All the controversial articles in Indonesia's criminal code overhaul," *Coconuts Jakarta*, September 19, 2019, https://coconuts.co/bali/features/rkuhp-explainer-all-the-controversial-articles-in-indonesias-criminal-code-overhaul-2/.
43   Agung Nugroho, "Comparative study on hoax handling policies in Indonesia and Singapore," *Advances in Social Science, Education and Humanities Research* 343, (2019): 360.
44   Tapsell, "Indonesia's policing of hoax news increasingly politicised," 6.

information or news that is uncertain, exaggerated or incomplete, and that may cause public unrest, may result in up to two years' jail.[45]

Apart from controversy surrounding proposed amendments, the use of the Criminal Code in its current form as a weapon against online misinformation has attracted considerable commentary and criticism. Institute of Criminal Justice Reform chief Anggara Suwahju says "commotion among netizens (citizens of the internet)" shouldn't be enough to trigger the "chaos" article of the law.[46] Critics also say the code is a "rubber article," with ambiguous definitions allowing the Government freedom to interpret and apply the law to suit its own interests.[47] Despite these concerns, there is strong support in Indonesia for the proposition that the Bill is due for revision to be relevant to modern realities.[48]

KUHP has been used during periods of crisis and potential public disorder in recent years to prosecute alleged cases of online misinformation. For example, the National Police charged more than a dozen people under Article 14(2) with spreading fake news about a series of purported child kidnappings, and about the Lion Air flight that crashed in October 2018.[49] But efforts to quell the spread of fear in the community have sometimes led to punishment of less educated Indonesians who unwittingly shared false information while genuinely trying to build awareness about serious events.[50]

The Jokowi Government has shown a willingness to use the Criminal Code against political opponents. After the 2019 presidential elections a Prabowo campaign spokesman and an Opposition party politician were charged "on suspicion of subversion and spreading hoaxes."[51]

The Criminal Code has also been used to crack down on the use of the internet by separatists in West Papua. However, in these cases the activists have been accused of treason rather than spreading misinformation.[52]

The Government has invoked articles 14 and 15 of KUHP against the spread of misinformation about the COVID-19 pandemic.[53] Efforts to police COVID-related posts have also extended to crackdowns on criticism of the Government's handling of the pandemic, including "anyone caught insulting the President and other top officials in relation to COVID-19 policies," which can result in 18 months' prison.[54]

Draft revisions of the Criminal Code

The Government's declaration in 2018 of its plans to amend the KUHP was met with enthusiasm by some observers who felt it was overdue – and serious apprehension by others who feared it could lead to further tightening of restrictions on civil freedoms. The first public outline of the proposed revisions confirmed these fears, leading to widespread public protests and the consequent postponing of a vote on the Bill in September 2019. However, renewed parliamentary deliberation has been flagged.[55]

Under proposed Article 262(1), anyone who knowingly disseminates false information, resulting in public unrest, would be liable for a maximum prison term of six years, or a fine of Rp500 million ($AUD47,000 approx). Under 262(2), someone who spreads news they may suspect is a hoax, and that they may reasonably believe could incite public unrest, faces up to four years jail or a fine of Rp200 million ($AUD19,000 approx).[56] Article 263 states that

disseminating news or information that is uncertain, exaggerated or incomplete, and that may reasonably be believed to cause public unrest, could result in two years in prison or a fine of Rp50 million ($AUD4,500 approx).[57]

Other provisions with the potential to limit public expression cover criticism of the President or Vice President (up to 4.5 years' jail, or a Rp200 million fine) and of the Government (four years and Rp500 million). There are also provisions covering blasphemy "against the religion adopted in Indonesia"[58] (five years' jail or a Rp500 million fine), and up to 18 months' jail, or a Rp10 million fine, for defaming someone in public writing or imagery. However, it would not be criminal if doing so was in the public interest or in the accused's defence.[59]

Political debate

Indonesia's opposition politicians have been relatively circumspect on the proposed amendments, leading to the suggestion by the *Jakarta Post* of "a holy alliance between the ruling and opposition camps in the House to get the amended Criminal Code enacted into law."[60] While several high-profile political figures, including the deputy head of Indonesia's House of Representatives, have raised concerns that some articles in the Bill could be used against civil liberties, the main political parties have stated publicly that they stand behind the new draft.[61]

The draft Bill has attracted criticism from politicians in neighbouring Southeast Asian countries. But these critics have focused mainly on proposals affecting private and same-sex relationships.[62]

45   Nugroho, "Comparative study on hoax handling policies in Indonesia and Singapore," 360.
46   Tapsell, "Indonesia's policing of hoax news increasingly politicised," 6.
47   Article 19 and Aliansi Jurnalis Independen [AJI], *Freedom of Expression and the Media in Indonesia*, (London and Jakarta: Article 19 and Aliansi Jurnalis Independen, 2005), https://www.refworld.org/pdfid/4754185f0.pdf.
48   "RKUHP Explainer: All the controversial articles in Indonesia's criminal code overhaul."
49   "Beware what you share: Police step up war on hoaxes," *The Jakarta Post*, November 12, 2018, https://www.thejakartapost.com/news/2018/11/12/beware-what-you-share-police-step-war-hoaxes-fake-news.html
50   Tapsell, "Indonesia's policing of hoax news increasingly politicised," 3.
51   "Prabowo campaign spokesman arrested on subversion charges," *The Jakarta Post*, May 21, 2019, https://www.thejakartapost.com/news/2019/05/21/prabowo-campaign-spokesman-arrested-on-subversioncharges.html.
52   "Open letter on the increasing use of makar charges against Papuan activists to stifle freedom of expression," Amnesty International, published October 2, 2019, https://www.amnesty.id/open-letter-on-the-increasing-use-of-makar-charges-against-papuan-activists-to-stifle-freedom-of-expression/.
53   Tri Indah Oktavianti, "National Police detail tightened measures to combat COVID-19, support government policy," *The Jakarta Post*, April 8, 2020, https://www.thejakartapost.com/news/2020/04/08/national-police-detail-tightened-measures-to-combat-covid-19-support-government-policy.html.
54   Ibid.
55   Irfan Fathurohman, "ICJR urges parliament and government to not need to hurry to pass the Criminal Code bill," IDNTimes, published July 11, 2020, https://www.idntimes.com/news/indonesia/irfanfathurohman/icjr-desak-pemerintah-dpr-tidak-buru-buru-sahkan-ruu-kuhp/4
56   RKUHP, Article 262.
57   Ibid., Article 263.
58   Ibid., Article 304.
59   Ibid., Article 440.
60   "Criminalisation code," *The Jakarta Post*, July 18, 2019, https://www.thejakartapost.com/academia/2019/07/18/criminalization-code.html.
61   Aisyah Llewellyn, "Punitive measures: Indonesia's new draft criminal code" Lowy Institute, published February 9, 2018, https://www.lowyinstitute.org/the-interpreter/punitive-measures-indonesias-new-draft-criminal-code
62   Saifulbahri Ismail, "ASEAN lawmakers urge Indonesia to reject changes to criminal code," *Channel News Asia*, February 7, 2018, https://www.channelnewsasia.com/news/asia/asean-lawmakers-urge-indonesia-to-reject-changes-to-criminal-9935950

Public reactions

Initial public reaction in Indonesia to the proposal to amend the law was often positive. Human Rights Watch's Andreas Harsono had hoped the changes could establish a "rights-respecting" and "modernising and open" Indonesia.[63] Others hoped it was an opportunity to make the law less discriminatory and toxic.[64] However, goodwill soon started to recede as fears grew that the amendments would be "used as a political tool."[65] Harsono said "the current draft is much more draconian" than the existing law.[66] Because the current draft is intended to please religious conservatives, it is likely to be more discriminatory against religious minorities, LGBT groups and women, he feared.[67]

This sentiment was highlighted during the September 2019 protests.[68] As leading Indonesian law firm SSEK stated: "Whatever the intention, the reality is that the KUHP would criminalise more conduct than the current Criminal Code."[69]

Concerns about freedom of speech and the media have dominated criticisms of the draft Bill, particularly in the media sector. One critic argued it would allow the Government to "imprison anyone it dislikes," including journalists.[70] Others claim deliberate ambiguity in the law about who is being targeted will enable suppression of media freedom.[71]

While there is sympathy among media supporters for the notion that hoaxes are an "enemy" of freedom of expression, the problem cannot be tackled "by arresting the people who share" hoaxes.[72] Damar Juniarto of the Southeast Asia Freedom of Expression Network (SAFEnet) said that by punishing both the producers and sharers of hoaxes, the Bill had the scope to charge almost anyone in Indonesia, particularly given the country's low media literacy.[73]

Information and Electronic Transactions Law

The Information and Electronic Transactions Law (ITE) has been the primary law used against online misinformation and hoaxes in Indonesia. Essentially, it extends the Criminal Code for offences including hate speech, slander, defamation and blasphemy where they are deemed to have occurred on the internet.[74] And unlike the corresponding law in Singapore, Indonesian citizens can report perceived breaches of the law to authorities to prosecute.[75]

Article 28 is commonly used to prosecute online hoaxes. It covers anyone who "knowingly… disseminates false and misleading information resulting in consumer loss in Electronic Transactions."[76] In practice, it has been used much more broadly. Breaches carry up to six years' jail and a fine of Rp1 billion ($AUD95,000 approx).[77] Article 28 also bans the spread of information that aims to incite hatred or hostility based on ethnicity, religion, race and other social divisions (SARA).[78]

Article 35 targets "any person who knowingly and without authority… manipulates, creates, alters, deletes, [or] tampers with electronic information" to make it "seem to be authentic."[79] Breaches carry up to 12 years' jail and fine of Rp12 billion ($AUD1.14 million).[80]

ITE also criminalises online defamation,[81] with up to four years' jail and a fine of Rp750 million ($AUD 70,000).[82]

When the law was revised in 2016, it included a controversial "right to be forgotten" clause (Article 26(3)), allowing applications to internet providers and platforms to have personal information removed. Critics have complained that this provision can be misused by politicians to censor unwanted commentary.[83] Another revision, Article 40, enables the Government, either directly or through an intermediary, to disable access to "prohibited" content.[84]

Political debate

The 2016 revisions to the law have not been universally supported by the political establishment. Before the amendments were implemented, the House of Representatives deputy chairman called on free speech advocates to generate momentum to force changes to the defamation clause, which he feared would be used to silence the public.[85] In the end, the maximum jail sentence under its defamation clause was increased.[86] The vice chair of the lower house said the ITE law should be revised as it contained double standards,[87] while 2019 vice presidential candidate Sandiaga Uno promised to revise the law "to protect us from ourselves" and because "I don't want us to be using those laws to hit our opponents."[88]

63   Andreas Harsono, "Indonesia's president urges delay on Criminal Code vote," Human Rights Watch, published September 23, 2019, https://www.hrw.org/news/2019/09/23/indonesias-president-urges-delay-criminal-code-vote
64   Ibid.
65   Veronica Koman quoted in Llewellyn, "Punitive measures: Indonesia's new draft criminal code."
66   Interview 2, interviewed by Andrea Cars, August 20, 2020.
67   Ibid.
68   Human Rights Watch, *World report 2020* (Human Rights Watch, 2020), 276, https://www.hrw.org/sites/default/files/world_report_download/hrw_world_report_2020_0.pdf
69   Dewi Savitri Reni and Syarifah Reihana Fakhry, "RKUHP: What it means for criminal justice in Indonesia," SSEK, published March 3, 2020, https://www.ssek.com/blog/rkuhp-what-it-means-for-criminal-justice-in-indonesia
70   "Criminalisation code."
71   Ade Wahyudin (public defender at LBH Press) quoted in Arzia Tivany Wargadiredja, "Indonesia's answer to fake news is a threat to free speech," Vice News, published February 6, 2018, https://www.vice.com/en_asia/article/j5bq54/indonesias-answer-to-fake-news-might-be-a-threat-to-free-speech
72   Ibid.
73   Damar Juniarto (regional coordinator of SAFEnet) quoted in Wargadiredja, "Indonesia's answer to fake news is a threat to free speech."
74   Andreas Harsono, interviewed by Andrea Carson, August 20, 2020.
75   Ibid.
76   UU ITE, Article 28(1).
77   Ibid., Article 45(2).
78   SARA is an "Indonesian abbreviation for ethnicity, religion, race, and other social divisions" (Nathaneal Sumaktoyo, "Ethnicity and Jakarta's election," New Mandala, published February 13, 2017, https://www.newmandala.org/ethnicity-jakartas-election/.)
79   UU ITE, Article 35.
80   Ibid., Article 51(1).
81   Ibid., Article 27(3).
82   "ITE law aims to protect, manage electronic information, transactions," *The Jakarta Post*, October 27, 2016, https://www.thejakartapost.com/news/2016/10/27/ite-law-aims-to-protect-manage-electronic-information-transactions.html.
83   Nadine Freischlad, "Controversial "right to be forgotten" finds its way into Indonesian law," Tech In Asia, published December 1, 2016, https://www.techinasia.com/indonesia-recognizes-right-to-be-forgotten.; Krithika Varagur, "Indonesia poised to pass Asia's first "right to be forgotten" law," *Voa News*, November 7, 2016, https://www.voanews.com/east-asia/indonesia-poised-pass-asias-first-right-be-forgotten-law
84   UU ITE, Article 40.
85   "Lawmakers push for amendment of electronic law," *Tempo*, September 13, 2013, https://en.tempo.co/read/512919/lawmakers-push-for-amendment-of-electronic-law
86   "ITE law aims to protect, manage electronic information, transactions."
87   S. Sudhakar, "Ahmad Dhani imprisoned, Fahri Hamzah encourages revised LAW," Suara, published January 29, 2019, https://www.suara.com/news/2019/01/29/144219/ahmad-dhani-dipenjara-fahri-hamzah-dorong-uu-ite-direvisi
88   Vice-Presidential candidate Sandiaga Uno quoted in "Q&A: Sandiaga Uno on economic policy," New Mandala, published March 4, 2019, https://www.newmandala.org/qa-sandiaga-uno-on-economic-policy/

Popular reactions

Community organisations and sections of the media have been vocal critics of the ITE law, claiming it threatens freedom of speech and media freedom. Asep Komaruddin of the Legal Aid Institute for the Press said the requirement for "electronic system organisers" to delete information at the direction of courts[89] was a potential threat to press freedom.[90]

SAFEnet argued that the defamation components of the Bill did not distinguish between civil and criminal defamation, and were generally ambiguous,[91] allowing people to press charges against anyone that insults or provokes them.[92] SAFEnet identified problems with deletion of information,[93] defamation,[94] termination of online access,[95] and the threat of criminal punishment.[96,97] It argued that the law had multiple potential interpretations, resulting in legal uncertainty and creating a "revenge" dynamic, enabling people to use the law against their enemies. It also had the potential to be used as "shock therapy" against the public, causing a chilling effect.[98]

Amnesty International Indonesia's Usman Hamid highlighted issues with the wording of the law, saying "electronic information" could reasonably cover emails and text messages, and thus threaten gross invasions of personal privacy.[99] Moreover, he said the law did not clearly differentiate between insults and defamation as defined in the country's Criminal Code.[100] And MAFINDO's Septiaji Eko Nugroho said the criminalisation of online speech

should be a "last resort," and that the focus should be on "mediation in the name of restorative justice."[101]

Similar arguments have been mounted by international observers. Human Rights Watch and Amnesty International have both warned that the Jokowi administration's growing use of the ITE Law threatens free speech.[102] Freedom House took particular issue with the defamation clause, which often lands alleged perpetrators in extended pre-trial detention.[103] While some defamation charges never actually make it to court, it said the threat of pre-trial detention was used by the Government to intimidate others. Human Rights Watch and SAFEnet agree that the Government's focus should be on providing correct information to citizens, rather than criminalising what citizens say because they lack correct information.[104]

Academic views

Academics have also been critical of the content and application of the ITE law. Usman Hamid, a lecturer in law at Indonesia's Jentera School, argued that while the law was introduced ostensibly to provide protections for consumers online, "in practice, the Government and law enforcement officials have abused the law to silence political dissidents."[105] Others said a lack of clarity in the law's defamation provisions could result in silencing of some people and groups, including women who speak out against gender-based violence.[106] Provisions such as article 40, which the Government has used to disable access to prohibited online content, were also seen to "carry huge risks of power abuses."[107]

Dr Ross Tapsell of Australian National University says ITE provisions were used during the most recent general election campaign against ordinary Indonesians who were unknowingly sharing fake news about serious events such as natural disasters.[108] Tapsell believes the extent of the Government's intervention in this space is in part due to the absence of effective controls from global tech platforms.[109] He says the Government's overreach against citizens could fuel increased distrust towards the state and the police, and a diminishing of "Indonesia's generally open and vibrant public sphere."[110] This has been confirmed in public opinion polls.[111] Tapsell has proposed an alternative strategy of policing to focus on "syndicates" that spread fake news for political or monetary purposes.

Uses and consequences

SAFEnet, which monitors the use of the ITE law, says the law was used 263 times from its inception in 2008 to the end of 2018,[112] overwhelmingly against members of the public rather than members of particular groups. In 2017 and 2018, journalists and media professionals were targeted more than any other groups (apart from the public). The number of court cases relating to ITE has risen dramatically, from 20 in 2015 to 292 in 2018. According to SAFEnet, 7 per cent of cases brought under the ITE law have related specifically to hoaxes, 10 per cent to information manipulation, 22 per cent to hate speech, and 24 per cent to defamation.

89   UU ITE, Article 26.
90   "Right contained in ITE Law to delete negative news threatens press freedom: Activist," *The Jakarta Post*, October 28, 2016, https://www.thejakartapost.com/news/2016/10/28/right-contained-in-ite-law-to-delete-negative-news-threatens-press-freedom-activist.html
91   Enricko Lukman, "How Indonesia's problematic internet law will impede freedom of expression," SafeNet, published September 10, 2014, https://safenet.or.id/2014/09/how-indonesias-problematic-internet-law-will-impede-freedom-of-expression/
92   Ibid.
93   UU ITE, Article 26.
94   Ibid., Article 36.
95   Ibid., Article 40.
96   Ibid., Article 45.
97   "Persoalan UU ITE dan Praktik Pelanggaran Hak Digital di Indonesia," SAFEnet, published November 14, 2019, https://id.safenet.or.id/wp-content/uploads/2019/11/Persoalan-UU-ITE-dan-Pelanggaran-Hak-Digital-SAFEnet-2019.pdf
98   Ibid.
99   Hamid, "Indonesia's Information Law has threatened free speech for more than a decade. This must stop."
100 Ibid.
101 Septiaji Eko Nugroho (head of Mafindo) quoted in "Indonesian police intensify crackdown on fake news," *Voa News*, November 21, 2018, https://www.voanews.com/east-asia-pacific/indonesian-police-intensify-crackdown-fake-news
102 Lee, "Analysis: How effective was Indonesia's war on fake news in its election?"
103 Freedom House, *Freedom on the Net* 2016 (Freedom House, 2016), 424, https://freedomhouse.org/sites/default/files/2020-02/Freedom_on_the_Net_2016_complete_book.pdf
104 "Hundreds Arrested for 'Fake News' in Asia," *Courthouse News Service*, April 10, 2020, https://www.courthousenews.com/asia-arrests-hundreds-for-fake-news-on-virus/
105 Hamid, "Indonesia's Information Law has threatened free speech for more than a decade. This must stop."
106 Fitri Bintang Timur, "Unequal power makes women brunt of cyber law," SafeNet, published March 11, 2017, https://safenet.or.id/2017/03/unequal-power-makes-women-brunt-of-cyber-law/
107 Wahyudi Djafar quoted in "Revised ITE Law could hamper freedom of expression: Researcher," *The Jakarta Post*, October 31, 2016, https://www.thejakartapost.com/news/2016/10/31/revised-ite-law-could-hamper-freedom-of-expression-researcher.html
108 Tapsell, "Indonesia's policing of hoax news increasingly politicised," 3.
109 Ibid., 7.
110 Ibid.
111 Tribunnews.com, "Publik Lebih Takut Berbicara Politik di Era Presiden Jokowi? Berikut Hasil Survei LSI", *Tribunnews.com*, 5 November 2019, https://www.tribunnews.com/nasional/2019/11/05/publik-lebih-takut-berbicara-politik-di-era-presiden-jokowi-berikut-hasil-survei-lsi?page=all.
112 "Persoalan UU ITE dan Praktik Pelanggaran Hak Digital di Indonesia."

Defamation

While public officials can use the Criminal Code's defamation clause to quash criticism, the number of legal cases involving personal defamatory statements has increased since the introduction of the ITE law.[113] The defamation clause is also "periodically used to prosecute alleged religious defamation,"[114] and has more recently been used against critical messages on WhatsApp.[115]

Ethnic and religious protections

The ITE law has been used in conjunction with the law on the Elimination of Race and Ethnic Discrimination[116] to prosecute hoaxes.[117] A recent case saw a member of the infamous online syndicate Saracen sentenced to 32 months' prison for intentionally spreading information to incite hate on social media.[118] In another case, a man was sentenced to five years jail after being found guilty of spreading hate speech in a Facebook post that "questioned the faith of other Muslims."[119]

Crackdown on dissent

Hundreds of Indonesians have been prosecuted under the ITE law over comments critical of the Government and President Jokowi in recent years. During Jokowi's first term (2014-2019), 241 individuals were "criminalised for criticising authority figures of the Jokowi administration," according to Usman Hamid relying on unpublished Amnesty International figures.[120] About a third of those involved instances of purported "hate speech" and "insults" towards Jokowi, of which a majority were communicated through social media. Conversely, Tapsell found no evidence of anyone being prosecuted by the state for spreading falsehoods about Jokowi's opponent, Prabowo, during the 2019 election campaign.[121] The ITE law was also used to block access to WhatsApp, Facebook and Instagram features during the 2019 post-election riots in Jakarta "to avoid incitement" from the spread of misinformation.[122]

Critics of the Government's high-profile prosecutions of political dissidents claim this has encouraged attacks on dissidents by government supporters, who in some cases have responded with physical intimidation.[123] Attempts by dissidents to challenge their prosecutions have repeatedly failed; a total of seven applications for judicial review have all been denied.[124]

West Papua

The Government also used the law against critics in West Papua, the scene of a long-running struggle for independence. In 2019 human rights lawyer and West Papua defender Veronica Koman was charged under the ITE law for allegedly spreading fake news that caused unrest in the region.[125] In August of that year the Government used Article 40 of the ITE law to shut down internet access in West Papua.[126] Legal experts argued the move was an illegal attack on freedom of speech.[127] But the Government said the situation in West Papua demanded strong measures to reduce misinformation and restore order – even though protests at which the action was targeted had already stopped.[128]

Also in 2019, Facebook removed hundreds of accounts that regularly posted about West Papua on the grounds that they demonstrated "coordinated inauthentic behaviour."[129] Indonesia's Minister for Communication and Information denied any government role in this intervention.

COVID-19

The ITE law has been the Government's principal weapon-of-choice against alleged COVID-19 hoaxes. Among the targets have been people spreading false information about the pandemic, perpetrators of alleged "health equipment frauds"[130] and critics of the Government's handling of the crisis[131] and Jokowi's leadership.[132] By April 2020, the Government had made more than 80 arrests over alleged COVID-related fake news.[133] The actions drew claims that COVID-19 was being used by authorities to justify crackdowns on journalists critical of Jokowi and the Government.'[134]

Other misinformation laws

Several other laws that have potential applications in the fight against online hoaxes in Indonesia have been used more sparingly.

113 Freedom House, Freedom on the Net 2016, 437
114 Ibid.
115 "[Press release] SAFEnet sends Amicus Curiae for the Saiful Mahdi case," SAFEnet, published February 11, 2020, https://id.safenet.or.id/2020/02/rilis-pers-safenet-kirim-amicus-curiae-untuk-kasus-saiful-mahdi/
116 "Law No. 40 of 2008 on Elimination of Racial and Ethnic Discrimination (Jakarta): 2008" HUKUM Online, accessed November 13, 2020, https://www.hukumonline.com/pusatdata/detail/28539/node/1011/uu-no-40-tahun-2008-penghapusan-diskriminasi-ras-dan-etnis
117 Muhammad Hatta, "The spread of hoaxes and its legal consequences," International Journal of Psychosocial Rehabilitation 24, no. 3 (2020): 1756-1757.
118 "Indonesia court sentences administrator of 'fake news factory' Saracen to jail," The Straits Times, January 12, 2018, https://www.straitstimes.com/asia/se-asia/indonesia-court-sentences-administrator-of-fake-news-factory-saracen-to-jail
119 "Indonesian man arrested for Facebook post allegedly insulting Islam," Mid-Day, May 1, 2018, https://www.mid-day.com/articles/indonesian-man-arrested-for-facebook-post-allegedly-insulting-islam/19374167.
120 Hamid, "Indonesia's Information Law has threatened free speech for more than a decade. This must stop."
121 Tapsell, "Indonesia's policing of hoax news increasingly politicised." 4.
122 Karina M. Tehusijarana and Jessicha Valentina, "Jakarta riot: Government temporarily limits access to social media, messaging apps," The Jakarta Post, May 22, 2019, https://www.thejakartapost.com/life/2019/05/22/jakarta-riot-government-temporarily-limits-access-to-social-media-messaging-apps.html
123 Hamid, "Indonesia's Information Law has threatened free speech for more than a decade. This must stop."
124 Ibid.
125 Kate Lamb, "Outcry as Indonesia seeks to arrest renowned West Papua rights lawyer," The Guardian, September 5, 2019, https://www.theguardian.com/world/2019/sep/05/outcry-as-indonesia-seeks-to-arrest-renowned-west-papua-rights-lawyer
126 Reuters, "Rights group, journalists press Indonesian govt to lift internet curb in restive Papua."
127 Oce Madril and Herlambang P Wiratraman cited in "The Experts: The Indonesia Ministry of Communication and Informatics and the President Violates Human Rights and State Administrative Law," SAFEnet, published March 17, 2020, https://safenet.or.id/2020/03/experts-the-ministry-of-communication-and-information-and-the-president-violates-human-rights-and-state-administrative-law/
128 "Indonesian gov't justifies maintaining internet block in Papua despite officials declaring security restored," Coconuts Jakarta, August 28, 2019, https://coconuts.co/jakarta/news/indonesian-govt-justifies-maintaining-internet-block-in-papua-despite-officials-declaring-security-restored/.
129 Adi Renaldi, "Facebook Removed Hundreds of Accounts for Allegedly Spreading Propaganda in Indonesia," VICE News, October 10, 2019, https://www.vice.com/en_asia/article/ne8qbq/facebook-removed-hundreds-accounts-spreading-propaganda-indonesia
130 Petir Garda Bhwana, "Coronavirus-crackdown aimed at anti-President smears, hoaxes," Tempo, April 6, 2020, https://en.tempo.co/read/1328272/coronavirus-crackdown-aimed-at-anti-president-smears-hoaxes
131 Kanis Dursin, "Hoax stories hamper Indonesia's COVID-19 fight," Bangkok Post, July 6, 2020, https://www.bangkokpost.com/opinion/opinion/1946480/hoax-stories-hamper-indonesias-covid-19-fight
132 Oktavianti, "National Police detail tightened measures to combat COVID-19, support government policy."
133 "Hundreds Arrested for 'Fake News' in Asia."
134 "Indonesia used Covid-19 to silence criticism of government," Reporters Without Borders, April 16, 2020, https://rsf.org/en/news/indonesia-used-covid-19-silence-criticism-government

Law No. 17/2011 on State Intelligence

Articles 30-34 give the State Intelligence Agency (BIN) the power to conduct surveillance, information extraction and other tasks relating to "activities that threaten national interests and security"[135] such as terrorism, political violence and "cyber warfare."[136] To the extent that the law is applied to hoaxes, BIN is tasked with investigating and combatting the "potential dangers they pose,"[137] and assisting with any prosecution under the other relevant laws.

Reactions

Efforts to enact new laws to combat terrorism and other security threats, particularly after the 2002 Bali bombings, initially failed amid public opposition to giving BIN "Stasi-like secret police" powers and status.[138] A revised bill was eventually passed in 2011, but has remained the subject of controversy since a failed 2012 bid by a coalition of civil society organisations to have judicial review of 16 of its clauses. Concerns included the law's "vague language and broad reach."[139]

Human Rights Watch, while acknowledging the need to protect Indonesians from threats such as terrorism, has called for the law's repeal, saying "loose language… invites dangerous misuse."[140]

Uses and consequences

Since around 2015, BIN has been empowered to increase its focus on online threats,[141] and specifically tasked with managing conflicts and intelligence during elections.[142] This was apparent during the 2019 protests, when BIN worked alongside the National Police and National Defence Forces to "safeguard the country."[143] Under a new regulation introduced in July 2020, BIN operates directly under the control of the President, raising concerns that it may become another instrument used to quell political dissent.[144]

The COVID-19 pandemic has brought BIN's activities further into the public spotlight. As the national overseer of intelligence, BIN has been given responsibilities that have "extended to everything related to the pandemic," including even using its resources to conduct contact tracing to monitor its spread.[145] BIN has also provided public information about the pandemic, announcing in July "the discovery of five combinations of drugs to fight COVID-19."[146] Embarrassingly for an institution tasked with stamping out misinformation, BIN recently disproved its own "99 per cent accurate" predictions on COVID case numbers and had to retract them.[147]

Terrorism Act 2018

Article 1 of the Terrorism Act can be used against "perpetrators of the spread of hoaxes… if there is an element of threat of violence (that) creates an atmosphere of terror and widespread fear," according to a senior police official.[148] A senior government official said this provision could apply in the cases of hoaxes threatening violence against community members to stop them turning up at election polling stations, which he said would be a form of terrorism.[149] Article 1.4 defines the threat of violence as "speech, writing, picture, symbol or body language… which could create widespread fear."[150]

Reactions

Some members of Parliament have rejected the idea of using the Terrorism Act against hoaxes, arguing that the ITE law is sufficient to prosecute them.[151] Human rights activists have complained that the 2018 Terrorism Act revisions had tightened what were already restrictive and punitive blasphemy and defamation laws.[152] As of March 2019, no person had been charged with spreading hoaxes under the Terrorism Law.[153]

Ministerial Regulation no.5/2020

In December 2020, the Indonesian government launched its new Ministerial Regulation no.5/2020 to further regulate how private Electronic Service Operators (ESO) such as cloud computing service providers, social media platforms and other applications serving Indonesians should operate. In essence, the ministerial regulation provides more authority for the government to obtain data for law enforcement purposes; and to hold platforms accountable to remove misinformation and other content deemed as public disorder with a strict turnaround time of four hours. Failure to comply can result in heavy financial penalties and even internet blocking of platforms.

135 "Law No. 17 of 2011 on State Intelligence (Indonesia), 2011," accessed November 13, 2020, Article 31(a), https://www.icj.org/wp-content/uploads/2011/01/Indonesia-intelligence-law-draft-2011-eng.pdf

136 Ibid., General I.

137 Budi Gunawan and Barito Mulyo Ratmono, "Social media, cyberhoaxes and national security: Threats and protection in Indonesian cyberspace," *International Journal of Network Security* 22, no.1 (2020): 99-101.

138 Bhatara Ibnu Reza, "Why strengthening anti-terror laws is not the answer" Indonesia at Melbourne, published February 1, 2016, https://indonesiaatmelbourne.unimelb.edu.au/why-strengthening-anti-terror-laws-not-the-answer/

139 Ibid.

140 Elaine Pearson, deputy Asia director of Human Rights Watch, quoted in "Indonesia: Repeal new intelligence law," Human Rights Watch, published October 26, 2011, https://www.hrw.org/news/2011/10/26/indonesia-repeal-new-intelligence-law.

141 Ina Parlina, "Jokowi declares fight against disseminators of fake news," *The Jakarta Post,* December 30, 2016, https://www.thejakartapost.com/news/2016/12/30/jokowi-declares-fight-against-disseminators-of-fake-news.html

142 "BIN budget cuts to jeopardise regional election security, says spy chief," *Jakarta Globe*, September 10, 2015, https://jakartaglobe.id/context/bin-budget-cuts-jeopardize-regional-election-security-says-spy-chief/

143 Minister for Home Affairs Tjahjo Kumolo quoted in Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation, "National political stability under control: Home ministry," Cabinet Secretariet of the Republic of Indonesia, published September 26, 2019, https://setkab.go.id/en/national-political-stability-under-control-home-ministry/

144 "New regulation to have intelligence agency work directly under President Jokowi," *The Jakarta Post*, July 20, 2020, https://www.thejakartapost.com/news/2020/07/20/new-regulation-to-have-intelligence-agency-work-directly-under-president-jokowi.html

145 Tangguh Chairil, "Indonesia's intelligence service is coming out to counter COVID-19" *The Diplomat*, June 19, 2020, https://thediplomat.com/2020/06/indonesias-intelligence-service-is-coming-out-to-counter-covid-19/

146 Wahyudi Soeriaatmadja, "Eucalyptus necklace among "cures" raising alarm in Indonesia," *The Straits Times*, July 10, 2020, https://www.straitstimes.com/asia/se-asia/eucalyptus-necklace-among-cures-raising-alarm-in-indonesia

147 Chairil, "Indonesia's intelligence service is coming out to counter COVID-19."

148 Dedi Prasetyo quoted in Lis Yuliawati and Bayu Nugraha, "Penyebar Hoax Dijerat UU Terorisme, Polri: Tergantung Fakta Hukum," Viva, March 21, 2019, https://www.viva.co.id/berita/nasional/1132456-penyebar-hoax-dijerat-uu-terorisme-polri-tergantung-fakta-hukum?

149 Coordinating Minister for Political, Legal and Security Affairs Wiranto quoted in "Senior Indonesian minister suggests anti-terrorism law be used against election hoax spreaders," *Coconuts Jakarta*, March 2, 2019, https://coconuts.co/jakarta/news/senior-indonesian-minister-suggest-anti-terrorism-law-used-election-hoax-spreaders/

150 Krithika Varagur, "Activists: Indonesian counterterrorism law threatens civil liberties," *Voa News,* May 30, 2018, https://www.voanews.com/east-asia-pacific/activists-indonesian-counterterrorism-law-threatens-civil-liberties

151 House of Representatives member Nasir Diamil quoted in "Senior Indonesian minister suggests anti-terrorism law be used against election hoax spreaders."

152 Varagur, "Activists: Indonesian counterterrorism law threatens civil liberties."

153 "Senior Indonesian minister suggests anti-terrorism law be used against election hoax spreaders."

Government bodies

Ministry of Communication and Information Technology

In addition to using the law in the fight against online misinformation, Indonesia's Ministry of Communication and Information Technology (KOMINFO) has actively engaged with the online industry and the community through various programs and operations.

The ministry has been particularly focused on seeking cooperation from social media platforms to monitor and remove false online information. In January 2018, for example, it persuaded nine social media and messaging platforms to sign an agreement to tackle hoaxes and hate speech on their sites – a move widely seen as an attempt to shore up controls ahead of that year's local elections.[154] Under the agreement, platforms were obliged to remove accounts designated as prohibited by Indonesia's election watchdog, the *Bawaslu*. KOMINFO has also established an artificial intelligence system, Cyber Drone 9, that seeks out "targeted content" on websites.[155] Once the content is identified, internet service providers are told to remove it.

KOMINFO has launched multiple initiatives to engage with the community on online misinformation. In 2018 it announced it would begin regular briefings to detail and correct hoaxes it had identified.[156] It has launched a dedicated website, "Stophoax," which in conjunction with MAFINDO and the Google News Initiative seeks to educate Indonesians about how to spot fake information.[157] In a similar vein, KOMINFO established the "Siberkreasi" program in 2017 to educate and involve the public in overcoming "the spread of negative content through the internet such as hoaxes, cyberbullying and online radicalism."[158] The program also seeks to engage with the private sector, academics, civil society organisations and the media.[159] Despite these initiatives, digital literacy in Indonesia has been found to be "incidental and sporadic."[160]

KOMINFO has also been involved in at times controversial initiatives targeting alleged political hoaxes. Before the 2019 presidential election, a "war room" of 100 staff was tasked with identifying online hoaxes 24 hours a day.[161] KOMINFO was also a key player in the curbing of social media access during post-election protests, including the blocking of video and photo uploads and downloads on several social media platforms.[162] However, these efforts had limited impact due to misinformation continuing "apace" on the encrypted Telegram.[163]

Uses and consequences

KOMINFO has used its powers to quell the spread of misinformation during non-political crises. For example, the 2018 Sulawesi earthquake prompted the spread of false reports that authorities believed had the potential to incite panic. KOMINFO issued press releases "debunking" the hoaxes, and said they would arrest those suspected of initiating them.[164] More recently, it blocked access to some online locations to fight the spread of misinformation about the COVID-19 pandemic.[165]

National Cyber and Encryption Agency

Like KOMINFO, the National Cyber and Encryption Agency (BSSN) has been empowered by the Indonesian Government to assist with the fight against online hoaxes. Unlike KOMINFO, however, its operations appear to be confined largely to monitoring online activity, rather than prosecuting breaches.[166] Established in 2017, it has a Head of Agency who reports directly to President Widodo.

In the lead-up to the 2019 presidential election, the agency was tasked with helping intelligence agencies and law enforcement efforts to combat online misinformation and hoaxes.[167]

Reactions

Politically, BSSN has come under scrutiny over the limits of its authority. One senior member of the House of Representatives warned that such limits need to be enforced so that BSSN does not become "a censorship agency."[168]

Civil society groups have argued that BSSN could be more proactive in providing guidelines to individuals on how to protect themselves against cybercrime, particularly during the COVID-19 pandemic.[169]

---

154 La Batu, "Nine social media, messaging apps agree to combat fake news."
155 Ibid.
156 Kate Lamb, "Indonesian government to hold weekly "fake news" briefings," *The Guardian*, September 27, 2018. https://www.theguardian.com/world/2018/sep/27/indonesian-government-to-hold-weekly-fake-news-briefings
157 "About Stophoax.id at a glance," Stophoax, accessed November 13, 2020, URL: https://stophoax.id/tentang-kami/
158 "About Siberkreasi."
159 Ibid.
160 Novi Kurnia and Santi Indra Astuti, "Researchers find Indonesia needs more digital literacy education," *The Conversation*, September 26, 2017, https://theconversation.com/researchers-find-indonesia-needs-more-digital-literacy-education-84570
161 Jack Board, "Inside Indonesia's 'fake news' war room, fighting political hoaxes in election season," *Channel News Asia*, April 13, 2019, https://www.channelnewsasia.com/news/asia/indonesia-election-fake-news-war-room-fighting-political-hoaxes-11439398
162 Quinton Temby, "Indonesia's election riots offer a lesson on the perils of fake news," *South China Morning Post*, September 9, 2019, https://www.scmp.com/week-asia/politics/article/3026057/indonesias-election-riots-offer-lesson-perils-fake-news
163 Ibid.
164 Kate Lamb, "Sulawesi tsunami: Indonesia battles fake news as hoaxers spread panic," *The Guardian*, October 4, 2018, https://www.theguardian.com/world/2018/oct/04/sulawesi-tsunami-indonesia-battles-fake-news-as-hoaxers-spread-panic
165 "Indonesia wages war against coronavirus misinformation as hoaxes spread online," The Jakarta Post, February 3, 2020, https://www.thejakartapost.com/news/2020/02/03/indonesia-wages-war-against-coronavirus-misinformation-as-hoaxes-spread-online.html
166 Vience Mutiara Rumata and Ashwin Sasongko Sastrosubroto, "Net-attack 2.0: Digital post-truth and its regulatory challenges in Indonesia" *Advances in Social Science, Education and Humanities Research* 165, (2018): 119
167 Daniel Funke and Daniela Flamini, "A guide to anti-misinformation actions around the world," Poynter, accessed November 14, 2020, https://www.poynter.org/ifcn/anti-misinformation-actions/#indonesia
168 Dewi Nurita, "Fadli Zon urge National Cyber Agency hit the brake," *Tempo*, January 8, 2018, https://en.tempo.co/read/914656/fadli-zon-urge-national-cyber-agency-hit-the-brake
169 eltsazar A. Krisetya, "COVID-19 exposes vulnerabilities in our cyberspace," *The Jakarta Post*, April 1, 2020, https://www.thejakartapost.com/academia/2020/04/01/covid-19-exposes-vulnerabilities-in-our-cyberspace.html.

Uses and consequences

In addition to providing information that enables other agencies to prosecute alleged hoax spreaders, BSSN has helped Facebook to identify accounts linked to the Saracen hate group.[170] It has also launched programs to raise cyber-security literacy and awareness,[171] leading BSSN head Siburian to credit the agency with Indonesia's rise from 70 to 41 in the Global Cybersecurity Index in 2017.[172]

Timeline of Indonesia's "fake news" laws and policies

⌄

Table 1.1: Timeline of various laws and regulations implemented in Indonesia

Year	Legislation/Policy Development
1946	Indonesia adopts the minimally-revised **Criminal Code (KUHP)** that had been enforced by the Dutch colonial authorities.
2008	Information and **Electronic Transactions Law (UU ITE)** is adopted. First judicial review of UU ITE fails.[173]
2009	Second judicial review of UU ITE fails.
2010	Third judicial review of UU ITE fails.
2011	Law No. 17 of 2011 on State Intelligence is adopted.
2012	Susilo Bambang Yudhoyono government plans to revise ITE law, but it does not proceed
2013	The government, through the Ministry of Law and Human Rights, tables the revised Criminal Code Bill (RKUHP) and Criminal Procedural Code Bill (RKUHAP) into the People's Representative Council (DPR). However progress of the Bill stops following public opposition and the timing of upcoming 2014 election.[174] Fourth judicial review of UU ITE fails.
2015	Recently elected President Joko Widodo signals that the revised Criminal Code is a priority bill.[175] Discussions between the Government and legislature over the drafting of a new Criminal Code begin.[176]
2016	Fifth and sixth judicial reviews of UU ITE fail. UU ITE revisions are adopted, which include an expanded definition of defamation under Article 27(3), increased maximum jail sentences for defamation from four years to six years, and a reduction of the fine from Rp1 billion ($AUD94,800 approx) to Rp750 million ($AUD70,500 approx).
2017	**National Cyber and Encryption Agency (BSSN)** is established in law, effectively amalgamating the National Encryption Agency ("Lemsaneg") and the National Cyber Agency.
2018	[January] National Cyber and Encryption Agency (BSSN) Head of Agency is named, beginning its operations in earnest. [January] After 50 years of failed attempts, the government reveals its plans to revise the Criminal Code, causing concern from civil society groups in Indonesia. [May] Terrorism Act is revised only nine days after the deadliest terror attack since 2002 Bali Bombings. Seventh judicial review of UU ITE fails.
2019	[September] The scheduled vote on the revised Criminal Code inspires mass demonstrations in Indonesia that last for over a month, mainly led by student protestors. They were the largest student protests since those that were central to the fall of Suharto in 1998. President Widodo postpones vote on RKUHP.
2020	[December] Indonesia passes the controversial **Ministerial Regulation 5/2020**, which, amongst other things, requires digital platforms to remove content "against the public order" within 4 hours, under the threat of severe penalties (including blocking of platforms).

Source: Authors

---

170 "Facebook takes down hundreds of Indonesian accounts linked to fake news syndicate," *Reuters*, February 1, 2019, https://www.reuters.com/article/us-facebook-indonesia/facebook-takes-down-hundreds-of-indonesian-accounts-linked-to-fake-news-syndicate-idUSKCN1PQ3JS

171 General Hinsa Siburian, head of BSSN, quoted in Febi Trihermanto and Helen Brown, "Indonesia focused on cyber resilience, open to foreign cooperation," Australia Indonesia Centre, published November 12, 2019, https://digital.australiaindonesiacentre.org/news/insights/indonesia-focused-on-cyber-resilience-open-to-foreign-cooperation/

172 Ibid.

173 SAFEnet, 'Persoalan UU ITE dan Praktik Pelanggaran Hak Digital di Indonesia', *SAFEnet*, 14 November 2019, URL: https://id.safenet.or.id/wp-content/uploads/2019/11/Persoalan-UU-ITE-dan-Pelanggaran-Hak-Digital-SAFEnet-2019.pdf

174 Eddyono, Supriyadi Widodo, Abidin, Zainal, Arsil and Yuntho, Emerson, 'Brief notes on the proposed discussion of 2015 Criminal Code Bill', *National Alliance for Criminal Code Reform*, 26 March 2015, URL: https://elsam.or.id/wp-content/uploads/2015/08/Brief-Notes-on-the-Proposed-Discussion-of-2015-Criminal-Code-Bill.pdf

175 Ibid.

176 Indonesia at Melbourne, 'Indonesians better get ready for jail, as flawed new criminal code looks set to pass', *University of Melbourne* [website], 3 September 2019, URL:https://indonesiaatmelbourne.unimelb.edu.au/indonesians-better-get-ready-for-jail-as-flawed-new-criminal-code-looks-set-to-pass/

Conclusion

Misinformation poses a serious and destabilising threat in Indonesia due to a combination of historical, demographic and political factors. Indonesia's status as one of the largest internet-using populations and its low levels of educational attainment also present significant challenges for actors seeking to defend the citizenry against misinformation. The nation's conservative religiosity, combined with national attitudes of anti-communism and anti-atheism, ensure the list of prohibited discourse is considerably long. Lingering memories of autocratic repression, and more recent state interference in public discourse, feed fears of government overreach.

These factors have helped create an often unruly information environment, where incendiary attacks on religious, ethnic, gender, sexual, and political grounds are unfortunately not uncommon.

The 2019 post-election riots encapsulated the highly charged experience of misinformation in Indonesia. While rioters were initially prompted by Prabowo's repudiation of the "facts" of the election result, further unrest was stoked by false reports of government attacks on sacred mosques.

Several key aspects of the Indonesian Government's response to misinformation are worth restating. Firstly, its multilateral programs and civil society coalition building are encouraging. With low digital literacy levels, public education is essential. However, commitment to this approach is undermined as the Government relies upon more blunt and efficient measures to police misinformation.

Secondly, and to that point, the punitive criminalisation of misinformation is highly problematic. The Indonesian Government has shown readiness to use the police to arrest those suspected of spreading misinformation, which appears to be largely unchecked by other mechanisms of the state. There is evidence to suggest that these arrests are intended to have an intimidatory effect, since many cases do not make it to trial.

Thirdly, there is a clear conflict of interest in the definition and use of anti-misinformation laws. For example, the prohibition of defamatory or insulting statements against the President has been used to prosecute those critical of the Government. These laws can be used to repudiate opposition and deny the validity of unwanted commentary. This was seen during the post-election riots, in West Papua and against opposition politicians.

Finally, the revised draft of the Criminal Code, which has partisan support, places further restrictions on civil liberties. While Indonesia has fair elections, there appears to be a ruling elite, existing across political lines, that has sought to consolidate its power at the expense of the civil liberties achieved since the fall of Suharto.[177] According to some commentators, this continued erosion of civil liberties suggests the country may be in the midst of protracted "democratic regression."[178] External statistics support this view. While press freedom has improved over the past decade (albeit still ranking in the bottom quartile globally),[179] internet freedom[180] and political and civil rights[181] have declined – particularly in the last couple of years.

There is an attendant complexity, however, to Indonesia's handling of misinformation. While questions are being asked of the Government's use of its anti-misinformation laws, the link between misinformation and disruptive public unrest in Indonesia is hard to ignore. As the existence of online shadow groups such as Saracen and the Muslim Cyber Army show, actors in Indonesia have exploited this reality to stoke the country's religious and political sensitivities in pursuit of their own goals. As such, any evaluation of the Government's measures to combat misinformation requires nuanced consideration of Indonesia's complex cultural, demographic and political realities.

---

177 Eve Warburton and Edward Aspinall, "Explaining Indonesia's democratic regression: Structure, agency and popular opinion," *Contemporary Southeast Asia* 41, no, 2 (2019): 268.
178 Ibid.
179 "Indonesia," Reporters Without Borders, 2020, https://rsf.org/en/indonesia.
180 "Freedom on the net 2019: Indonesia," Freedom House, 2019, https://freedomhouse.org/country/indonesia/freedom-net/2019
181 "Freedom in the world 2020: Indonesia," Freedom House, 2020, https://freedomhouse.org/country/indonesia/freedom-world/2020

CHAPTER 2

Singapore's approach to online misinformation

Introduction

In January 2018, Singapore's ruling People's Action Party (PAP) appointed a parliamentary committee to investigate the spread of misinformation and deliberate falsehoods online. In its report later that year, the committee found that proliferation of online falsehoods posed a growing threat[1] to social cohesion, public confidence in government institutions, democracy and national sovereignty. The report proposed a new multi-pronged offensive, focusing on the roles of journalists, fact checkers, technology companies, the Government and citizens. Among its proposals was public education to help Singaporeans identify misinformation; training of journalists to enhance quality and accuracy; and further regulation of technology companies.

But arguably the most consequential proposal was for new mechanisms to enable swift government intervention to provide the necessary "scope, speed and adaptability" to combat the problem.[2] This led to the introduction in April 2019 of the Protection from Online Falsehoods and Manipulation Act (POFMA), providing sweeping new powers to ministers to call out instances of falsehoods and to prosecute those responsible – including the technology companies that host alleged breaches. POFMA quickly superseded other laws as the Government's primary tool in the war against online falsehoods. At the same time, detractors claim it also became a new and highly effective weapon to silence critics, suppress freedom of speech, and further entrench government power.

In this chapter, we look at the evolution of the Government's approach to online misinformation over the past decade, culminating in the enactment of POFMA, and how the Government's approach fits in with Singapore's unique historical, demographic and cultural characteristics. A timeline of the implementation of "fake news" laws and policies is tabled at the conclusion of the chapter (Table 2.1).

Background and context

As a city-state located in the heart of Southeast Asia, Singapore has a relatively small population of around 5.7 million, comprising diverse cultures and ethnicities.[3] Its multi-racial and multi-faith demography is central to Singapore's identity – and to the policy approaches of the ruling party, which has been in power continuously since 1959.

The importance of maintaining social cohesion amid Singapore's "fragile racial and religious harmony" is often invoked by politicians when introducing and justifying new laws – especially those that establish more intrusive governmental powers.[4] This theme has been continued when it comes to measures to tackle online misinformation.

The PAP's continuous hold on power for more than six decades has been marked by a combination of authoritarian and paternalistic themes, with frequent allusions to "the public interest" being used to justify government determinations – both in public statements and the text of legislation. Hence, restrictive anti-misinformation measures, including POFMA, have been accompanied by references to "right things"[5] and "what is in the public interest," as determined by the Government.[6]

---

1   Ministry of Communications and Information and Ministry of Law, *Deliberate and Online Falsehoods: Challenges and Implications* (Singapore: Parliament of Singapore, 2018), https://www.nas.gov.sg/archivesonline/government_records/Flipviewer/grid_publish/6/6797717d-f25b-11e7-bafc-001a4a5ba61b 06012018Misc.10of2018/web/html5/index.html?launchlogo=tablet/GovernmentRecords_brandingLogo_.png&pn=1

2   Parliament of Singapore, *Report of the Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures*, (Singapore: Parliament of Singapore, 2018), 164. https://sprs.parl.gov.sg/selectcommittee/selectcommittee/download?id=1&type=subReport

3   74% of Singaporeans identify as Chinese, while Malays (13%), Indians (9%) and those nominating 'Other' (3%) are the other notable ethnic groups that live in Singapore (Department of Statistics Singapore 2020). Religion provides even greater diversity as a marker, with Buddhists (34%), Christians (18%), Muslims (14%), Taoists (11%), Hindus (5%) and non-religious people (16%) representing significant proportions of the population. SBS, "Cultural Atlas", *SBS* (2016), https://culturalatlas.sbs.com.au/singaporean-culture/singaporean-culture-greetings#singaporean-culture-greetings

4   Howard Lee and Terence Lee, "From contempt of court to fake news: public legitimisation and governance in mediated Singapore," *Media International Australia* 173, no. 1 (2019): 83-84; Alex Au Waipang, "Singapore bloggers wary of news site licence scheme," Committee to Protect Journalists, published June 4, 2013, https://cpj.org/2013/06/singapores-news-site-license-plan-raises-questions/

5   Au Waipang, "Singapore bloggers wary of news site licence scheme."

6   Parliament of Singapore, *Protection from Online Falsehoods and Manipulation Act* Parliament of Singapore, 2019, https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625

The Government's approach to tackling misinformation

Since its introduction in 2019, the Protection from Online Falsehoods and Manipulation Act (POFMA) has been the primary tool employed by Singapore's Government in the fight against online misinformation. The Government has used the law's extensive coercive powers to force the removal or amendment of online content it deems to be false or misleading – including multiple instances of false content about COVID-19.

Controversially, the Government has also frequently targeted online political content, drawing accusations from rival politicians, journalists, academics and technology companies that it is using the Act as a weapon not just against misinformation but to silence political opponents and further restrict freedom of speech and the media.[7]

In this respect its approach has parallels with that of the Indonesian Government, which has also been accused of using anti-misinformation laws to silence its political opponents in the lead-up to national elections. As in Indonesia, the Government of Singapore has also cited the need to maintain harmony between the nation's diverse ethnic groups as justification for a heavy-handed approach to online misinformation. And in Singapore, as in Indonesia, critics have highlighted the inherent conflicts of interest in laws that give the Government extensive powers and discretion to decide what constitutes misinformation.[8]

Another notable element of the Singapore Government's approach to online misinformation, including since the advent of POFMA, has been an emphasis on the need for speed in responding to and prosecuting cases. The imperative was described by one parliamentarian in these terms: "A lie can travel halfway around the world while the truth is still putting on its shoes."[9] A potential casualty of the high-speed approach, however, can be fairness – and the judiciary's ability to adequately adjudicate the merits of each case.

Laws and regulations

Controversy surrounding the Singapore Government's approach to tackling online falsehoods and misinformation long pre-dates the introduction of POFMA. Several other laws and regulations have been utilised over the past decade or so – and continue to be used – to clamp down on alleged online misinformation and other activities deemed by the Government to be against the public interest. And controversy has often followed.

Sedition Act

The Sedition Act 1948 has been used a number of times to prosecute the authors of online statements to which the Government has objected. Critics say the absence of a definition of sedition in the law[10] leaves wide scope for people to be accused of inciting contempt of the Government or ill-will among the citizenry under the Sedition Act, even when they have claimed a defence of truth.[11] An example of this was the charging of cartoonist Leslie Chew with sedition in 2013 for cartoons published on a Facebook page about a fictitious country, "Demon-cratic Singapore." The site makes clear that all characters, parties, etc. are fictional. He was charged with sedition because of two cartoons, one about race, claiming that Singapore's "Malay population was declining" – something he asserted was "a fact."[12]

In another recent case, the Government pursued charges against *The Real Singapore,* an independent online news site that came under scrutiny for publishing alleged falsehoods relating to ethnic groups in Singapore. The case centred on an article about an alleged dispute between a Filipino family and members of the Tamil community. The news site was judged to have published "deliberately fabricated articles"[13] that

---

7   Howard Lee and Terence Lee, "From contempt of court to fake news: public legitimisation and governance in mediated Singapore,; Alex Au Waipang, "Singapore bloggers wary of news site licence scheme," Committee to Protect Journalists.
8   Karishma Vaswani, "Concern over Singapore's anti-fake news law," *BBC News*, 4 April 2019, https://www.bbc.com/news/business-47782470
9   "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill," Parliament of Singapore, 8 May 2019, 94, Part 2, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-367
10   Human Rights Watch, *Kill the Chicken to Scare the Monkeys: Suppression of Free Expression and Assembly in Singapore* Human Rights Watch, 2017, 43, https://www.hrw.org/sites/default/files/report_pdf/singapore1217_web.pdf
11   Ibid., 45.
12   Human Rights Watch, *Kill the Chicken to Scare the Monkeys*, 47-48.
13   "Singaporean authorities shut down *The Real Singapore* news website," Committee to Protect Journalists, published May 5, 2015, https://cpj.org/2015/05/singaporean-authorities-shut-down-the-real-singapo/.

undermined national harmony[14] – a common justification for Sedition Act prosecutions.[15] The site was shut down, and its editors jailed for 8-10 months.[16]

Online News Licensing Scheme

The 2013 Online News Licencing Scheme, which extends content standards established under the Broadcasting Act and Internet Code of Practice,[17] has also been used against perceived online falsehoods. Under the framework, news sites meeting certain criteria – such as having at least 50,000 unique Singaporean visitors each month – are required to pay $S50,000 annually for a licence, and can be ordered to remove prohibited content[18] within 24 hours, or be shut down.[19] Licenced websites are banned from receiving financial support from foreign sources.[20] And in response to concerns the framework would constrain individuals' freedom of speech online,[21] the Government stated that personal blogs would not be covered "so long as they do not morph into news sites."[22]

Like other laws and measures, the licensing framework does not provide specific definitions of fake news or misinformation. However, the Government has drawn on familiar themes to justify its use. At the time of its introduction, the Minister for Communications and Information said the new rules aim to "to protect the interest of the ordinary Singaporean" and "to make sure they read the right things."[23] One of its stated purposes is to prohibit "content that undermines racial or religious harmony."[24] This aim was invoked against *The Real Singapore* for an alleged breach of content standards, leading to its shutdown order[25] concurrently with its prosecution under the Sedition Act (see above).

Critics have claimed that the new licencing framework was established in response to the PAP's historically poor election result in 2011, which was attributed in part to the increasing prominence of online news and blogs.[26]

Defamation Act

The Defamation Act,[27] covering slander, libel and other falsehoods, has been "the Government's most powerful non-criminal weapon" against its opponents, according to the international organisation Human Rights Watch.[28] It claims the law has been used to sue, bankrupt and intimidate government critics. Damages owed by those found guilty of defaming the Government have been as high as S$150,000,[29] and criminal defamation charges can lead to jail time of up to two years.[30]

The large penalties under the Defamation Act are claimed to have served as a highly effective deterrent against speaking ill of the Government,[31] with self-censoring widely observed and practised,[32] and Government-initiated defamation actions invariably succeeding.[33] Prime Minister Lee Hsien Loong has invoked the Act several times, including a defamation suit against *The Online Citizen* (TOC) editor Terry Xu over a story detailing a family feud between him and his siblings, which was before the court at the time of writing.[34] PM Lee has also filed a lawsuit against a financial blogger for sharing a story about his alleged involvement in money laundering.[35] In a separate case, PM Lee also unsuccessfully demanded that Facebook remove an Australian-based blogger's "false and malicious" post.[36] While the law's criminal provisions are used rarely,[37] one writer for *The Online Citizen* is currently facing trial over an article alleging government corruption.[38]

Protection from Harassment Act

The Protection from Harassment Act (POHA), introduced in 2014, outlaws and provides remedies against various actions, including "civil remedies related… to false statements of fact."[39]

Section 15 of the Act allows individuals to apply for court orders against false statements published about them.[40] An attempt by the Government to use the Act against critical reporting of a ministry[41] was disallowed by the High Court on the grounds that the

14 Pearl Lee, "TRS co-founder Yang Kaiheng jailed 8 months for sedition," *The Straits Times,* June 28, 2016. https://www.straitstimes.com/singapore/courts-crime/trs-co-founder-yang-kaiheng-jailed-8-months-for-sedition

15 Human Rights Watch, *Kill the Chicken to Scare the Monkeys,* 46.

16 Lee, "TRS co-founder Yang Kaiheng jailed 8 months for sedition."

17 Infocomm Media Development Authority, *Internet code of practice* (Infocomm Media Development Authority, 1997), https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/Regulations/Codes-of-Practice/Codes-of-Practice-Media/PoliciesandContentGuidelinesInternetInterneCodeOfPractice.pdf

18 As outlined in the Internet Code of Practice 1997, which covers all licenced 'Internet Service Providers and Internet Content Providers' – 'Prohibited material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws' (pp. 1-2)

19 Human Rights Watch, *Kill the Chicken to Scare the Monkeys*, p. 49.

20 Paul Meyer, "Singapore's First Election Under the Fake News Law," *The Diplomat,* July 7, 2020. https://thediplomat.com/2020/07/singapores-first-election-under-the-fake-news-law/

21 Au Waipang, "Singapore bloggers wary of news site licence scheme."

22 "What is the licensing framework for online news sites all about?," Singapore Government, published June 18, 2013, https://www.gov.sg/article/what-is-the-licensing-framework-for-online-news-sites-all-about

23 Au Waipang, "Singapore bloggers wary of news site licence scheme."

24 Infocomm Media Development Authority. *Fact Sheet - Online news sites to be placed on a more consistent licensing framework as traditional news platforms* (Infocomm Media Development Authority, 2019), https://www.imda.gov.sg/news-and-events/Media-Room/archived/mda/Media-Releases/2013/fact-sheet--online-news-sites-to-be-placed-on-a-more-consistent-licensing-framework-as-traditional-news-platforms

25 Valerie Koh, "Govt orders shutdown of *The Real Singapore,*" *Today Online,* May 4, 2015, https://www.todayonline.com/singapore/mda-suspends-licence-socio-political-website-real-singapore

26 Meyer, "Singapore's First Election Under the Fake News Law."

27 Parliament of Singapore, *Defamation Act (Singapore)* (Parliament of Singapore, 1965), https://sso.agc.gov.sg/Act/DA1957

28 Human Rights Watch, *Kill the Chicken to Scare the Monkeys,* 96.

29 Lydia Lam, "PM Lee sues blogger Leong Sze Hian for defamation over sharing of article," *Channel News Asia,* December 7, 2018. https://www.channelnewsasia.com/news/singapore/pm-lee-sues-blogger-leong-sze-hian-defamation-libellous-article-10999710

30 Parliament of Singapore, *Penal Code* (Singapore) (Parliament of Singapore, 1972), Section 499, https://sso.agc.gov.sg/Act/PC1871?ProvIds=pr499-

31 Ibid.

32 Ibid., 6

33 Ibid., 96.

34 Amy Gunia, "Singapore's prime minister threatens website editor with libel," *Time,* September 2, 2019, https://time.com/5666835/singapore-prime-minister-lee-hsien-loong-libel/; https://www.straitstimes.com/singapore/courts-crime/pm-lee-hsien-loongs-defamation-suit-against-tocs-terry-xu-begins-monday

35 Fathin Ungku, "Singapore PM files defamation suit against blogger who shared article on Facebook," *Reuters,* December 5, 2018, https://www.reuters.com/article/us-singapore-politics-malaysia-scandal/singapore-pm-files-defamation-suit-against-blogger-who-shared-article-on-facebook-idUSKBN1O414L

36 Belmont Lay. "Facebook declines S'pore govt request to take down States Times Review post linking PM Lee with 1MDB," *Mothership,* November 10, 2018, https://mothership.sg/2018/11/facebook-turns-down-singapore-request/

37 Human Rights Watch, *Kill the Chicken to Scare the Monkeys,* 118.

38 Lam, "PM Lee sues blogger Leong Sze Hian for defamation over sharing of article."

39 Parliament of Singapore, *Protection from Online Harassment Act (Singapore)* (Parliament of Singapore, 2014), https://sso.agc.gov.sg/Act/PHA2014.

40 Ibid., section 15.

41 Human Rights Watch, *Kill the Chicken to Scare the Monkeys,* 100

Government is not a person, and that the reporting was not false.[42] This helped set the scene for POFMA a few years later, with the Ministry of Law stating in response to the High Court's POHA ruling: "The Government will study the judgment, and consider what further steps it should take to correct the deliberate spreading of falsehoods."[43]

Under amendments passed in 2020, entities including companies can now use POHA to obtain remedies against online falsehoods including stop, correction and disabling orders,[44] similar to remedies available under POFMA. The Government and its agencies – to the dismay of critics – remain exempt from prosecution under the law.[45]

Protection from Online Falsehoods and Manipulation Act (POFMA)

POFMA is the primary legislative instrument now used by the Singapore Government to tackle online falsehoods. The Act, which became law in 2019, incorporates and significantly expands

upon some previous legislative measures, and is the first law created specifically to target the issue.

It bestows extensive powers on the Government and its ministers. Under Part 3, any minister can declare information to be "false or misleading" and force its publisher to apply a correction notice or remove the material.[46] Ministers can use this power if they believe publication of the statement is against the "public interest."[47] Both criteria, the charge of "false and misleading" and "against the public interest," must be met. Under Part 4, ministers can order internet intermediaries (such as social media platforms and internet service providers) to remove a false article of information from their web locations.[48] And Part 5 allows ministers to instruct internet intermediaries to block access to declared online locations if they have received at least three POFMA orders.[49] This can be three pieces of content that are subject to the same order; it does not necessarily need to be three separate orders.[50]

The Act defines a "statement of fact" as "a statement which a reasonable person seeing, hearing or otherwise perceiving

it would consider to be a representation of fact."[51] A statement is deemed to be false "if it is false or misleading, whether wholly or in part, and whether on its own or in the context in which it appears."[52] Controversially, however, the Act does not seek to define "misleading."

Penalties for breaches of the Act are significant. 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$1 million in fines plus $100,000 per day of non-compliance per section 27 of POFMA. These penalties also apply to fake online accounts or bots being used to spread online falsehoods.[53] Internet companies that decline to disable access to locations of false statements face fines of up to S$20,000 per day up to a total of $500,000.[54]

Legal experts have suggested that POFMA allows the Government to effectively force internet intermediaries to track their users' viewing habits and keep records of this information,[55] adding to concerns about privacy on the internet.[56]

---

42 Ibid., 101
43 Ibid., 102-103.
44 Parliament of Singapore, *Protection from Online Harassment Act (Singapore)*, section 15.
45 Jalelah Abu Baker, "Exemption of Government from being sued under POHA amendments a "glaring omission": Pritam Singh," *Channel News Asia,* May 7, 2019, https://www.channelnewsasia.com/news/singapore/exemption-government-sued-under-poha-amendments-pritam-singh-11511118.
46 Parliament of Singapore, *Protection from Online Falsehoods and Manipulation Act* , section 7.
47 See *Protection from Online Falsehoods and Manipulation Act*, section 4, for definition and section 7; Section 7 defines statements against the public interest once they are 'prejudicial to Singapore's security', 'public health, safety, tranquillity or finances', its relations with other countries, they might influence the outcome of elections, 'Incite feelings of enmity, hatred or ill-will between different groups of persons', or 'Diminish public confidence in the government.'
48 Parliament of Singapore, *Protection from Online Falsehoods and Manipulation Act*, Part 4.
49 Ibid., section 32.
50 Ibid., section 40
51 Ibid., section 2.
52 Ibid.
53 "Singapore Fake News Laws: Guide to POFMA (Protection from Online Falsehoods and Manipulation Act)," Singapore Legal Advice, published February 3, 2020, https://singaporelegaladvice.com/law-articles/singapore-fake-news-protection-online-falsehoods-manipulation/
54 Shibani Mahtani, "Singapore introduced tough laws against fake news. Coronavirus has put them to the test," *Washington Post,* March 16, 2020, https://www.washingtonpost.com/world/asia_pacific/exploiting-fake-news-laws-singapore-targets-tech-firms-over-coronavirus-falsehoods/2020/03/16/a49d6aa0-5f8f-11ea-ac50-18701e14e06d_story.html.
55 Jennifer Daskal, "This "fake news" law threatens free speech. But it doesn't stop there," *New York Times,* May 30, 2019, https://www.nytimes.com/2019/05/30/opinion/hate-speech-law-singapore.html.
56 Ibid.

The use of POFMA

Critics of the Government

The first use of POFMA came in November 2019 in the form of a correction order against Progress Singapore Party member Brad Bowyer, in response to a Facebook post implying government control of investments by government-linked companies.[57] The Minister of Finance said the post was false and "undermines public trust in government."[58] Since then, the law has been used multiple times against outspoken critics of the Government, including *New Naratif*[59] and Lawyers for Liberty (LFL – a Malaysian NGO), which posted allegations that the Singapore Prisons Service committed human rights abuses during executions.[60] LFL refused to obey a POFMA order "a correction direction" to juxtapose the alleged falsehoods with "the facts" according to the government. This refusal prompted the Government to block access to its website.[61]

Khairulanwar Zaini found that "most of these orders have been directed at opposition politicians or anti-establishment critics."[62] According to the online website *POFMA'ed*,[63] which regularly reports about uses of POFMA orders, 31 out of 71 POFMA orders relate to ruling party critic Alex Tan and his various webpages. See Box 2.1.

Box 2.1 Alex Tan Case Study

Alex Tan is a Singapore-Australian blogger and former opposition candidate who is an outspoken critic of the Singaporean government. He has lived in Australia in recent years yet maintained a consistent online presence in Singapore, writing at one time or another for several websites including *The Real Singapore*, which was forced to shut down by the Singapore Media Development Authority.[64]

Central to why he has written for so many online publications is that the Singaporean government has been active in closing them – and their associated Facebook pages. In response, Tan has repeatedly started a "new page from zero", as he puts it.[65]

As of July 2020, he has been implicated in more POFMA orders than anyone else with 31 of 71 total orders, 14 of which have been issued to him directly. These include orders for false information relating to misquotes of government ministers, the availability of face masks, COVID-19 outbreaks and arrests and POFMA criticism. While he contends that he has "achieved what I intended which is exposing the hypocrisy of the Singaporean government", others observe that his websites are "known more for the vehemence rather than the accuracy of [their] frequent diatribes against the PAP government."[66] His websites have been labelled "very anti-government in rhetoric", with "no fact checking – they clearly make up stuff."[67] The PAP argue that Tan has "repeatedly conveyed falsehoods and not complied with any of the POFMA directions".[68]

The POFMA orders targeting Tan include correction direction orders, orders for Facebook to disable access to his various pages, and deeming his Facebook pages a 'Declared Online Location'. Tan is the first to receive a DOL. Under a DOL, Tan's Facebook pages are required to declare themselves as such, notifying visitors of their "history of communicating falsehoods."[69] Tan is also not able to derive financial benefit from these pages.

As a result of these disabling measures, Tan's once substantial Facebook followership of almost 60,000 has dwindled to about 3000.[70]

Tan is based in Australia and his capacity to ignore POFMA orders arguably demonstrates POFMA's inability to counter claims of foreign disinformation.

Nonetheless, Tan's case shows what tools the government has at its disposal to combat alleged misinformation: First, to demand that citizens adhere to its correction and takedown orders and, failing that, to demand that the online platforms respond. Facebook was compelled to comply with the Government's demand to revoke local access to Tan's website, despite voicing concern for the precedent POFMA sets about limiting freedom of expression in Singapore.[71]

---

57   "Fake news law invoked for the first time over Facebook post," *The Straits Times,* November 26, 2019, https://www.straitstimes.com/politics/fake-news-law-invoked-for-the-first-time-over-facebook-post.
58   Ibid.
59   "Thum Ping Tjin, *New Naratif* to challenge POFMA notice despite compliance."
60   "Singapore: Use of Anti-Fake News Law reveals institutional framework that undermines the promotion and protection of human rights," FORUM-ASIA, published February 11, 2020, https://www.forum-asia.org/?p=30931.
61   Khairulanwar Zaini, "Singapore in 2019: In holding pattern," *Southeast Asian Affairs*, no. 1 (2020): 305
62   Ibid.
63   Teo Kai Xiang, "About," POFMA'ed, accessed November 13, 2020, http://pofmaed.com/.
64   Other sites Tan has written for were: Temasek Review News, Straits Times Review (later changing the name to States Times Review), Singapore States Times, National Times Singapore, among others.
65   Alex Tan quoted in Wilson, Cameron, 'This man's Facebook page was blocked for spreading false information about the coronavirus', *BuzzFeed News*, 19 February 2020, URL: https://www.buzzfeed.com/cameronwilson/singapore-facebook-fake-news-law-alex-tan-coronavirus
66   Zaini, Khairulanwar, 'Singapore in 2019: In Holding Pattern', *Southeast Asian Affairs*, 2020(1), p. 305.
67   Kirsten Han, Interview #6
68   Minister for Communications and Information S. Irawan quoted in 'This man's Facebook page was blocked for spreading false information about the coronavirus'.
69   Ministry of Communications and Information, 'The "Singapore States Times" and Alex Tan's Facebook pages declared as declared online locations under POFMA' [Media release], 6 May 2020, URL: https://www.pofmaoffice.gov.sg/documents/media-releases/2020/May/pofma-pr-mci-06may2020-01.pdf
70   Xiang, Teo Kai, 'About', *POFMA'ed* [website], 2020.
71   Facebook spokesperson quoted in Tham, Yuen-C, 'Facebook blocks access in Singapore to States Times Review page for breaching Pofma', *The Straits Times*, 18 February 2020, URL: https://www.straitstimes.com/politics/facebook-blocks-access-to-states-times-review-page

Independent media have been the target of 33 out of 71 POFMA orders. Apart from Tan, who is included in this category, other independent media operators to have faced POFMA orders include Kirsten Han and PJ Thum as well as *The Online Citizen*, *AB-TC City News* and *The Independent Singapore*. Singapore Press Holdings (SPH), which owns *The Straits Times*, is a publicly listed company and it has also been issued a POFMA order, however this related to a post made by an anonymous user on its "HardwareZone" Forum and not the company itself. Channel NewsAsia, belonging to the state-owned Temasek Holdings' Mediacorp, also received a POFMA order during the 2020 election.

POFMA'ed data also reveals that 34 orders have targeted political groups or figures (including Alex Tan). Of the 27 cases giving rise to the 71 POFMA orders,[72] 20 involved statements about the Government, one of its agencies or a government-linked company. The three cases that did not involve criticism of the Government all related to false COVID-19 reports. One digital platform expert contrasted the figures with the Government's assurances that "they would stay away from opinions and political speech."[73]

Appeals process

Concerns over the effectiveness of POFMA's appeal mechanisms have been underlined by two recent cases (detailed below) in which judges disagreed over interpretations of the law.[74]

In January 2020, the Singapore Democratic Party was charged with communicating false statements about growing local retrenchments. A High Court judge dismissed the SDP's appeal against the charge on the grounds that the statements were false "in the face of statistical evidence against them" –

which the SDP did not challenge.[75] In his ruling, the judge said the burden of proof was on the Government to prove the falsity of information.

In a separate appeal in February 2020, *The Online Citizen* (TOC) was charged with communicating false statements from a press release by Lawyers For Liberty alleging abuses during executions by the Singapore Prisons Service. TOC's appeal failed on the grounds that the initial statement was not held to be true.[76] In this case, however, in direct contrast to the SDP case, the judge determined that the burden of proof fell on TOC.[77] The Court of Appeal is set to resolve this matter shortly.

Despite claims of its efficiency, the appeals process has also been criticised for its combative nature, and for the high cost to litigants.[78] Contested POFMA orders remain in effect during the appeals process, confirming initial concerns that the law "effectively reverses the traditional presumption that an accused is innocent until proven guilty."[79]

Elections

One of POFMA's most controversial aspects is that, through built-in delays in the appeals process, the Government has effective power to silence critics during election campaigns – which last for a minimum of nine days. During elections, powers to exercise POFMA passes to the civil service. The first point of appeal against a POFMA order is the relevant Minister and then, if that fails, the High Court. But the best appellants can hope for is to have their case heard as early as nine days after a challenge is first brought.[80] In other words, barring a change of heart from the Minister, a POFMA order applies for at least nine days – the same period for which conventionally politicians campaign in general elections.[81] Hence, information

can theoretically be blanketed under a POFMA order for the entirety of the election period.

Data on the use of POFMA during the July 2020 election campaign shows an unusually high incidence of orders against political opponents of the Government. Of 18 POFMA orders issued during the campaign period, 12 (67 per cent) targeted opposition political statements, including five against websites that had posted claims by the leader of the SDP. In 55 previous uses of POFMA, only about 20 per cent fitted the same criteria.

POFMA has also had a controversial impact on online political advertising, with a provision requiring internet intermediaries to keep records of all online political advertisements, prompting Google to remove such content altogether in Singapore.[82] One critic claimed this showed the provision may "worsen the asymmetric playing field between the incumbent party and the Opposition."[83]

COVID-19

A high proportion of POFMA orders have involved allegedly false or misleading statements about COVID-19 (35 out of 71 orders up to 11 July 2020). Data from the watchdog website *POFMA'ed* shows many of these cases concern claims critical of Singapore's handling of the crisis, as well as alleged falsehoods relating to certain groups in society, including migrant workers.[84]

The potentially life-threatening spread of misinformation during the pandemic has allowed the Government to claim vindication for its introduction of stringent misinformation laws.[85]

72 While there were 72 total uses of POFMA (as of July 11), many of these related to the same case; for example, different publishers of the same material were handed notices, or the same publisher was handed separate types of notices.
73 Interview 1, interviewed by Andrea Carson, 7 August 2020
74 N. Tang, "POFMA: A song of fact and opinion," The Online Citizen, published February 4, 2020, https://www.onlinecitizenasia.com/2020/02/04/pofma-a-song-of-fact-and-opinion/
75 Justice Ang Cheng Hock quoted in Lydia Lam, "Judge dismisses SDP's POFMA challenge, says statements were false in face of statistical evidence," *Channel News Asia,* February 5, 2020, https://www.channelnewsasia.com/news/singapore/judge-dismisses-sdp-s-pofma-challenge-says-statements-were-false-12394932?cid=h3_referral_inarticlelinks_24082018_cna.
76 Nicole Chang, "Judge dismisses The Online Citizen's POFMA challenge," *Channel News Asia,* February 19, 2020, https://www.channelnewsasia.com/news/singapore/the-online-citizen-toc-pofma-challenge-appeal-dismiss-12449826
77 Ibid.
78 Han, "Big Brother's regional ripple effect," 68; Foreign Correspondents Association of Singapore, "The Foreign Correspondents Association of Singapore is deeply…"
79 Kaye, *Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 6
80 Yuen-C Tham, "Fake news Act: Speed, cost of appeals process set out," *The Straits Times,* October 2, 2019, https://www.straitstimes.com/politics/fake-news-act-speed-cost-of-appeals-process-set-out
81 "Parliamentary elections," Elections Department Singapore, accessed November 13, 2020, https://www.eld.gov.sg/elections_parliamentary.html
82 Meyer, "Singapore's First Election Under the Fake News Law."
83 Ibid.
84 Ministry of Health and Ministry of Manpower, "Joint MOM-MOH statement on the issuance of correction directions under the Protection from Online Falsehoods and Manipulation Act (POFMA) against National University of Singapore Society (NUSS), The Online Citizen Asia (TOC), CNA and *New Naratif*," POFMA Office, published July 5, 2020, https://www.pofmaoffice.gov.sg/documents/media-releases/2020/July/pofma-pr-mom-05jul2020-01.pdf
85 Yuen-C Tham, "Falsehoods on coronavirus show why Pofma is necessary," *The Straits Times,* February 4, 2020, https://www.straitstimes.com/politics/falsehoods-on-coronavirus-show-why-pofma-is-necessary

Reactions to POFMA

Political

Singapore's main opposition party, the Workers' Party (WP), has been the most prominent parliamentary critic of POFMA, with some MPs accusing the PAP of creating and using POFMA to crush dissent and strengthen its hold on power.[86] One former MP, Low Thia Khiang, said POFMA had tightened a "dictatorial government's…hold onto absolute power."[87] He feared the ruling party would "manipulate opinions and spread falsehoods in order to win elections."[88] Another MP raised the spectre of a "chilling" of free speech, particularly "expressions of views that run counter to the government narrative."[89]

The Workers' Party highlighted the Act's inherent conflicts of interest,[90] and expressed doubt about whether the Government could make fair judgements in cases where it was the subject of the alleged falsehood.[91] It said the Government could exploit the Act's lack of a definition of "misleading" to defend its policies and public image.[92] It also criticised the "onerous" appeals process against POFMA orders, particularly as the burden of proof lay with the appellant,[93] and as contested online statements could be corrected or removed even before the appeals process had run its course.[94]

Despite its vocal opposition to POFMA, the Workers' Party has not yet been subjected to it. It is not entirely clear why the WP has escaped sanction but it may be due to its leader Pritam Singh's public commentary about open society when he said: "we believe that the national discourse should be conducted on the basis of objective facts." While there is still "a lot of room for opinion," he said public commentators risked the charge of falsity under POFMA as it currently exists.[95] Another possible explanation for the lack of POFMA orders against the WP is that the PAP has other, softer means of censure. This was evident prior to the 2020 election when prominent members of the PAP questioned Singh and his party's loyalty to Singapore.[96] During the election campaign, a police investigation sanctioned by the Attorney-General's office was opened into two Facebook posts published by a WP candidate, said to promote racial and religious enmity.[97] One of the posts was more than two years old.

Why the PAP has not used POFMA against the WP (but does so against smaller opposition parties) may be to avoid giving too much attention to its leading opposition, whose popularity reached new heights during the 2020 election.[98]

Critics have focused on ambiguities in the Act including its lack of differentiation between facts and opinions,[99] the

potential conflation of public interest with political gain,[100] and the lack of a definition for "misleading." The ambiguities have caused uncertainty among Singaporeans about what they can and can't post, and fear that the door is wide open for the abuse of anti-misinformation laws for political purposes.[101]

Several Nominated MPs – non-partisan members appointed by the President – offered less strident assessments, neither fully opposing nor fully supporting POFMA. Three Nominated MPs[102] proposed amendments to ensure that opinion, satire and other forms of non-factual commentary were excluded.[103]

Law and Home Affairs Minister Kasiviswanathan Shanmugam known as K Shanmugam, who led the Government's side of the POFMA debate, dismissed the criticisms, arguing the law narrowed rather than widened government powers, and that it provided "greater judicial oversight."[104] He also questioned the notion of universal free speech before POFMA was enacted, stating: "There's been no engagement on the key issue on why there should be free speech in this area. What speech are you protecting? Why are these things entitled to free speech?"[105]

---

86 Low Thia Khiang quoted in Vernon Lee, "Fake news law is ploy by government to hold on to "absolute power": Workers' Party MP Low Thia Khiang," *Yahoo News Singapore,* May 8, 2019, https://sg.news.yahoo.com/fake-news-law-is-ploy-by-government-to-hold-absolute-power-low-thia-khiang-155910029.html.

87 Ibid.

88 Ibid.

89 MP Perera quoted in "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill," Parliament of Singapore, published May 8, 2019, Vol. 94 Part 1, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-366.

90 Pritam Singh quoted in Fann Sim, "Workers' Party opposes online falsehoods Bill, says Pritam Singh," *Channel News Asia,* May 7, 2019, https://www.channelnewsasia.com/news/singapore/online-falsehoods-workers-party-opposes-bill-pritam-singh-11511450.

91 Muhamad Faisal Bin Abdul Manap quoted in "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill', Parliament of Singapore, published May 8, 2019, Vol. 94, Part 1, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-366.

92 Ibid.

93 Sylvia Lim quoted in "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill," Parliament of Singapore, published May 8, 2019, Vol. 94 Part 1, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-366.

94 Ibid,

95 Nicholas Yong, "GE2020: Workers' Party is not 'pulling its punches' in spite of POFMA, says Pritam Singh," *Yahoo News Singapore,* July 7, 2020, https://sg.news.yahoo.com/ge-2020-workers-party-is-not-pulling-its-punches-in-spite-of-pofma-says-pritam-singh-063326754.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAIrOu4fGibE2qg0_wGysQZWxGlrMs_D4ufdDdO6OzEkNrRDGDD45KSSR9ldVhmsr66-Mvrh8dfWWIKbYwHBHci5KarXgRua1iR2bMVxuLWxI9cNhQYQxFivabsbiKXpcqH0JFTv89ncOn32AUssYPlQuGdUBNVyXjXRcmXF-A-5H

96 Jalelah Abu Baker, "Tan Wu Meng's opinion piece on Pritam Singh was 'serious' and 'thoughtful': Shanmugam," *Channel News Asia,* June 21, 2020, https://www.channelnewsasia.com/news/singapore/tan-wu-meng-pritam-singh-aflian-shanmugam-12856406

97 Rei Kurohi, "Singapore GE2020: WP's Raeesah Khan apologises for posts which allegedly promoted enmity between different groups," *The Straits Times,* updated September 1, 2020, https://www.straitstimes.com/politics/singapore-ge2020-wps-raeesah-khan-apologises-for-posts-which-allegedly-promoted-enmity

98 "Singapore ruling PAP party wins elections, but support falls," *BBC,* July 10, 2020, https://www.bbc.com/news/world-asia-53358650

99 MP Khiang quoted in "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill," Parliament of Singapore, published May 8, 2019, Vol. 94 , Part 2, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-367.

100 NMP Prof. Walter Theseira quoted in "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill', Parliament of Singapore, published May 8, 2019, Vol. 94, Part 1, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-366.

101 For political discussion of this lack of definition, see Low Thia Khiang quoted in Singapore "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill," Parliament of Singapore, published May 8, 2019, Vol. 94 , Part 2, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-367; Human rights groups have criticised POFMA's ambiguity, as outlined in 'Reactions' below.

102 'NMPs contribute independent and non-partisan views in Parliament' (see "Members of parliament," Parliament of Singapore, accessed November 13, 2020, https://www.parliament.gov.sg/about-us/structure/members-of-parliament.).

103 Benjamin Joshua Ong, "Symposium on POFMA: Parliamentary debates about POFMA – Hansard beyond statutory interpretation?," *Research Collection School of Law* (November 2019): 3, https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4926&context=sol_research

104 "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill," Vol.94, Part 2.

105 Ibid.

Media, academic, digital platforms and civic groups

POFMA has attracted widespread commentary and criticism in Singapore, much of it in line with the main objections raised by opposition MPs. Journalists and civil rights groups fear the Government's increased powers may go unchecked.[106] Some have cited the broad and opaque definitions of breaches, and the potential for any form of government criticism to be judged false or misleading in service to the "public interest,"[107] with intimidation of independent media and government critics resulting.[108]

The exemption of the Government and its agencies from prosecution under POFMA[109] has, according to some commentators, created a "two-tiered" society in which the Government and its allies "can spread falsehoods with impunity" while its critics are heavily policed.[110] This highlights the Government's conflicted position as an arbiter of the Bill.

Critics pointed out ambiguities in the law, with distinctions between facts and opinions, satire and other forms of commentary blurred.[111] This could leave a journalist with a different interpretation of facts to the Government vulnerable to prosecution under POFMA.

Others have attacked POFMA more broadly as inherently anti-democratic and a threat to freedom of speech and freedom of the media. Media professionals and human rights organisations expressed concern over the "chilling effect" that stringent policing of speech could elicit.[112] POFMA orders, they argued, would discourage public discourse,[113] drive news organisations to withhold important stories,[114] and ultimately result in self-censorship.[115]

Some have predicted that, given Singapore's international reputation as an "efficient, highly-respected government," its regulatory approach to fake news may legitimise the introduction of similar laws in neighbouring countries.[116]

While there is general acknowledgment of the need for action against online misinformation, alternative strategies are proposed.[117] Journalist Kirsten Han argued the Government's successful response to COVID-19 "demonstrated that there are many ways we can communicate, interact, and build trust in the system *without* resorting to POFMA."[118] Others suggested improving the public's media literacy, which would allow citizens to discern falsehoods themselves,[119] and having independent bodies to adjudicate POFMA cases.[120]

Global digital technology companies with Asia-Pacific headquarters in Singapore have also expressed concern

about POFMA's impact on freedom of speech and innovation. Facebook cited the broadening of Singapore's powers to "compel us to remove content they deem to be false."[121] Google expressed broader fears for "innovation and growth of the digital information ecosystem,"[122] while Twitter raised concerns about freedom of expression and regulatory overreach.[123]

Human rights groups and NGOs have argued for more media literacy, rather than more restrictions. Some have questioned the Government's motives with POFMA, and advocated for greater powers of arbitration to be conferred on the courts.

Academics fear that POFMA will have a detrimental impact on academic discourse and research in Singapore. The advocacy group Academics Against Disinformation stated that the new restrictions may "compromise Singapore's notable efforts to develop itself into an internationally-recognised hub for excellence in higher education."[124] They also feared the law would be emulated in other countries. The group also questioned the implicit notion in the law that statements could always be objectively determined as false or misleading,[125] saying interpretations of even generally agreed upon "facts" may vary greatly.[126]

106 Kirsten Han, "Big Brother's regional ripple effect," *Index on Censorship* 48, no. 2 (2019): 67–69.; "Thum Ping Tjin, *New Naratif* to challenge POFMA notice despite compliance," *Yahoo News Singapore,* May 15, 2020. https://sg.news.yahoo.com/thum-ping-tjin-new-naratif-to-challenge-pofma-notice-despite-compliance-071938288.html
107 Han, "Big Brother's regional ripple effect," 67, 69
108 "Thum Ping Tjin, *New Naratif* to challenge POFMA notice despite compliance."
109 POFMA, section 61, reads: 'The Minister may, by order in the *Gazette,* exempt any person or class of persons from any provision of this Act.'
110 'Joint statement regarding the Protection from Online Falsehoods and Manipulation Bill' [Joint statement from arts and civil society organisations], https://theindependent.sg/nearly-30-civil-society-arts-and-community-groups-express-concerns-over-draft-fake-news-law/
111 Journalists, 'Journalists call for withdrawal of Singapore's "fake news" Bill' [letter to Minister of Communications and Information S Iswaran], 24 April 2019.
112 Tessa Wong, "Singapore fake news law polices chats and online platforms," *BBC,* May 9, 2019. https://www.bbc.com/news/world-asia-48196985.
113 Charles Santiago quoted in "Singapore: Amend the "fake news" bill," ASEAN Parliamentarians for Human Rights, published May 7, 2019, https://aseanmp.org/2019/05/07/singapore-fake-news-bill/?fbclid=IwAR114nescHaE8VQ5NDYlV8YxxTcKi_6ogBLXROZFR-8C5Uf5OnwCVjePQZ8
114 Jewel Stolarchuk, "Sarawak Report founder joins other prominent journalists in calling for the withdrawal of POFMA," *The Independent News and Media,*, 25 April 2019, https://theindependent.sg/sarawak-report-founder-joins-other-prominent-journalists-in-calling-for-the-withdrawal-of-pofma-bill/
115 Foreign Correspondents Association of Singapore, "The Foreign Correspondents Association of Singapore is deeply concerned about the Singapore government's passing of a bill…", Facebook, 9 May 2019, https://www.facebook.com/FCASG.org/posts/2358487210882553.
116 Han, "Big Brother's regional ripple effect."
117 Function 8, "Submission to the Parliamentary Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures," Facebook, February 28, 2018, https://m.facebook.com/story.php?story_fbid=911516705691971&id=350013055175675.; Terry Xu, "TOC's submission to Select Committee on Deliberate Online Falsehoods," *The Online Citizen,* March 7, 2018, https://www.onlinecitizenasia.com/2018/03/07/tocs-submission-to-select-committee-on-deliberate-online-falsehoods/.
118 Kirsten Han, "Coronavirus: How effective is Singapore's anti-fake news law?," *The News Lens,* April 8, 2020, https://international.thenewslens.com/article/133521.
119 Xu, "TOC's submission to Select Committee on Deliberate Online Falsehoods."; Association of Women for Action and Research. *No new restrictions needed: AWARE submission to Select Committee on "Deliberate Online Falsehoods* (Association of Women for Action and Research, 2018), 1, http://d2t1lspzrjtif2.cloudfront.net/wp-content/uploads/AWARE-submission-to-Select-Committee-on-Deliberate-Online-Falsehoods-1.pdf
120 Stephanie Neubronner, "Bill to protect from online falsehoods: Refinements needed," *RSIS Commentary* 85, (April 30, 2019): n.p.
121 Simon Milner quoted in Fathin Ungku, "Facebook, rights groups hit out at Singapore's fake news bill," *Reuters,* April 1, 2019, https://www.reuters.com/article/us-singapore-politics-fakenews/facebook-rights-groups-hit-out-at-singapores-fake-news-bill-idUSKCN1RD279.
122 Aradhana Aravindan, "Google says Singapore's fake news law could hamper innovation," *Reuters,* May 9, 2019, https://www.reuters.com/article/us-singapore-politics-google-idUSKCN1SF08X.
123 Ibid.
124 "POFMA: Media release," Academics Against Disinformation, published April 14, 2019, http://www.academia.sg/pofma-media-release/.
125 "POFMA: Letter to Education Minister," Academics Against Misinformation, published April 11, 2019, http://www.academia.sg/pofma-letter/.
126 Ibid.

Others criticised the lack of academic consultation before the law was enacted, and the Government "surreptitiously setting norms on what is appropriate and inappropriate academic work."[127]

However, some academics have defended POFMA. Wei Yao and Kenny Chng[128] echoed Minister Shanmugam's doubts about the inherent sanctity of free speech. Others defended the Government's central role in tackling falsehoods, saying courts were too slow, and that relying on internet companies would be less democratic and less accountable than relying on the Government.[129]

Ong[130] defended the lack of definition of "misleading" in POFMA as necessary, saying it prevented the law "being evaded through selective statements of facts that are individually true but collectively paint a false picture."[131] Ong argued that the judiciary had historically acted as an effective check on the Government's power. Similarly, Howe concluded that judicial oversight of the Act was "indeed, adequate."[132]

Professor of Journalism Cherian George questioned the courts' capacity under the existing structure of the law to keep the Government accountable, saying the interference of courts in "the executive's assessment of what the public interest requires" was frowned upon in Singapore.[133] He proposed explicit amendments ensuring judicial review powers.[134]

Howard and Terence Lee observed how the appearance of public debate in the lead-up to the enactment of POFMA established its legal and public legitimacy.[135] This careful and limited "incorporation of democratic elements" into the law-making process also legitimised the PAP's right to govern.[136] By establishing an "us versus them" dynamic during the law-making process,[137] they believed the Government had sought to portray POFMA's detractors as being against the interests of the country.

International reactions

International human rights groups have criticised POFMA as a threat to free speech. The International Commission of Jurists assailed the law's judicial review mechanism,[138] while Amnesty International argued the PAP's legislated role as the arbiter of falsehoods would stifle the voices of its critics.[139] The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression[140] also took issue with POFMA's legal appeals process, saying it reversed the presumption of innocence until proven guilty.[141]

However, POFMA is also being considered as a model for tackling online misinformation in other countries. Nigeria is considering an almost identically named "Protection from Internet Falsehood and Manipulation Bill 2019." One of its key Senate promoters named Singapore as an inspiration for the Nigerian legislation.[142]

127 Howard Lee and Terence Lee, "Polarising dissent: The constructed narrative of Singapore's new "fake news" law," *The Asia Dialogue*, June 10, 2019, https://theasiadialogue.com/2019/06/10/polarising-dissent-the-constructed-narrative-of-singapores-new-fake-news-law/.
128 Wei Yao and Kenny Chng, "Symposium on POFMA: Reflections on thinking about the POFMA," *Singapore Public Law*, (November 2019): n.p. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4944&context=sol_research.
129 Siyuan Chen and Chen Wei Chia, "Singapore's latest efforts at regulating online hate speech," *Research Collection School of Law*, (2019): n.p. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4879&context=sol_research.
130 Benjamin Joshua Ong, "Looking beyond the vague terms in Singapore's fake news laws," *TodayOnline*, May 14, 2019, https://www.todayonline.com/commentary/looking-beyond-vague-terms-fake-news-laws.
131 Ibid.
132 Lee Kay Howe, "True or false or misleading: [A]dequate judicial oversight over Part 3 directions under the Protection from Online Falsehoods and Manipulation Act," *Singapore Comparative Law Review*, (2019): 239.
133 Cherian George, "Online falsehoods bill: Will words in legislation mean whatever S'pore govt chooses them to mean?," Mothership, published April 6, 2019, https://mothership.sg/2019/04/online-falsehoods-cherian-george/
134 Ibid.
135 Howard Lee and Terence Lee, "From contempt of court to fake news," 82
136 Ibid.
137 Ibid., 86
138 "Singapore: Parliament must reject internet regulation bill that threatens freedom of expression," International Commission of Jurists, published April 4, 2019, https://www.icj.org/wp-content/uploads/2019/04/Singapore-fake-news-bill-News-web-story-2019-ENG.pdf.
139 Wong, "Singapore fake news law polices chats and online platforms."
140 David Kaye, *Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (United Nations, 2019), https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_SGP_3_2019.pdf.
141 Ibid., 6
142 Ellie Bothwell, "Fake news laws may 'catch on' during coronavirus," *Times Higher Education*, April 6, 2020, https://www.timeshighereducation.com/news/fake-news-laws-may-catch-during-coronavirus

Timeline of Singapore's "fake news" laws and policies

Table 2.1: Timeline of various laws and regulations implemented in Singapore

Year	Legislation/Policy Development/Initiative
1963	Malaysia's **Sedition Ordinance 1948** is extended to Singapore upon joining the Federation of Malaysia.
1965	Singapore maintains sedition legislation upon gaining independence from Malaysia. **Defamation Act** is enacted.
1985	Current version of **Sedition Act** is enacted.
1997	Within the **Broadcasting Act**, the **Internet Code of Practice** comes into effect. It outlines responsibilities for internet service and content providers to ensure content standards are in line with the public interest, decency, and national harmony.[143]
2013	Online News Licencing Scheme is established, under the Broadcasting Act.
2014	Defamation Act is revised. Protection from Harassment Act commences.
2018	[January] Singaporean government tables its green paper, ***Deliberate Online Falsehoods: Challenges and Implications***, which establishes a Select Committee to investigate online falsehoods. A call for public submissions to the committee also goes out.[144] [March] Singapore government conducts public hearings over eight days, inviting advocacy groups, tech companies such as Facebook and Twitter, among others to air their views about deliberate online falsehoods[145] [September] Select Committee presents its report on online falsehoods to parliament.
2019	[January] Ministry of Culture, Community and Youth launches seminar module, **Combatting Fake News.**[146] It aims to educate religious and community groups on fake news and how to detect it. [April] **POHA** amendments, which include the establishment of a specialist court, protections against "doxing," and strengthened protections for victims of harassment and falsehoods, are tabled to parliament.[147] [May] **Protection from Online Falsehoods and Manipulation Act (POFMA)** is passed in parliament, 72 in favour to 9 against. [October] **POFMA** comes into force in Singapore. [November] First use of **POFMA**. It is against Progress Singapore Party member Brad Bowyer.
2020	**POHA** amendments come into force, extending access to the law's use from individuals to companies.

Source: Authors

---

143 Infocomm Media Development Authority, *Internet Code of Pr*actice (Singapore: IMDA, 1997), https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/ Regulations/Codes-of-Practice/Codes-of-Practice-Media/PoliciesandContentGuidelinesInternetInterneCodeOfPractice.pdf

144 Ministry of Communications and Information and Ministry of Law, *Deliberate and Online Falsehoods: Challenges and Implications* (Singapore: Parliament of Singapore, 2018), https://www.nas.gov.sg/archivesonline/government_records/Flipviewer/grid_publish/6/6797717d-f25b-11e7-bafc-001a4a5ba61b 06012018Misc.10of2018/web/html5/ index.html?launchlogo=tablet/GovernmentRecords_brandingLogo_.png&pn=1.

145 ,Fathin Ungku, "Singapore invites rights group to fake news hearing as dispute grows," Reuters, March 28, 2018, https://www.reuters.com/article/us-singapore-politics-malaysia-scandal/singapore-pm-files-defamation-suit-against-blogger-who-shared-article-on-facebook-idUSKBN1O414L.

146 "Combating fake news," National Library of Singapore, last updated October 29, 2020, https://sure.nlb.gov.sg/resources/audience/adults/combating-fake-news

147 Ministry of Law, *Enhancements to the Protection from Online Harassment Act ('POHA')* (Singapore: Ministry of Law, April 1, 2019), https://www.mlaw.gov.sg/news/press-releases/enhancements-to-the-protection-from-harassment-act-poha

Conclusion

⌄

As noted in the introduction, Singapore's unique demographic and political structure has strongly influenced its approach to tackling online misinformation, as with so many other issues in the past. A culturally and ethnically diverse population, while part of the national identity, is also viewed by policymakers as a potential point of instability, prompting strict regulatory and legislative measures such as POFMA.

Evidence that the Government has used POFMA as an effective tool to silence political opponents and suppress media freedom should not come as a surprise to students of Singaporean history who can recall how former leader Lee Kuan Yew once held that freedom of the press must be "subordinate to the primacy of purpose of an elected government."[148]

And any notion that a Government might be deterred from abusing its power for fear of an electoral backlash[149] would not appear to apply in Singapore, rated as "partly free" with a democracy score of 50 out of 100,[150] enabling the PAP Government to reign over the island state since 1959.

---

148 Quoted in Human Rights Watch, *Kill the Chicken to Scare the Monkeys,* 22
149 Yao and Chng, "Symposium on POFMA: Reflections on thinking about the POFMA."; Minister K Shanmugam quoted in "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill," Parliament of Singapore, published May 8, 2019, vol. 94, Part 2, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-367.
150 Sarah Repucci, "A Leaderless Struggle for Democracy: Democracy and Pluralism are under assault", *Freedom House, 2020.*

The European Union: Approaches to online misinformation and disinformation

Introduction

This chapter examines the European Union's approach to tackling online misinformation and disinformation – including the development and performance of the EU's Code of Practice on Disinformation, established in September 2018.

As a first-of-its-kind, voluntary agreement between the European Commission, digital platforms and advertising groups, the Code has proved to be an influential example of self-regulation internationally, and is considered by many as the current benchmark for action on misinformation and disinformation.

This chapter investigates EU and independent assessments of the Code over its first two years of operation, demonstrating that while considerable progress has been achieved, much more is required to sufficiently combat the problem. Actions taken against misinformation and disinformation in individual EU member states are also documented. A timeline summarising Europe's major laws and policies addressing this pernicious problem is provided at the end of the chapter. Full details of the different regulations and laws are available in Appendix C.

Background and context

In March 2015, in one of the first major European initiatives to counter online falsehoods, the European Council, citing Russia's sustained disinformation campaigns, proposed an Action Plan on Strategic Communication.[1] This led to the creation of EUvsDisinfo, a website set up to identify and counter Russia's ongoing disinformation campaigns.[2]

In April 2018 the European Commission released *Tackling Online Disinformation: A European Approach*, which became the central document for further actions in the field.[3] It stated that the main threat was disinformation, not 'fake news' or misinformation.[4]

The report defined disinformation as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm."[5] Public harm may include "threats to democratic political and policymaking processes" or "EU citizens' health, the environment or security." Excluded from the definition were "reporting errors, satire and parody, or clearly identified partisan news and commentary."[6]

The report enshrined four overarching principles for online communication: transparency, credibility of information, diversity of information and inclusive cooperation.[7] Its focus was on online platforms; fact checking; online accountability; election integrity; media literacy; quality journalism; and strategic communication. However, the most important aspect of the report was a commitment by the Commission to support the development of a voluntary Code of Practice.[8] It called on digital platforms to participate in the Code and forecast its establishment by 2018.

The EU outlined fundamental requirements be met in its war on disinformation. Foremost was the need to balance the fundamental right to freedom of expression with the right of the public to be properly informed.[9] Disinformation impaired freedom of expression, yet state actors had an obligation to refrain from censorship, since legal content even when harmful was generally protected under freedom of expression principles.[10] A focus on responsible behaviour in conveying information to end users, a pluralistic media policy that increased exposure of diverse content, and the empowerment of online consumers through media literacy initiatives was prioritised.[11]

---

1   European Council, "European Council meeting (19 and 20 March 2015) – Conclusions," published March 20, 2015, EUCO 11/15, 5, https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf
2   "About," EUvsDisInfo, accessed November 17, 2020, https://euvsdisinfo.eu/about/
3   European Commission, *Tackling Online Disinformation: A European Approach* (Brussels: European Commission, April 26, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&qid=1583456906698&from=EN
4   The HLEG characterised misinformation as "misleading or inaccurate information shared by people who do not recognise it as such," in Commission High Level Expert Group on Fake News and Online Disinformation, *A Multi-Dimensional Approach to Disinformation: Report of the Independent High-Level Expert Group on Fake News and Online Disinformation* (Brussels: European Commission, 2018), 10, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271
5   European Commission, *Tackling Online Disinformation: A European Approach*, 3-4.
6   Ibid., 3.
7   Ibid., 6.
8   Ibid., 8.
9   European Parliament, *Charter of Fundamental Human Rights of the European Union (2000/c 364/01)* (European Parliament, December 18, 2000), Article 11, https://www.europarl.europa.eu/charter/pdf/text_en.pdf; European Court of Human Rights, *European Convention on Human Rights* (European Court of Human Rights, 2010), Article 10, https://www.echr.coe.int/Documents/Convention_ENG.pdf
10   European Commission, *Tackling Online Disinformation*, 1.
11   Andrea Renda, *The Legal Framework to Address "Fake News": Possible Policy Actions at the EU Level* (Brussels: Policy Department for Economic, Scientific and Quality of Life Policies, June 2018), 20-21, https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf

The EU Code of Practice

In September 2018 the Code of Practice was voluntarily agreed to by 13 signatories, including Facebook, Twitter, Google and Mozilla. Microsoft signed up to the Code in 2019 and TikTok in June 2020.[12]

The Code is based on five pillars setting out actions relating to:

- Scrutiny of ad placements
- Political advertising and issue-based advertising
- Integrity of services (which largely concerns inauthentic and manipulative activity)
- Empowering consumers
- Empowering the research community.[13]

EU agencies urged the Commission to take further regulatory action if measures against disinformation and other elements of the Code were not implemented quickly or satisfactorily.[14] Appraisals of the Code by the Commission itself and relevant stakeholders are discussed shortly.

Action Plan against Disinformation

Soon after the establishment of the Code, the Commission released its *Action Plan against Disinformation* in December 2018.[15] It outlined the Commission's commitments to monitoring the Code and also earmarked the European Regulators Group for Audiovisual Media Services (ERGA) to provide additional monitoring services.[16]

The Action Plan focused on improving the capabilities of EU institutions to:

- Detect and analyse disinformation
- Coordinate joint responses to disinformation
- Mobilise the private sector to tackle disinformation
- Improve societal awareness and resilience.[17]

The Commission would seek to train journalists in better quality media practices[18] and, as part of Media Literacy Week (March 2019), support cross-border cooperation among media literacy practitioners.[19]

It also committed to establishing a European network of independent fact checkers with investment in new technologies for content verification.[20] The Social Observatory for Disinformation and Media Analysis (SOMA) was launched to enable networking and knowledge exchange between independent fact checkers.[21]

12   Natasha Lomas, "TikTok joins the EU's Code of Practice on Disinformation," *TechCrunch,* June 22, 2020, https://techcrunch.com/2020/06/22/tiktok-joins-the-eus-code-of-practice-on-disinformation/

13   European Commission, *EU Code of Practice on Disinformation* (Brussels: European Commission, September 26, 2018), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454

14   European Economic and Social Committee, *Opinion on Action Plan against Disinformation* (Brussels: European Commission, March 20, 2019), https://webapi2016.eesc.europa.eu/v1/documents/EESC-2018-06302-00-00-AC-TRA-EN.docx/content; European Committee of the Regions, *Opinion of the European Committee of the Regions on "Tackling online disinformation: a European Approach"* (Brussels: Official Journal of the European Union, May 16, 2019), comment 24, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018IR3908&qid=1583456906698&from=EN

15   European Commission, *Action Plan against Disinformation* (Brussels: European Commission, December 5, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0036&qid=1583456906698&from=EN

16   European Commission, *Assessment of the Code of Practice on Disinformation – Achievements and Areas for Further Improvement* (Brussels: European Commission, September 10, 2020), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212

17   European Commission, *Tackling COVID-19 Disinformation – Getting the Facts Right* (Brussels: European Commission, June 10, 2020), 2, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0008&from=EN

18   European Commission, *Action Plan against Disinformation,* 15.

19   Ibid., 11.

20   Ibid., 9.

21   "About us," Social Observatory for Disinformation and Media Analysis, accessed November 19, 2020, https://www.disinfobservatory.org/about-us/; European Commission, *Report on the Implementation of the Action Plan against Disinformation* (Brussels: European Commission, June 14, 2019), 6-7, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

Assessments of the Code

Since its implementation in September 2018, the code's performance has been assessed by the Commission and various independent consultants.

Post-2019 EU elections

The European parliamentary elections in May 2019 were identified in the *Action Plan against Disinformation* as a critical test of the code's capacity to protect and ensure transparency around Europe's democratic processes.[22] To this end, the Commission observed that the Code helped "increase transparency of political communications", limit online information manipulation and enabled citizens to discern the source of political ads.[23] High ranking EU officials said in a joint statement that Facebook, Google and Twitter had "made some progress under the Code of Practice."[24] Despite this acknowledgement, the Commission said there was still much to be done to combat the evolving threat of disinformation campaigns.

First annual self-assessment reports

In October 2019, Code signatories tabled their first annual self-assessment reports, from which the Commission provided a summary and analysis. The Commission championed the Code for increasing transparency of platforms' policies on disinformation, and establishing "a framework for structured dialogue to monitor, improve and effectively implement those policies."[25] Signatories' reports demonstrated their "comprehensive efforts" to meet the commitments of the Code, such as granting insights into their actions against coordinated inauthentic behaviour.[26] Nonetheless, in keeping with its monitoring responsibilities, the Commission focused on areas requiring immediate improvement.

The Commission surmised that efforts to empower users and the research community lagged behind measures to improve scrutiny of ad placement, political and issue-based advertising and integrity of services. It called on platforms to facilitate better relationships with relevant stakeholders such as researchers, fact checkers and the media. In particular, platforms' reticent and "episodic" data sharing was said to hamper independent research and fact checking efforts.[27] This underdeveloped cooperation meant the potential to identify "persistent or egregious purveyors of disinformation" was not being fulfilled.[28] The implementation of ad scrutiny and brand safety measures was also hampered by signatories' lack of coordination with these stakeholders.

While user empowerment initiatives, such as media literacy campaigns and training, had improved before the Code's inception, the Commission experienced difficulty in measuring their impact and efficacy. Again, platforms' inadequate reporting was identified as a central cause.[29] The absence of specificity in the information shared by platforms made it hard for the Commission to measure "malicious behaviour specifically targeting the EU and the progress achieved by the platforms to counter such behaviour".[30]

Other issues noted in the Commission's analysis concerned the accuracy of signatories' political ad labelling[31] and the modest interest in the Code from the digital and advertising industries.[32]

ERGA: Assessment of the Implementation of the Code of Practice

ERGA's May 2020 assessment of the Code shared many of the Commission's concerns. It found signatories' self-assessment reports lacked sufficient data, which was a particular problem in regard to strengthening political advertising, ad placement and integrity of services measures.[33] Limited access to and transparency of data hindered independent investigations of the code's performance and prevented adequate evaluation of the code's impact by the EU and member states.[34] Like the Commission, ERGA lamented the "limited" number of signatories, arguing that "significant" actors such as private messaging platforms WhatsApp and Messenger were "missing."[35]

ERGA raised some other issues with the code's performance over its first year. It found the measures of the Code "too general in terms of content and structure", with "a lack of uniformity in the procedures (and the definitions) adopted by the different platforms".[36] As a result, ERGA encouraged signatories to strive for greater consistency and specificity in their definitions and measures, including in the way they respond to fact-checked news.[37] ERGA also found media literacy initiatives had been "conducted in a scattered manner".[38]

---

22 European Commission, *Action Plan against Disinformation*, 2.
23 "A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council," European Commission, Published June 14, 2019, https://ec.europa.eu/Commission/presscorner/detail/en/IP_19_2914
24 Ibid.
25 European Commission, *Code of Practice on Disinformation: First Annual Reports* (Brussels: European Commission, October 2019), 1, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62698.
26 Ibid., 8-9.
27 Ibid., 2.
28 Ibid., 5.
29 Ibid., 10-11.
30 Ibid., 9.
31 Ibid., 7.
32 Ibid., 2.
33 European Regulators Groups for Audiovisual Media Services, *ERGA Report on Disinformation: Assessment of the Implementation of the Code of Practice* (Brussels: European Commission, May 2020), 47-48, https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf
34 Ibid., 3,49
35 Ibid., 3.
36 Ibid., 3.
37 Ibid., 52.
38 Ibid., 48.

ERGA's primary recommendation was to shift the code's approach towards co-regulation, since the current self-regulatory model exhibited various compliance issues.[39] While the specifics of such an approach were not outlined, ERGA supports the implementation of more stringent reporting obligations and "the introduction of a formal backstop mechanism to deliver the required monitoring and enforcement elements".[40] Hence, ERGA is in favour of empowering the Commission and national regulatory authorities to more effectively hold platforms accountable to deliver on their commitments.[41]

Independent consultation

The Commission appointed consultancy firm Valdani, Vicari and Associates to conduct an independent review of the policies and performance of signatories under the Code.[42] Released in May 2020, the review stated that the code's regular monitoring framework fostered greater transparency of social media platforms during elections and other political campaigns. In line with previous assessments, it said pillars 1-3 had "produced a more positive change" than pillars 4 and 5.[43]

For pillar 4 (empowering users), while it was reported that the Code had contributed to improving consumers' awareness of disinformation, better reporting on the results of platforms' tools and actions was needed.[44]

For pillar 5 (empowering the research community), while social media platforms were said to have increased collaboration with researchers and fact checkers, and improved their access to relevant data, the research community reported being unsatisfied with the responses from platforms in relation to data requests.[45] Platforms' concerns about user data privacy

violations may have contributed to this reticence.[46] Effort was needed from both sides to improve the effectiveness of this relationship.

The report also suggested refinement of the use of the terms disinformation and misinformation. It was argued a better understanding of *intent* may resolve the ambiguity of terminology and "improve the effectiveness of specific actions to combat specific behaviours".[47]

Tackling COVID-19 disinformation

In a June 2020 report, the Commission reviewed the COVID-19 "infodemic" and the various instruments working to combat coronavirus-related misinformation and disinformation. The Commission found that platforms had reported "adjustments to their policies to address the COVID-19 disinformation threat", including promoting "accurate and authoritative information" from trusted sources such as the World Health Organisation and professional media outlets.[48] Platforms demoted false and misleading content, limited suspicious ads and removed content deemed to have the potential to cause health and public harm.[49]

However, the Commission observed that platforms had failed to empower civil society actors, fact checkers and researchers – due largely to limited information sharing. The Commission said the crisis had further highlighted the need for greater transparency and accountability from platforms.[50]

The report outlined safeguards which the Commission expected platforms to implement to combat the COVID-19 infodemic.[51] The Commission vowed to monitor how platforms were tracking in this space on a monthly basis. Signatories have been asked to provide information regarding the promotion of

authoritative content, their actions to improve users' awareness, manipulative behaviour on their platforms, and advertising of COVID-19 disinformation on their platforms and third-party sites.

In September 2020, the Commission released Code signatories' first baseline reports on these COVID-19-related asks. The reports demonstrated signatories had increased access to and visibility of authoritative information.[52] Notably, however, the application of these measures was not uniform across the EU.

In particular, platforms "did not detect coordinated disinformation operations with specific focus on COVID-19 run on their services".[53] This finding suggests that misinformation and uncoordinated disinformation were more common manifestations of harmful content about COVID-19. Yet the Commission argued that misinformation did not necessarily require government intervention, since public literacy and fact checking could intervene. Disinformation, on the other hand, needed "to be addressed through other means, including actions taken by governments".[54]

In the second phase of the process, the Commission committed to provide monthly assessments of the effectiveness of these measures from August to December 2020.

European Commission's assessment of the Code of Practice

The European Commission's assessment of the Code in September 2020 to examine its initial 12 months of operation praised the establishment of a framework for dialogue between relevant stakeholders, monitoring, and greater transparency and accountability of platform operations.[55] Improvements were noted under each "pillar". Greater scrutiny of ad placements had

39   Ibid., 3.
40   Ibid., 4.
41   Ibid., 3.
42   Valdani, Vicari and Associates, *Study for the Assessment of the Implementation of the Code of Practice on Disinformation* (Brussels: European Commission, May 2020). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66649.
43   Ibid., 96-97.
44   Ibid., 97.
45   Ibid.
46   Ibid., 58.
47   Ibid., 97.
48   European Commission, *Tackling COVID-19 Disinformation – Getting the Facts Right,* 8.
49   Ibid.
50   Ibid.
51   Ibid., 9.
52   "First baseline reports – Fighting COVID-19 disinformation monitoring program," European Commission, Published September 10, 2020, https://ec.europa.eu/digital-single-market/en/news/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme
53   Ibid.
54   European Commission, *Tackling COVID-19 Disinformation – Getting the Facts Right,* 4.
55   European Commission, *Assessment of the Code of Practice on Disinformation – Achievements and Areas for Further Improvement*, 4.

"contributed to reducing monetisation incentives for actors that disseminate disinformation online for economic gain"[56] Labelling measures increased transparency of political and issue-based advertising and provided information on the source, audiences and impact of these ads.[57] Action against inauthentic accounts led to their disclosure.[58]

Technological tools that promote reliable information, improve access to a broad diversity of information sources and new disinformation flagging tools empowered users, while cooperation with fact checkers also enhanced users' capacity to critically assess information.[59] Some data sharing initiatives with researchers and fact checkers were also noted.

Yet the central message of the Commission's review was that signatories were still falling short of the code's expectations. The Commission outlined four main issue areas:

- Inconsistent and incomplete application of the Code across platforms and Member States;
- Lack of uniform definitions;
- Gaps in the coverage of Code commitments;
- Other limitations intrinsic to the self-regulatory nature of the Code.[60]

Incomplete and inconsistent application of the Code

User empowerment initiatives, while increasing during the COVID-19 crisis, were not deployed across all European countries and languages. No data was provided to measure their effectiveness in increasing user engagement with credible information, critical thinking and civic participation.[61] User complaints mechanisms were found to be lacking uniformity and ease of accessibility across platforms – should they exist at all. The Commission found they were unable to conduct comparisons between platforms' different fact checking measures, since measurable performance indicators were not provided.[62]

Lack of uniform definitions

The lack of clarity and uniformity around definitions of the problem was identified as a significant issue in the Code. The COVID-19 "infodemic" emphasised the need to differentiate between different forms of false and misleading information and manipulative behaviour.[63] Such that the Commission argued for greater incorporation of misinformation and "influence operations"[64] in understandings of the wider problem.[65]

Gaps in the coverage of Code commitments

The Commission argued that "the vagueness of the Code's commitments… creates serious risks of incomplete action" against forms of inauthentic activity that might fall outside its scope, such as micro-targeting of political ads and fairness in political advertising online.[66] Moreover, the absence of clear and measurable key performance indicators in the Code stymied objective measurements and comparisons between platforms.[67]

Meanwhile collaboration with independent fact checking initiatives fell short of the Commission's expectations.[68] Sufficient access to data and resources for fact checking and research activities as outlined in the Code had "not been achieved" and remained "episodic and arbitrary,"[69] the Commission found.

Regarding actions targeting inauthentic behaviour and content, signatories did not provide accurate, relevant, location-specific data, meaning the Commission could not evaluate their effectiveness in the EU and its Member States.[70] These measures were also found to focus too closely on foreign interference, with EU-based actors escaping due attention.[71]

Issues with the voluntary model

The Commission acknowledged multiple inherent problems with the code's voluntary model. First, it created "regulatory asymmetry", where signatories were at a disadvantage to non-signatories since they must implement sometimes costly measures to fulfil their commitments.[72] Further, malicious actors had the option of using non-signatory platforms to spread disinformation, which the Commission observed throughout the pandemic.

Second, key actors in the disinformation space outside the Code, such as private messaging platforms and advertising groups, were under no obligation to become signatories.[73]

Third, a voluntary model meant there were no mechanisms to ensure adequate independent oversight, cooperation with member state authorities, and compliance with Code commitments.[74] Consequently, the sole sanction for non-compliance was expulsion from the Code – a penalty that somewhat optimistically depended on signatories' aversion to reputational damage.[75]

Finally, the Code did not have procedures to ensure that "fundamental rights", such as freedom of speech, were upheld by signatories.[76]

In sum, despite recognising the achievements of the Code, the Commission also acknowledged glaring deficiencies in its design, scope, terminology and practice. Signatories were strongly encouraged to escalate their efforts in addressing misinformation and disinformation as the EU reviewed its strategy.

---

56   Ibid.
57   Ibid., 5.
58   Ibid.
59   Ibid., 6.
60   Ibid., 7.
61   Ibid.
62   Ibid.
63   European Commission, *Assessment of the Code of Practice on Disinformation – Achievements and Areas for Further Improvement*, 12.
64   The Commission defines influence operations as "information campaigns by third-country actors that employ false or misleading information in combination with manipulative online techniques to interfere in EU or Member State electoral or policy-making processes, where the intention to deceive the public may be presumed" (Ibid.).
65   Ibid.
66   Ibid., 14.
67   Ibid., 15.
68   Ibid., 11.
69   Ibid.
70   Ibid., 9.
71   Ibid., 10.
72   Ibid., 17.
73   Ibid., 18.
74   Ibid.
75   Ibid.
76   Ibid., 19.

Reactions to the EU approach

Much of the public commentary surrounding the EU's approach echoes the Commission's evaluations.

Tasked by the Commission to assess the Code, a 'Sounding Board' comprising representatives from the media, civil society, fact checkers and academia argued the Code contained:

> No common approach, no clear and meaningful commitments, no measurable objectives or KPIs, hence no possibility to monitor process, and no compliance or enforcement tool: it is by no means self-regulation, and therefore the Platforms, despite their efforts, have not delivered a Code of Practice.[77]

Misinformation scholars found the scope and terminology of the Code lacked clarity.[78] Leaving platforms to resolve these ambiguities presented a possible risk for freedom of expression.[79] The code's ill-defined terminology "indicates a lack of consensus among key stakeholders regarding the scope of the issue and therefore its potential solutions".[80] What actions had been undertaken so far were also characterised by unclear legal foundations and an unreliable political mandate.[81]

Some academics have argued for a mandatory co-regulatory model, with one calling it the "best imperfect" approach to tackling disinformation.[82] Co-regulation would see the EU legislate the objectives of actions against disinformation, which digital platforms would then fulfil under the auspices of a Code developed in conjunction with civil society and the Commission.[83] A similar model was endorsed elsewhere.[84]

Other notable critiques were that the EU's approach lacked baseline reporting, had budgetary and institutional restraints and a lack of effective cooperation with member states, posing a significant problem for the integrity of elections.[85]

Recently, some member states have tabled their official judgement of the Code. In June 2020, Estonia, Lithuania, Slovakia and Latvia released a position paper which argued that the self-regulatory framework "is insufficient and unsuitable" to address online disinformation.[86] In September 2020, the heads of state of France, Lithuania and Latvia published a joint statement that implored the Commission to push for more stringent measures, particularly concerning the protection of democratic elections.[87] They called for more effective mechanisms enabling member states to identify and counter disruptive activity, and to ensure transparency and enforcement of Code measures. Consistent in both these critiques is the view that the Code has not gone far enough.

The digital platform experts interviewed for this study were largely ambivalent on suggestions that the EU approach might be the global standard for tacking misinformation and disinformation. One expert stated that the platform they worked for "would prefer" a European-style cross-platform and self-regulatory approach, rather than "more prescriptive" regulation as seen in countries such as Singapore.[88]

---

77 Sounding Board, *The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice* (European Commission, September 24, 2018), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54456.
78 James Pamment, *The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission* (Washington: Carnegie Endowment for International Peace, March 2020), 4, https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-Commission-pub-81187.; Nenadic, "Unpacking the 'European approach' to tackling challenges of disinformation and political manipulation," 13.
79 Ibid.
80 Pamment, *The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission*, 5.
81 James Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative* (Washington: Carnegie Endowment for International Peace, June 2020), 5, https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf.
82 Paul-Jasper Dittrich, *Tackling the Spread of Disinformation: Why a Co-regulatory Approach is the Right Way Forward for the EU* (Berlin: Jacques Delors Centre, December 12, 2019), 10, https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/EZ_JDI_BST_Policy_Paper_Disinformation_Dittrich_2019_ENG.pdf
83 Ibid., ii.
84 Chris Marsden, Trisha Meyer, and Ian Brown, "Platform values and democratic elections: How can the law regulate digital disinformation?," *Computer Law and Security Review* 36 (2020): 1, DOI: 10.1016/j.clsr.2019.105373.
85 Kanzanira Thorington, "*Europe's elections: The fight against disinformation,*" Council on Foreign Relations, Published May 23, 2019, https://www.cfr.org/blog/europes-elections-fight-against-disinformation.
86 Samuel Stolton, "EU code of practice on disinformation 'insufficient and unsuitable,' member states say," *EURACTIV.com*, June 5, 2020, https://www.euractiv.com/section/digital/news/eu-code-of-practice-on-disinformation-insufficient-and-unsuitable-member-states-say/.
87 Emmanuel Macron, Gitanas Nauseda and Arturs Krisjanis Karins, *Joint Statement By The Presidents Of France And Lithuania, And Prime Minister Of Latvia On Protection Of Democracies* (Paris: Palais de l'Elysee, September 28, 2020), https://static.lsm.lv/documents/z5.pdf
88 Interview 1, interviewed by Andrea Carson, August 7, 2020.

Other EU measures to tackle false information online

While the Code of Practice is the central initiative aimed at tackling misinformation and disinformation, there are other programs the EU has established.

Rapid Alert System

Outlined in the *Action Plan Against Disinformation*, the *Rapid Alert System* was established in March 2019 and is a data and knowledge sharing network. It is used to connect disinformation experts across Europe and facilitate communication and strategic responses between governments.[89] Despite its intentions, in practice the system is not often used by Member States. James Pamment ascribed this to "major differences in how Member States view the threat of disinformation" and "a lack of trust" between them.[90] As such, issues around inadequate information sharing appear to afflict not only signatories' efforts but also those of governments.

Media Literacy Initiatives

Other initiatives focus more directly upon public awareness. A November 2018 directive of the European Parliament and Council stated that Member States are required to promote and oversee the development of their citizens' media literacy skills.[91] Additionally, media service providers and video-sharing platforms are required to provide "for effective media literacy measures and tools and [to] raise users' awareness of those measures and tools."[92]

New Laws

There are also several important parliamentary initiatives still to be released in 2020 by the EU. The *European Democracy Action Plan* closed public consultation in September. It aims to "ensure that citizens are able to participate in the democratic system through informed decision-making free from unlawful interference and manipulation."[93] In addition to disinformation, it will include measures on electoral integrity, media freedom and media pluralism. It has been said that it will build on the progress of the *Action Plan* and Code of Practice and help Europe determine next steps in its fight against disinformation.[94]

Further, a *Digital Education Act Plan* was scheduled to be tabled in the EU in late 2020 that aims to facilitate digital literacy.[95] A stated aim is to help people counter disinformation.

The *Digital Services Act* was also slated to be enacted late 2020. It aims to modernise the legal framework of Europe's digital market. It is expected to provide new regulatory obligations on digital service providers so that platforms clearly outline their responsibilities to users.[96] It is anticipated that new powers will address platform responses to online disinformation.[97]

---

89   European Commission, *Tackling COVID-19 Disinformation – Getting the Facts Right,* 2.
90   Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative,* 9.
91   European Parliament and the Council, *Directive (EU) 2018/1808 of the European Parliament and of the Council* (Brussels: European Parliament, November 14, 2018), Article 33a, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN
92   Ibid., section 3j.
93   "Protecting European democracy from interference and manipulation – European Democracy Action Plan," European Commission, accessed November 19, 2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12506-European-Democracy-Action-Plan
94   Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative,* 10.
95   https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
96   "The Digital Services Act package," European Commission, last updated June 22, 2020, https://ec.europa.eu/digital-single-market/en/digital-services-act-package
97   Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative,* 10.

Member States' initiatives

Among Europe's Member States, only Germany, France and Hungary have passed laws aimed at tackling disinformation and misinformation. Some states have implemented other non-legislative measures.

Germany

Germany introduced a 2018 law that bans online hate speech and requires social media platforms to remove or block "manifestly unlawful content" within 24 hours and "unlawful content" within seven days.[98] *The Network Enforcement Act*, known commonly as 'NetzDG', covers social media platforms with over two million users. It mandates an accessible user complaint process with platforms to report biannually on their handling of user complaints regarding unlawful content.

NetzDG has had significant influence on other countries' approach to regulation. A report published by Danish think tank *Justitia* found that among European countries, France, the United Kingdom, Russia and Belarus had all cited NetzDG in policy discussions.[99] Beyond Europe, other nations had considered Germany's approach, including Singapore and Australia. The law has come under criticism for perceived breaches of freedom of speech, and social media platforms have been observed pre-emptively deleting "more content than necessary out of fear of incurring large fines."[100]

France

France passed its law against the manipulation of information in November 2018, which addresses false information disseminated on social media and media outlets influenced by foreign states.[101] The law is specifically aimed at curbing misinformation and disinformation around elections. The law allows judges "to order the immediate removal of online articles" containing disinformation during the election campaign.[102] Other measures enable the national broadcasting agency to suspend foreign television channels which "deliberately disseminate false information likely to affect the sincerity of the ballot," while online political campaigns are required to disclose their spend and financial backers.[103] Breaches of the law could result in a one-year jail term or fine of €75,000. The law was considered an affront to liberty by critics,[104] and was twice rejected in the Senate before the bill was passed. French opposition parties and journalist associations have criticized the law for curtailing press freedom and jeopardising pluralist debate necessary in a healthy democracy.[105]

Hungary

In response to the Coronavirus 'infodemic', Hungary passed new measures that enabled President Orbán to "rule by decree", as some critics claimed.[106] It allowed the Government to issue prison sentences to those caught intentionally spreading false information that could hamper the government's response to the pandemic. The Bill's opponents feared it could be misused to censor criticism of the government.[107] While the Government rescinded its extraordinary powers in June,[108] critics fear the legislation allows the Government to reinstate another state of emergency and its "rule by decree" as it sees fit under the pretence of fighting COVID-19.[109]

Others' measures

Other Member States have implemented non-legislative measures to mitigate the spread of fake news. The Netherlands, in early 2019, launched an online campaign around fake news in the lead up to its elections.[110] Finland has deployed fact checking organisation *Faktabaari* to teach professional fact checking techniques in Finnish schools.[111] Spain employed members of the International Fact-Checking Network to monitor its 2019 elections.[112] Since 2017, Italy has introduced media literacy into the school curriculum.[113] In the lead up to the 2018

---

98   Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), Bundestag, (July 12, 2017), 2-3, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

99   Jacob Mchangama and Joelle Fiss, *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Citizenship* (Copenhagen: Justitia, November 2019), https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf

100 Florian Saurwein and Charlotte Spencer-Smith, "Combating disinformation on social media: Multilevel governance and distributed accountability in Europe," *Digital Journalism* 8, no. 6 (2020): 830.

101 Marine Guillaume, *Combating the Manipulation of Information – A French Case* (Helsinki: Hybrid CoE, 2019), https://www.hybridcoe.fi/wp-content/uploads/2019/05/HybridCoE_SA_Combating-the-manipulation-of-information.pdf

102 Sarwein and Spencer-Smith, "Combating disinformation on social media: Multilevel governance and distributed accountability in Europe," 828.

103 Michael-Ross Fiorentino, "France passes controversial 'fake news' law," *Euronews,* May 9, 2019, https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law

104 Marc Watin-Augouard, "Law no. 2018-1202 of 22 December 2018 on combating the manipulation of information," FIC-Observatory, published November 1, 2019, https://observatoire-fic.com/en/law-no-2018-1202-of-22-december-2018-on-combating-the-manipulation-of-information-by-general-marc-watin-augouard-founder-of-the-fic/

105 Fiorentino, "France passes controversial 'fake news' law."

106 Benjamin Novak, "Hungary moves to end rule by decree, but Orban's powers may stay," *New York Times,* June 16, 2020, https://www.nytimes.com/2020/06/16/world/europe/hungary-coronavirus-orban.html

107 Shaun Walker and Jennifer Rankin, "Hungary passes law that will let Orban rule by decree," *The Guardian,* March 31, 2020, https://www.theguardian.com/world/2020/mar/30/hungary-jail-for-coronavirus-misinformation-viktor-orban

108 "Coronavirus update: Bill on rescinding the government's emergency powers submitted to parliament today," About Hungary, published May 26, 2020, http://abouthungary.hu/news-in-brief/coronavirus-update-bill-on-rescinding-the-governments-emergency-powers-submitted-to-parliament-today/ ; Anyone who violates the law could face one year in prison and a fine of €75,000.

109 Novak, "Hungary moves to end rule by decree, but Orban's powers may stay."

110 "Dutch Government to launch anti-fake news campaign," *NL Times,* December 13, 2018, https://nltimes.nl/2018/12/13/dutch-government-launch-anti-fake-news-campaign

111 Emma Charlton, "How Finland is fighting fake news – in the classroom," World Economic Forum, published May 21, 2019, https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom/

112 Cristina Tardaguila, "Spain has a new government and its fact-checkers had an impact on the campaign," Poynter, published May 3, 2019, https://www.poynter.org/fact-checking/2019/spain-has-a-new-government-and-its-fact-checkers-had-an-impact-on-the-campaign/

113 Yasmeen Serhan, "Italy scrambles to fight misinformation ahead of its elections," *The Atlantic,* February 24, 2018, https://www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/

elections, Italians were also able to report fake news directly to the police, leading to concerns about the undue interference of the state.[114] Belgium, Finland, Latvia, Cyprus, Luxembourg, Sweden and France have also enacted national media literacy campaigns, while Greece has an official website debunking fake news since 2013.[115] In 2017, the Czech government established a monitoring unit that debunks misinformation and maintains a Twitter account informing the public of its actions.[116]

Some argue that these national-level efforts lead to stronger regulation of internet platforms and less reliance on protections traditionally provided by the European Union.[117] Table 3.1 recaps the major initiatives to tackle fake news in Europe since 2015 when Russian disinformation campaigns in Europe triggered the first policy response to online disinformation.

Timeline of Europe's "fake news" regulations and policies

Table 3.1: Timeline of various laws and regulations implemented in Europe

Year	Legislation/Policy Development/Initiative	Jurisdiction
2015	EEAS East StratCom Task Force's **Action Plan on Strategic Communication**	EU
2016	**Joint Framework on Countering Hybrid Threats is released**	EU
	Finland media literacy schooling curriculum introduced	Finland
2017	[June] **Network Enforcement Act is passed by Bundestag**	Germany
2018	[April] **Tackling Online Disinformation: A European Approach**	EU
	[September] **Code of Practice against Disinformation**	EU
	Observatory for Social Media Analysis (SOMA) is established	EU
	[November] **Law against the Manipulation of Information approved**	France
	[December] **Action Plan against Disinformation**	EU
2019	Netherlands **online fake news awareness campaign**	Netherlands
	[March] **European Media Literacy Week**	EU
	[June] European Commission reports on the performance of the Code concerning the May 2019 EU elections	EU
	[October] **First self-assessment reports** tabled by signatories to EU Code of Practice	EU
2020	[March] **Act XII of 2020 on the Containment of the Coronavirus** enables the Government to imprison anyone found disseminating untrue or misrepresented facts	Hungary
	[May] ERGA release assessment of first year of EU Code	EU
	[May] Independent consultants VAA release assessment of first year of EU Code	EU
	[June] Hungarian Government rescinds extraordinary powers policing COVID-19 misinformation	Hungary
	[June] **Tackling COVID-19 Disinformation – Getting the Facts Right is released, outlining the Commission's expectations for signatories to counter COVID-19 misinformation**	EU
	[September] First baseline reports on signatories' measures to counter COVID-19 misinformation	EU
	[September] European Commission releases its assessment of the first year of the Code	EU

Source: Authors

---

114 Daniel Funke, "Italians can now report fake news to the police. Here's why that's problematic," Poynter, published January 19, 2018, https://www.poynter.org/fact-checking/2018/italians-can-now-report-fake-news-to-the-police-heres-why-thats-problematic/; La Cour, Christina, "Governments countering disinformation: The case of Italy," Disnfo Portal, accessed November 19, 2020 https://disinfoportal.org/governments-countering-disinformation-the-case-of-italy/

115 European Commission, *Assessment of the Implementation of the Code of Practice on Disinformation.* 75-77; Saurwein and Spencer-Smith, "Combating disinformation on social media: Multilevel governance and distributed accountability in Europe," 827-830.

116 Emily Schultheis, "The Czech Republic's fake news problem," *The Atlantic,* October 21, 2017, https://www.theatlantic.com/international/archive/2017/10/fake-news-in-the-czech-republic/543591/

117 Saurwein and Spencer-Smith, "Combating disinformation on social media: Multilevel governance and distributed accountability in Europe," 834.

Conclusion

Europe's actions to facilitate digital platforms' self-regulation to tackle misinformation and disinformation reveal not only the challenges of the endeavour, but outcomes that can be achieved. The assessments of the EU's framework conveyed in this chapter show that such an approach can be effective in parts.

It has mitigated some of the impacts of false and misleading information during elections and crisis events, such as the COVID-19 "infodemic"; promoted reliable, trustworthy information to online users; opened dialogue between platforms and governments; and helped restrict inauthentic and manipulative activity.

Yet, as the Commission acknowledges, while progress has been made toward improving the digital industry's response to the problem – an indication that its expectations are not merely aspirational – more actions by all stakeholders are needed. Overall, the measures signatories implemented under the Code were viewed as incomplete and inconsistent. The monitoring of the code's effectiveness proved difficult – a product of platforms' reluctance to fully embrace the transparency that comes with open information sharing and stakeholder cooperation. And definitions of the problem's scope and terminology were found to be too vague and restrictive. Initially concerned primarily with "disinformation" at the commencement of the Code, the Commission has recently recognised the necessity of incorporating misinformation into the scope of its regulatory remit. The experience of the COVID-19 infodemic, in particular, has demonstrated the urgent threat posed by the spread of misinformation. This shift indicates that attempts to curb the spread of false information cannot be reduced to a study of user "intent". A more nuanced understanding of the complex and often organic exchange of false and misleading information is needed.

Consistent in the Commission's messaging about the Code is an increasing impatience for greater accountability from platforms. The Code is not enforceable as it currently exists, with the Commission indicating a graduation from self-regulation to a more stringent model is under consideration. That said, the EU – alongside independent commentators – have suggested tweaks, not drastic transformation. A shift toward mandated co-regulation has been flagged. Yet despite the EU's rhetoric, such a move is sure to raise concerns about government over-reach as platforms look to protect freedom of speech and their own autonomy. The impending *European Democracy Action Plan* and *Digital Services Act* may suggest the future direction of the EU's framework for managing the spread of misinformation and disinformation online.

While many of the commentators in this chapter and interviewed for this study were reluctant to label the EU approach as the global "gold standard", several admit it may be the best model developed so far. As we see with the development of a Code of Practice in Australia, Europe has had a strong influence on regulation development in other jurisdictions. Despite its self-admitted shortcomings, the EU framework remains an instructive model for legislators around the world.

Australia's approach to online misinformation

Introduction

⌄

This chapter examines recent discussions and developments around voluntary regulatory approaches to misinformation and disinformation in Australia. With the onset of the COVID-19 pandemic and heightened need for quality health information on and offline, 2020 was a watershed year for news and media organisations around the world. It was also a critical year for digital technology companies, with the Australian Government setting an end-of-year deadline for the digital platforms to establish a voluntary framework to counter low-quality and harmful information online. The voluntary code also requires the companies to establish ways for the public to make informed decisions in relation to content quality.

This chapter outlines the background to the formation of these self-regulatory initiatives, beginning with an overview of the Australian Media and Communications Authority's (ACMA) position paper, *Misinformation and news quality on* *digital platforms in Australia: A position paper to guide code development*. The ACMA position paper, released in June 2020, sets out the Australian Government's guidelines for an industry-wide voluntary code of practice for

addressing misinformation on digital platforms and improving news quality. This initiative was born out of the 2019 Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry final report. In response to the ACMA and ACCC initiatives, the platform providers, represented by the Digital Industry Group Inc. (DIGI), produced an *Australian Code of Practice on Disinformation* for public consultation in October 2020. DIGI also commissioned a discussion paper produced by academics at the University of Technology Sydney Centre for Media Transition as a companion document to the draft code.

While there are commonalities and overlap between each of the documents, this chapter discusses the substance of each and points of differences between ACMA's and DIGI's positions that may require further attention before a consensus approach to tackling the problem can be developed.

Background ACCC Digital Platforms Inquiry

In December 2017, then Treasurer Scott Morrison directed the Australian Competition and Consumer Commission (ACCC) to undertake an inquiry into the digital platforms amid concerns about their influence on competition, consumers and society. The inquiry received submissions from Facebook, Fairfax, Google, Netflix and Twitter, among others.[1]

The final report, released in July 2019, included two recommendations dealing specifically with online misinformation and disinformation. Recommendation 14 covered "monitoring efforts of digital platforms to implement credibility signalling,"[2] while recommendation 15

called for the implementation of a "digital platforms code to counter disinformation".[3]

The report recommended that a code to address both disinformation and "malign" information be established, overseen by an independent regulator such as ACMA.

The ACCC advised that a voluntary code should apply to "complaints about disinformation that meet a 'serious public detriment' threshold as defined in the code."[4] The ACCC defines disinformation as "inaccurate information created and spread with the intent to cause harm in relation to news and journalism, or content presented as news and journalism, on their services". As is discussed in more detail in the next chapter of this report, the ACCC definition of disinformation diverges from that of platforms and some commentators. This is not unexpected, as there is no universally agreed definition for disinformation.

---

1   Full list of submissions - https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry/submissions
2   ACMA defines credibility signalling as "flagging trusted sources and providing users with access to information on publishers and other sources" (Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia: A position paper to guide code development* (Canberra: ACMA, 2020), 29, https://www.acma.gov.au/sites/default/files/2020-06/Misinformation%20and%20news%20quality%20position%20paper.pdf
3   Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final report* (Canberra: ACCC, 2019), 34, https://www.accc.gov.au/system/files/Digital%20 platforms%20inquiry%20-%20final%20report.pdf
4   Australian Competition and Consumer Commission, *Digital Platforms Inquiry,* 34.

Like the definition in the *EU Code of Practice on Disinformation,* the ACCC definition is notable for its emphasis on intent. According to the ACCC definition, disinformation involves a deliberate intention to mislead, while misinformation does not. The ACCC also holds that content must be inaccurate to be classified as disinformation. Some technology companies, such as Facebook, argue that the intent of the

person posting suspect content, while pertinent, is for practical purposes too difficult to divine with confidence. So, they focus more on the *behaviour* of online users to detect "inauthentic" use of their platforms. They also point out that not all disinformation is necessarily false information (see chapter five).

The ACCC recommended that ACMA conduct regular monitoring of the

voluntary code. If the code was deemed to be ineffective, it said a more direct regulatory approach should be considered.[5] In response to the inquiry, the Government asked major digital platforms with an online presence in Australia to "develop a voluntary code to cover the recommendations",[6] with ACMA overseeing its development and performance in addressing "the state of disinformation in Australia".[7]

ACMA position paper

ACMA's June 2020 position paper outlined its expectations and recommendations for the code's development. The paper came at a time of significant concern over misinformation in Australia. Widespread online misinformation surrounding the 2019-20 bushfires and the COVID-19 pandemic highlighted the potential for the problem to cause significant community harm.[8] ACMA's position paper was informed by discussions with digital platforms including Facebook, Google, Twitter, Microsoft, TikTok, Apple and Amazon, as well as DIGI. Australian Government agencies such as the ACCC and international media regulators from the UK, Ireland and Canada also contributed insights and expertise.

Consistent with the European Union's approach (see chapter three), a single industry-wide code was favoured.[15] ACMA argued that a single code would engender greater efficiency, more collaboration between platforms and standardisation – leading to more streamlined complaints handling, reporting and measurement processes.[16] It also suggested an "outcome-focused" rather than process-focused approach, with signatories to the code having the freedom to determine what measures to adopt to meet the stated objectives.[17] In doing so they would publicly "demonstrate commitment to addressing misinformation"[18] and a willingness to participate in the code.

ACMA acknowledged that most digital platforms had already implemented measures to combat misinformation and disinformation, as well as to deal with issues around news quality in general. Nonetheless, the position paper argued that greater codification, stringency and transparency were needed.[9] Codification was recommended on the grounds that it would guide new entrants into the industry.[10]

Scope

ACMA argued for a voluntary code that platforms could individually implement. Digital platforms across the industry, comprising "online search engines, social media platforms and other digital content aggregation services with at least one

million monthly active users in Australia," were considered to fall within the scope of a future code.[11] According to ACMA, this would cover Facebook, YouTube, Twitter, Google Search and Google News, Instagram, TikTok, LinkedIn, Apple News and Snapchat.[12] However, it was proposed that other private messaging platforms such as WhatsApp, Weibo and WeChat be excluded from the code – raising questions over why Snapchat, which has similarities to those platforms, *was* included. Major news outlets with an online presence were also excluded from the proposed code because they were "not considered key distributors of misinformation in Australia".[13] ACMA expected platforms to engage in public consultation during the code's development.[14]

Definitions

As noted earlier, there is no general consensus within Australia (or elsewhere) on definitions of terms relating to false and harmful information online. DIGI's approach, which shares some aspects of the European approach, focuses on the term "disinformation" – which it defines broadly as "inauthentic" behaviour. According to DIGI, inauthentic behaviour "includes spam and other forms of deceptive behaviours (including via automated systems) which encourages users of Digital Platforms to propagate content which may cause harm".

5   Australian Competition and Consumer Commission, *Digital Platforms Inquiry,* 34. The report also has recommendations (12 & 13) around digital media literacy in the community and in schools.
6   Australian Communications and Media Authority, Misinformation and news quality on digital platforms in Australia, 1.
7   Ibid., 4.
8   Ibid., 2.
9   Ibid., 9; 2
10   Ibid., 19.
11   Ibid., 3.
12   Ibid.
13   Ibid., 22.
14   Ibid., 25.
15   Ibid., 20.
16   Ibid.
17   Ibid., 23.
18   Ibid., 3.

By comparison, ACMA uses misinformation "as an umbrella term to cover all kinds of potentially harmful, false, misleading or deceptive information, with deliberate disinformation campaigns considered a subset of misinformation".[19] ACMA's position paper adopts similar definitions for individual terms to Claire Wardle's First Draft, and to Hossein Derakhshan's typology often used in Europe (see introduction and chapters three and five). Thus, disinformation is identified as "false or inaccurate information that is deliberately created and spread to harm a person, social group, organisation or country." [20] Misinformation is defined as "false or inaccurate information that is not created with the intention of causing harm."[21] And malinformation is defined as "accurate information inappropriately spread by bad-faith actors with the intent to cause harm, particularly to the operation of democratic processes".[22] ACMA acknowledged that it was sometimes hard to distinguish between these types of malign information.

ACMA also pointed out that potential harm was not always intended. Intention itself "can be difficult to determine", making "the line between bad actors and innocent users… not always clear."[23] ACMA found the 2019-2020 Australian bushfires and the COVID-19 pandemic had highlighted how misinformation, though not intentionally harmful, "has the potential to cause significant harm".[24] Hence, ACMA said discussions limited to disinformation failed to account for the threat posed by forms of false and misleading information where ill-intent was not apparent. It noted that the European code's focus on disinformation would have failed to address the types of misinformation associated with the bushfires and

pandemic.[25] Academics James Meese and Edward Hurcombe, in their policy brief *Regulating Misinformation,* support ACMA's typology, with misinformation as an overarching umbrella term to capture grey areas between definitions.[26]

ACMA divided harm caused by misinformation into two categories – "acute harms", which it said, "have an immediate impact on people, property or society", and "chronic harms", which "result from the cumulative effect of misinformation and may only become apparent over time".[27]

It also argued that the "concept of news quality can be subjective," further complicating the task of measuring information credibility.[28] ACMA also alluded to the wider societal value of access to reliable news content, saying quality news and information "is accurate, reliable and timely, providing people with the knowledge they need to make informed choices and to participate in public life".[29]

ACMA proposed a graduated and risk-based approach, where measures used in response to misinformation and disinformation were proportionate to the risk the content posed. Adopting this approach "may also alleviate some concerns around freedom of speech", since censorship and other strong measures would only apply to the most harmful content.[30] Platforms would thus not be expected to serve as arbiters of truth.[31] Criteria to assess the risk of harm would include content and context; agent and purpose; breadth and speed of dissemination; and distribution channel.[32] DIGI has also referenced the need for a proportional response, and lists 11 different factors to consider before applying one or more measures to counter disinformation.[33]

Monitoring and quality-control activities

As ACMA supports an outcome-based approach, platforms are encouraged to adopt measures to contain misinformation as they see fit.[34] Some of the suggested measures included fact checking, labelling of advertisements, flagging suspicious content, and providing media literacy tools.

The ACMA position paper recognised the importance of data sharing by platforms. It also recognised that the EU code had not yet fully achieved its goal of empowering research communities by overseeing data sharing between platforms and independent researchers.[35] ACMA's approach aimed to address this gap,[36] urging platforms commit to "facilitate research, share relevant data and undertake activities to improve the understanding of misinformation in Australia".[37]

To address a perceived lack of transparency in the industry, ACMA recommended platforms publish community guidelines outlining the responsibilities of platforms and users, and promoting this information widely through emails, landing pages and tutorials.[38] In doing so, ACMA highlighted a lack of transparency in the EU's code of practice.[39] Facebook already had some examples of this kind of practice with its published Community Standards and QandA sections on its webpages.[40] ACMA also proposed a clear complaint handling process to enable users to easily "submit complaints about the performance of the platform against the code and its application of published policies and procedures".[41] This proposal comes amid criticism of the EU code for failing to have clear performance indicators and meaningful objectives and commitments, which is said to have hampered monitoring and compliance.[42]

19   Ibid., 1.
20   Ibid., 9.
21   Ibid., 10.
22   Ibid., 10.
23   Ibid.
24   Ibid.
25   Ibid., 15.
26   James Meese and Edward Hurcombe, Regulating Misinformation: Policy Brief (Melbourne, Analysis & Policy Observatory, RMIT University), https://apo.org.au/node/309357
27   Ibid., 11-12.
28   Ibid., 9.
29   Ibid.
30   Ibid., 12-13
31   Ibid., 12.
32   Ibid., 15.
33   Digital Industry Group Inc., *Australian code of practice on disinformation: Draft for public consultation* (DIGI, October 16, 2020), 9-10, https://digi.org.au/wp-content/uploads/2020/10/Disinformation-Code-draft-for-public-consultaion-.pdf.
34   Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia,* 29.
35   Ibid., 7, 17.
36   Ibid., 17.
37   Ibid., 24.
38   Ibid., 30.
39   Ibid.
40   Guy Rosen, Katie Harbath, Nathaniel Gleicher, and Rob Leathern, *Helping to protect the 2020 US elections*, (Facebook, October 21, 2019).
41   Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia,* 30
42   J. Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative* (Washington D.C.: Carnegie Endowment for International Peace, 2020), 5; Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia,* 16.

ACMA also proposed a monitoring and reporting framework to be developed with input from academia, digital platforms and government agencies.[43] Signatories would be required to create an action plan and then report annually on their performance against the plan. ACMA and/or other independent organisations would also conduct rigorous assessments of the signatories.[44]

Further, ACMA proposed a "misinformation and news quality monitoring and reporting framework".[45] This would guide industry on how ACMA would "measure the effectiveness of the code" and evaluate "the overall impact" of platforms' contributions to combatting misinformation in Australia.[46] As part of its monitoring duties, ACMA would advise the Government on whether further regulatory action was needed if code objectives were not being met.[47]

Local reactions

Australian mainstream journalists and commentators were largely supportive of the ACMA proposals, arguing that technology companies should be bound by the same rules as newspapers, TV and radio. In Australia, journalism ethics are guided by the self-regulatory and voluntary Media Entertainment and Arts Alliance (MEAA) Journalist Code of Ethics; the ABC Act 1983 (for the public broadcaster), and ACMA's oversight of the standards and codes for TV and radio broadcasters that contain specific provisions stipulating "accuracy and fairness" in content. Journalist David Swan wrote that, "the code would make social media platforms responsible for misinformation in the same way that Australian media organisations are bound by regulatory requirements for journalistic ethics and accuracy in news reporting".[48]

DIGI draft code: Australian Code of Practice on Disinformation

In October 2020, DIGI released a draft of the proposed Australian Code of Practice on Disinformation for public consultation. Developed with assistance from the University of Technology Sydney's Centre for Media Transition (CMT) and First Draft, an international project fighting disinformation and misinformation, the DIGI draft code responded to the Australian Government's *Regulating in the Digital Age*[49] – which was the Government's official response to the ACCC's *Digital Platforms Inquiry* – and ACMA's position paper.

DIGI also commissioned the CMT and its affiliate First Draft to assist in the production of a discussion paper to accompany the draft code and provide background context. The discussion paper acknowledges the influence of international examples on DIGI's approach – primarily the EU code and, to a lesser degree, the approaches of Taiwan and India.[50] While acknowledging the need for more action on the issue, DIGI also highlighted measures already implemented by digital platforms "to tackle the propagation of disinformation" on their services.[51]

Scope

DIGI's draft code embraces voluntary elements of ACMA proposals, with digital platforms to "opt-in" to whichever measures they prefer depending on their business model and operational needs. Since "not all objectives and outcomes will be applicable" to all signatories, DIGI said each "may adopt one or more of the measures set out… in a manner that is relevant and proportionate to their different services and products".[52] The opt-in provision would mean platforms are only bound to those commitments that they have nominated.[53] In theory, this aims to accommodate the multiplicity of platforms and their varying characteristics, functions and

43   Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia,* 38
44   Ibid., 24
45   Ibid., 36
46   Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia,* 36.
47   Ibid., 4.
48   David Swan, "Code to rein in spread of fake data," *The Australian,* June 26, 2020.
49   Australian Government. *Regulating in the digital age: Government response and implementation roadmap for the Digital Platforms Inquiry* (Canberra: Commonwealth of Australia 2019), https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf
50   UTS Centre for Media Transition, *Discussion paper on an Australian voluntary code of practice for disinformation* (DIGI, October 16, 2020), 39, https://digi.org.au/wp-content/uploads/2020/10/Discussion-Paper-Final.pdf
51   Digital Industry Group Inc., *Australian code of practice on disinformation,* Section 1.3.
52   Ibid., Section 5.2.
53   Ibid., Section 7.1.

uses. As stated in the discussion paper, "no single technological fix, labelling system or filter" will suffice.[54] Instead, the diversity across digital platforms requires "an equally diverse approach to resolving the impact of misinformation and disinformation".[55] While not directly opposing ACMA's industry-wide approach, DIGI's proposal seeks greater accommodation of the industry's diversity and complexity.

The DIGI proposal covers search engines and platforms that accommodate user-generated content. However, it excludes private messaging services, media texts for entertainment or educational purposes, email services and content authorised by the Australian Government.[56] Hence, the code excludes WhatsApp, Weibo and other popular messaging platforms, as suggested by ACMA.

Definitions

The discussion paper outlined several influences on DIGI's conceptualisation of misinformation and disinformation. Primary influences were the EU code and First Draft, while Britain's Full Facts' definition of levels of harm was also cited.[57] Wardle and Derakhshan's umbrella term of "information disorder", which covers misinformation, disinformation and malinformation, was highlighted in the discussion paper (see also chapter five).[58] ACMA's approach to definitions differs from DIGI's draft insofar as it defines misinformation as the overarching term, under which disinformation and malinformation sit as subsets. An ACMA spokesperson said this was intended to capture a range of harms:

> We adopted 'misinformation' as a catch-all umbrella term – reflecting any potentially harmful false, misleading or deceptive information distributed online, with or without malicious intent. In light of the types of material we were seeing circulating

on digital platforms following the summer bushfires and early stages of the COVID-19 pandemic, we felt this terminology provided platforms with the necessary flexibility to address a range of harmful behaviours and content, while encouraging graduated, proportionate measures that appropriately reflect the level of harm.[59]

The ACMA spokesperson acknowledged the narrower scope of DIGI's draft *Australian Code of Practice for Disinformation* when it comes to false news online:

> DIGI has proposed a much narrower scope – addressing only inauthentic behaviour from users of digital platforms that results in the propagation of potentially harmful digital content for the purposes of economic gain or to mislead the public. Harm in this context is also defined narrowly as imminent and serious threats to democratic political and policymaking processes or public goods such as the protection of citizens' health, the environment or security.[60]

Like the ACMA position paper on misinformation, DIGI's draft code acknowledges the overlap between disinformation, misinformation and similar terms.[61] It accepts that there is no universal definition of the problem, and that in the course of implementing measures to combat it, such terms are likely to be used interchangeably by signatories.[62]

Referring to definitional issues, the ACMA spokesperson stated:

> "As a voluntary industry process, it is ultimately up to interested platforms to reach a consensus on this issue. We are continuing to actively work with DIGI and platforms to better understand each other's views on scope prior to the finalisation of the code."[63]

An affiliate at Harvard University's Berkman Klein Centre and fellow in New America's Cybersecurity Initiative, Camille François, uses a "disinformation ABC" framework – focusing on actors, behaviour and content – to understand harmful online content. Francois, whose framework was cited in the DIGI discussion paper, identified "manipulative actors" (people or groups with the clear intention to disrupt the information ecosystem), "deceptive behaviors" (tactics and techniques used by the actors) and "harmful content" (used to hurt, undermine or influence) as "three key vectors characteristic of viral deception."[64] The DIGI-commissioned report agreed that it was a useful rubric to understand the facets of disinformation.

While DIGI's discussion paper canvassed academic and practical definitions of the problem, it resisted committing to a single approach – perhaps reflecting diversity of views among platforms that comprise DIGI's membership.

Disinformation is defined in DIGI's draft code as inauthentic behaviour, and covers content that is promulgated "for the purpose of economic gain or to mislead or deceive the public, that may cause harm and is not otherwise unlawful".[65] This focus on harm and intention is in step with other approaches, including ACMA's. The DIGI code also adopts a similar definition of disinformation as the EU Code, including "an imminent and serious threat" to "democratic political and policymaking processes".

---

54 UTS Centre for Media Transition, *Discussion paper on an Australian voluntary code of practice for disinformation,* 25.
55 Ibid.
56 Digital Industry Group Inc., *Australian code of practice on disinformation,* Section 4.1; Section 4.2.
57 UTS Centre for Media Transition, *Discussion paper on an Australian voluntary code of practice for disinformation,* 10-11.
58 Clair Wardle and Hossein Derakhshan, *Information disorder: Toward an interdisciplinary framework for research and policy making* (Council of Europe Report, September 27, 2017), https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
59 Interview 14. Correspondence with Andrea Carson, 18 November 2020.
60 Ibid.
61 Digital Industry Group Inc., *Australian code of practice on disinformation,* Section 5.4.
62 Ibid.
63 Interview 14. Correspondence with Andrea Carson, 18 November 2020.
64 Camille Francois, *Actors, behaviours, content: A disinformation ABC: Highlighting three vectors of viral deception to guide industry & regulatory responses* (The Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, September 20, 2019), https://science.house.gov/imo/media/doc/Francois%20 Addendum%20to%20Testimony%20-%20ABC_Framework_2019_Sept_2019.pdf
65 Digital Industry Group Inc., *Australian code of practice on disinformation,* Section 3.2.

Consistent with broader discussions about fake news definitions, the UTS discussion paper questioned the inclusion of intent as a key component when defining disinformation, arguing that, "the question of whether disinformation requires an element of intention needs careful consideration". It said "the difficulties in establishing intention may make it more appropriate to make conduct, rather than content, the focus of regulatory attention".[66] The UTS paper observed that "not all manipulated content is malicious",[67] which complicated the use of intent as a marker of disinformation.

Guiding principles and objectives

The DIGI draft code outlines a set of "guiding principles" underpinning the approach of digital platforms. These included the protection of freedom of expression and user privacy, scrutiny of advertising placement, user empowerment, integrity and security of services and products, supporting independent researchers, and acting "without prejudice" towards other anti-disinformation initiatives.[68]

In step with ACMA's recommendations, DIGI's draft code adopts an outcome-based approach. It's six objectives are to:

- Improve "safeguards against disinformation", including preventing the spread of and exposure to disinformation, and introducing better reporting mechanisms for users
- Disrupt advertising and monetisation incentives for disinformation
- Work to ensure the public benefit of services and products delivered by digital platforms
- Empower consumers to make better informed choices of digital content, particularly around matters that may cause harm

- Strengthen public understanding of disinformation through support of strategic research
- Publicise the measures (signatories) take to combat disinformation, including regular reports to government and/or the public.[69]

These objectives intersect with several areas that ACMA wanted to improve, including data sharing, transparency, and monitoring and compliance processes.

DIGI proposed 16 further "measures" to which platforms could "opt-in" via a "nomination form". While little description was provided of what these measures would specifically entail, the draft code provides examples of specific actions platforms might take, including content removal, partnerships with third-party groups and fact checking.[70]

In line with ACMA's recommendations, DIGI's draft code suggests a graduated risk-based approach to evaluating disinformation. Under this model, measures would be "proportionate and relevant to their specific context".[71] Risk factors that platforms might consider include the:

- Types of actors involved
- Breadth and speed of the content's dissemination
- Level of harm
- Behaviours and intent behind the online activity
- Credibility of the content
- Freedom of speech considerations.[72]

As with the EU Code, the importance of freedom of speech is emphasised in DIGI's proposed code. For example, the document states that signatories should not be required to "remove content solely on the basis of perceived falsity if the content would not otherwise be unlawful".[73] Requirements to "signal the veracity" of user content are also rejected.[74] In this way, platforms uphold their "strong desire" to avoid being

arbiters of truth.[75] Instead, they state that their responsibility is to protect users from potentially harmful content while upholding their freedom of expression.[76]

DIGI's proposal states that, in addition to digital platforms, "a range of relevant stakeholders have roles and responsibilities in dealing with disinformation including public authorities, academia, civil society, and news organisations".[77] It also stresses the need for collaboration between all stakeholders, and endorses regulation encouraging media literacy and digital literacy as a way to ensure further sharing of responsibility for combating the problem by news organisations and the public.[78]

Monitoring and quality-control measures

Under monitoring mechanisms outlined in the code, DIGI would serve as the code administrator, and oversee a committee that would meet every six months to evaluate signatories' performances in meeting their nominated commitments.[79] Signatories would report progress annually to DIGI, the Government and/or the public. Signatories would also commit to a complaints-handling mechanism within six months of the code's commencement, and submit to regular monitoring from DIGI to evaluate code compliance. The code would be reviewed after two years, with input from all relevant stakeholders.

66   UTS Centre for Media Transition, *Discussion paper on an Australian voluntary code of practice for disinformation,* 10.
67   Ibid., 36.
68   Digital Industry Group Inc., *Australian code of practice on disinformation,* Section 2.8.
69   Digital Industry Group Inc., *Australian code of practice on disinformation,* Section 5.
70   Ibid., Section 6.2.
71   Ibid., Section 6.1.
72   Ibid.
73   Ibid., Section 2.2.
74   Ibid., Section 5.6.
75   UTS Centre for Media Transition, *Discussion paper on an Australian voluntary code of practice for disinformation,* 25.
76   Digital Industry Group Inc., *Australian code of practice on disinformation,* Section 2.2.
77   Ibid., Section 1.6.
78   UTS Centre for Media Transition, *Discussion paper on an Australian voluntary code of practice for disinformation,* 22.
79   Digital Industry Group Inc., *Australian code of practice on disinformation,* Section 7.3.

Comparing ACMA and DIGI positions on a new code

DIGI's proposed code of practice responds to some key elements in ACMA's position paper. It supports a requirement on platforms to share data with one another and with other stakeholders, including independent researchers, to address the spread of online disinformation.[80] The code also addresses concerns about transparency, outlining commitments for financial support and non-interference in independent research.

However, the draft code also demonstrates DIGI's concerns about privacy and the "need for transparency to be balanced against disclosure risks".[81] It states that, "in implementing commitments to promote the public transparency of measures taken under this code,"[82] the release of information to the public opens digital platforms to exploitation by malicious actors, "which can result in more deceptive behaviour".[83] In addition to maintaining user privacy, platforms are also concerned about protecting the integrity of their services and existing measures that aim to combat disinformation. The ACCC has criticised as "opaque" existing measures and algorithms that platforms employ to demote misleading content. It argued this lack of transparency limited a regulator's capacity to measure their efficacy in achieving the code's stated outcomes.[84]

DIGI's proposals do not detail intended consequences for platforms that fail to follow through on their commitments. This may be due to the assumption that under the monitoring and compliance procedures set out by the code, ACMA will oversee such penalties.

ACMA responded critically to DIGI's draft code in comments reported in *The Sydney Morning Herald* in late October 2020. Citing the absence of detail about how DIGI would achieve the code's objectives, ACMA chair Nerida O'Loughlin was quoted saying: "The draft code released by DIGI for public consultation is a long way from the model that we proposed to address these important issues."[85] *The Sydney Morning Herald* article pointed out that DIGI's proposed criteria for evaluating and acting on contested content could allow material from anti-vaccination activists or conspiracy theorists "not published with malice" to escape action under the code.

ACMA has warned that if differences in perspectives between the parties on voluntary co-regulation are too great, a government regulatory framework may be the inevitable next step.[86]

Table 4.1: Expected dates for draft and implementation plan of Australia's voluntary Disinformation Code

Estimated Date	Expected Action
June 2020	ACMA position paper
July-August 2020	Workshops to discuss ACMA monitoring and assessment
October 2020	Monitoring framework
October 2020	Industry draft code released for public review and consultation
24 November 2020	Public submissions to DIGI's Draft Code close
December 2020	Industry code delivery deadline
January 2021	Action plan published by signatories
June 2021	Assessment report to government

Source: Author

80   Ibid., Section 5.19.
81   Ibid., Section 5.7.
82   Ibid.
83   UTS Centre for Media Transition, *Discussion paper on an Australian voluntary code of practice for disinformation,*19.
84   Australian Competition and Consumer Commission, *Digital Platforms Inquiry,* 1.
85   Zoe Samios and Lisa Visentin, "ACMA: Tech giants' code to handle fake news fails to meet expectations," *Sydney Morning Herald,* October 26, 2020.
      https://www.smh.com.au/politics/federal/acma-tech-giants-code-to-handle-fake-news-fails-to-meet-expectations-20201026-p568oq.html
86   Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia,* 37.

Conclusion

Australia's approach to tackling the spread of misinformation on digital platforms so far is based upon voluntary cooperation between the major digital platforms (represented by DIGI) and Australia's media regulator (ACMA). This is consistent with the European model of voluntary co-regulation to tackle online disinformation. As confirmed in this chapter, ACMA and DIGI share a stated commitment to addressing online misinformation and disinformation, and share some common ground about what is required to achieve it.

Their proposals are informed by key aspects of the European approach – in particular the shared preference for voluntary participation, and for an outcome-focused approach. However, the parties' differing approaches to defining misinformation and disinformation – ACMA has a broad conceptualisation of misinformation capturing all forms of deceptive behaviour, information, and conduct, while DIGI's proposes narrower definitions – leaves them at odds on key issues. Without a shared understanding of these key concepts, attempts to build consensus towards the voluntarily regulation of the quality of information, and to adhere to a common standard of conduct in the digital sphere, may be jeopardised.

The next three chapters report the original findings of this study. The three chapters (chapter 5-7) focus exclusively on the user experiences of online misinformation and governments' and digital platforms' responses to it in Singapore and Indonesia. These findings provide rich lessons for Australia as it considers its next steps to manage this urgent, yet insidious problem.

CHAPTER 5

What is online misinformation — and why is it a problem?

Introduction

⌄

The lack of a clear, universally agreed definition of online misinformation is perhaps the biggest obstacle to achieving consensus on how to tackle the problem in countries like Indonesia and Singapore.

Among those who participated in this research project, significant diversity of views emerged on:

- What defines online misinformation
- The prevalence and scale of the problem
- The consequences for digital platform users.

Yet, amid the contrasting viewpoints on the nature of online misinformation,

there was general consensus on the notion that it is a compelling problem in both Indonesia and Singapore, requiring major remedial action. Participants broadly agreed that unchecked online misinformation has the potential to seriously disrupt citizens' access to reliable information, and that this can have dire implications for democratic participation, freedom of speech and, in some instances, public health and safety.

In this chapter we explore in detail the views of participating experts – technology company experts, journalists, editors, academics and community-based activists – about the nature and scale of online misinformation, and their individual online experiences that helped shape their views. This provides essential background to the next chapter, which examines ways in which governments and digital platforms in Indonesia and Singapore can (and do) manage perceived online misinformation, and identifies particular areas that contributors to this project believe require the most attention.

Definitions: Misinformation, disinformation and malinformation

As suggested in the introduction, online misinformation is a complex phenomenon that cannot be simply or universally defined. National governments, technology platforms, academics and other experts have so far failed to achieve consensus on precise definitions of popular terms such as misinformation, disinformation and fake news.

To try to mitigate the confusion and achieve consistency and clarity, this report has adopted the following definitions for online misinformation and disinformation:

**Online misinformation** is the spread of inaccurate or misleading content online.

Online disinformation is the spread of inaccurate or misleading content online with conscious intent to mislead, deceive or otherwise cause harm.

Thus, we characterise online disinformation as a major subset of the broad, overarching problem of misinformation. By our definition, misinformation can be spread with or without ill-intent, while disinformation necessarily involves ill-intent. We have adopted these definitions – and in particular a broad interpretation of misinformation – in part because they closely align with the usage of experts who participated in this project.

We accept that these definitions are not standardised. For example, First Draft, a non-profit global coalition of newsrooms, universities, online platforms and civil society groups, led by academic Claire Wardle, recognises seven types of potentially problematic online content – or what it calls "information disorder" – in three broad categories: misinformation, disinformation and malinformation[1] (see Figure 5.1 next page).

---

1   Claire Wardle, "The Need for Smarter Definitions and Practical, Timely Empirical Research on Information Disorder." *Digital Journalism*, 6,8 (2018): 951-963.

Figure 5.1: Seven types of "information disorder" ranging from low to high risk of harm
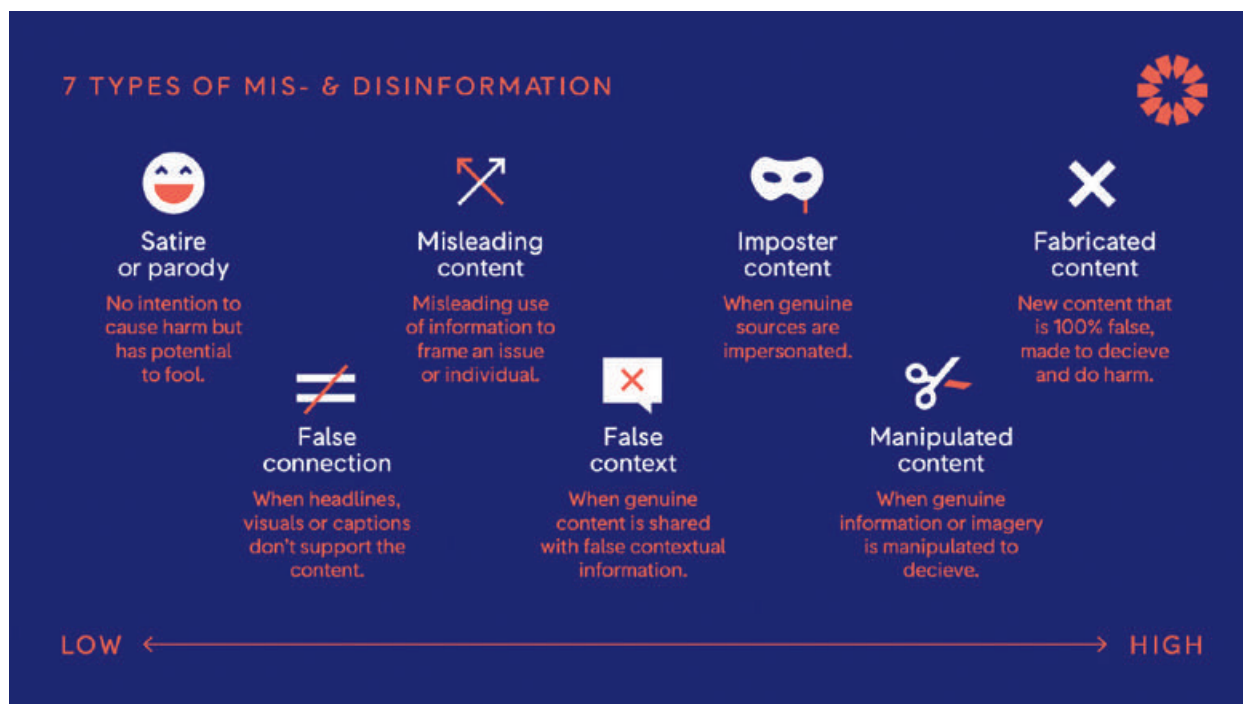
Source: First Draft, 2020[2]

According to this schema, "misinformation" refers to verifiably false content that is spread *without* the intention of causing harm. 'Disinformation', by contrast, is false information spread with the *intention* of causing harm. The British Government is more expansive when defining disinformation – referring to false or manipulated information that has been produced or distributed for political ends that may be damaging to democratic processes, or that may lead to personal or financial harms.[3] Wardle identifies a further sub-category of problematic online content – malinformation – which she defines as truthful information intended to cause harm, such as malicious gossip.

Wardle's fake news typology, like this report's terminology, is not universally accepted, as the extensive debates and disagreements outlined in this chapter reveal.

Facebook's approach to the issue starts from the premise that a person's intention when posting information online is difficult to divine. The company therefore defines misinformation based on the veracity of the content, rather than on the perceived intent of the user. And it defines disinformation with reference both to the actions of those who spread it, and to the content's propensity to cause harm. However, it labels such activity "coordinated inauthentic behaviour" rather than the more popular disinformation.[4]

Wardle acknowledges that information disorder is a "fluid spectrum". This is readily observable in the ways false content can be variously classified as misinformation and disinformation, sometimes depending on its timing, and how it can have varying consequences, depending on who circulates it, how it is spread, and why. So while the overwhelming focus of this chapter is

on misinformation, we also examine disinformation – in part because of the inherent fluidity of these concepts and definitions. The variety of views among participants in this project on how to define the issue and its essential components is reflective of a lack of clear consensus in wider community debates.

Amid the debates, however, there is at least some agreement among experts on how to distinguish misinformation from disinformation. According to one digital platform expert, a useful way to define misinformation is by what it is *not*:

> Misinformation is false and misleading information that is shared not necessarily out of bad intent. It is shared when people may not be fully aware that it's false. And that's very different from disinformation, which is false information that is shared by a person who knows that it's false, and they do so with an intention to mislead other people.[5]

2   Claire Wardle, "The Need for Smarter Definitions and Practical, Timely Empirical Research on Information Disorder.", 953; Figure used with permission from First Draft, email correspondence with author, 17 November 2020.
3   James Meese and Edward Hurcombe, *Regulating Misinformation: Policy Brief* (Melbourne: RMIT University, 2020), 1.
4   Nathanial Gleicher, *Coordinated Inauthentic Behavior Explained.* (Facebook, 2018, 6 December), https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/
5   Interview 1, interview with Andrea Carson, 7 August 2020

The Editor-in-Chief of *Tempo* magazine in Indonesia, Wahyu Dhyatmika, stressed the importance of intention when separating the two concepts and referred to the First Draft concepts:

> Misinformation is when false information is published or shared widely, not with ill-intent, but mostly because of ignorance. Disinformation is more dangerous because there's an intention to spread confusion or anxiety.[6]

But some observers, including participants in this project, find this emphasis problematic because, they argue, it is not possible to know an individual's intentions when sharing false information online. Hence, some experts are more focused on the *behaviours* of online users and the veracity of the *content* rather than *intention*.

Technology companies have become particularly focused on *behaviours* of individual users when seeking to identify online disinformation. For example, a "super poster" who generates the same content hundreds of times can attract scrutiny in this context, as can people setting up multiple accounts with fake identification and other apparently "inauthentic" actions. By contrast, the platforms tend to identify misinformation not by behaviour but by the factuality of the content. One digital platform expert described the approach thus:

> Misinformation typically deals with content, false information, being shared, being spread. We believe that disinformation is not about content, because someone proposing disinformation may be doing it based on truth – they may be promoting true things – but misrepresenting it in certain ways. And therefore we look at users' behaviours.[7]

When *misinformation* is defined by the veracity of the content, a logical response to the problem is fact checking.[8] By contrast, managing *disinformation* tends to involve tracking and curbing behaviours and, if harm is occurring, removing the content and/or the user.[9] However, distinguishing between misinformation and disinformation can be more complicated than just focusing on the content and behaviour, as one academic explained:

> It gets muddled up when an individual picks up disinformation and spreads it unknowingly. False information may be deliberately planted, designed to be picked up by individuals, and then spread by individuals on their closed social media networks.[10]

This potential for disinformation to be unwittingly distributed by others who believe it to be true adds another layer of difficulty to defining, and therefore mitigating the problem. And the emergence of video and pictorial content such as "deep fakes" – doctored images of individuals, often celebrities – further complicates these issues:

> A deep fake is a special classification where it's a hybrid between misinformation and disinformation. It's misinformation, because it's usually synthetic and fake. It's also disinformation because someone has to be purposely trying to create it to deceive. So there is an adversarial motive behind the scenes.[11]

Thus, according to the typology of Wardle and others, a false story can be either, or both, misinformation and disinformation depending on who is spreading it and why, and its impacts and potential for harm.

Another key consideration is transparency. Historian and Managing Director of the *New Naratif* in Singapore PJ Thum believes the lack of transparency about who's behind a fake news story and what their intent is, are the main problems with misinformation online. He argued that unlike real news, where reporting agendas are more transparently subjective, those behind fake news disguise their subjectivity:

> With fake news, the problem is that it tries to present itself very often in a way that is objective in order to mislead, to influence politics and influence public opinion. But it's not transparent about its intention. So I think those are the two main things – designed to mislead, and lack of transparency about who's behind it, where it's coming from and what are its intentions.[12]

Wahyu Dhyatmika argued that anonymous and fake automated (bot) accounts made it easier for organisations and individuals to attack, bully and spread misinformation. He said his outlet often received anonymous online threats after publishing critical stories about powerful individuals and organisations, including the Indonesian Government. "Most of the threats come from bot accounts, so it's orchestrated. But we never can pinpoint these cyber-attacks."

The case for banning and removing anonymous and bot accounts to reduce misinformation online might seem compelling. However, such an approach could have unintended consequences in countries where some activists rely on anonymity to circumvent government restrictions on freedom of expression.

---

6   Author interview with Wahyu Dhyatmika, Editor-in-Chief of *Tempo* magazine, 24 August 2020
7   Interview 4, interview with Andrea Carson, 7 August 2020
8   ibid
9   Interviews 4; Interview 9, interview with Andrea Carson, 8 September 2020
10   Interview 3, Interview with Andrea Carson, 18 August 2020
11   Interview 4
12   Author interview with PJ Thum, Historian and Managing Director of the *New Naratif,* 19 August 2020

As one platform expert stated:

> It's a complicated issue. We have very clear policies, like the "real name policy" so that we can remove fake accounts. But then there are certain jurisdictions where it's harder to enforce because people in opposition under authoritarian regimes rely on those fake accounts to be able to express themselves without persecution.[13]

Further, not all fake content is potentially harmful. A fake account set up in a pet's name would be in most cases an example of harmless online misinformation. An online parody relying on obviously false content might also be deemed harmless. But where should the line be drawn? One interviewee said: "When it comes to fake accounts, are we talking about malicious fake accounts? What is it that we're trying to solve here?" Social media and digital platform experts argued that more clarity and agreement on definitions of misinformation and disinformation would enable all platforms to operate more consistently and develop consistent standards.[14] This included avoiding the broad term "fake news".

> We don't really use the term fake news, because we understand that it means different things to different people... So the term that we use a lot is false news, because then it's very neutral and it doesn't make a judgement about intent.[15]

One academic disliked the term fake news for another reason – it was an oxymoron. "I don't agree with the concept of fake news because news is not fake."[16]

Indonesians commonly describe fake or false news stories as "hoaxes" – though usually in reference to disinformation rather than misinformation, according to participants in this project:

> Hoax is relatively similar to the concept of disinformation, meaning that the information is not accurate, and it is intentionally produced or distributed to harm people. Misinformation is actually different in terms of its intention.[17]

Misinformation and disinformation have been around for centuries. What's different now is that the internet has enabled and facilitated the easy and rapid spread of false information by almost any individual, and on a scale previously unimaginable – in volume and audience reach. The mass penetration of online misinformation into the everyday lives of citizens in countries like Indonesia and Singapore has led some observers to suggest people may now be more alert to falsehoods and crude propaganda than in the past. PJ Thum said that in the first decades of advertising, citizens were more susceptible to claims that, by today's standards, would seem "obviously invented" or "exaggerated". At the same time, despite increasing public awareness of propaganda and false claims, the "people who run misinformation campaigns are getting more sophisticated at it," said PJ Thum.

One academic argued there should be no distinction between online and offline when it comes to regulating misinformation:

> I think intention is key. We've always had human errors as a result of being rushed with deadlines to get to the printers and so forth. I think the issue with misinformation is the deliberate attempt to influence using false information. We've had [propaganda] like in the Hearst newspapers in the US [during the Spanish-American war]. So I don't see a difference there. It's just

> now, I think the difference is that for, especially online, it is being spread not by companies, but by individuals. So your friends are now spreading such information, not just the mainstream media.[18]

As discussed in the next section, ambiguity around the definitions of misinformation and disinformation, and the overlap between them, can present serious challenges for authorities trying to deal with false information online – in particular for persuading technology platforms and citizens, including activists, to comply with state measures to remove it.

Government definitions

Although government representatives did not participate in this project, several interviewees shared their experiences and insights into how legislators in Singapore and Indonesia view and define misinformation and disinformation. "A lot of countries look at misinformation and disinformation as a content problem, and that makes it really hard for us," said a digital platform expert.[19] The tendency of governments to conflate misinformation and disinformation can have significant consequences when it comes to prosecution of cases. For example, a true believer in a false conspiracy theory may spread the information with a virtuous intention to "enlighten" others.[20] But if governments define this content as disinformation, they "risk criminalising people who themselves have been duped." This punitive approach, arising out of a catch-all definition and a legislated response, may make it more difficult for Facebook and other social media companies to combat disinformation:

> Targeting or criminalising people sharing this type of misinformation may not be the best solution to solving disinformation because it simply drives them underground and then they try to hide their sources.[21]

---

13   Interview 13, Interview with Andrea Carson, 16 September 2020
14   Interview 13
15   Interview 1
16   Interview 7, interview with Andrea Carson, 19 August 2020
17   Interview 7
18   Interview 3
19   Interview 4
20   Interview 4
21   Interview 4

Such situations may encourage conspiracy theorists to create fake online accounts. And if there are many fake accounts, "that creates lots of noise," said the digital platform expert. "How do we locate the really bad ones in a timely manner?"[22]

Fake Facebook accounts – which the company says its reports show constitute about five per cent of worldwide monthly active users – are now officially banned under company policy. In the second quarter of 2020 alone, Facebook said it blocked and deleted about 1.5 billion fake accounts.[23] However, as mentioned previously, this policy has potentially negative implications for activists vulnerable to political persecution in less liberal countries.

Digital platform companies also have misgivings about the binary approach of governments to defining misinformation – saying they tend to divide content simply between real and false. This approach failed to address the need for a balance between free and "responsible" expression. It was used by some governments to favour censorship over freedom of speech. As one digital platform expert said, the Indonesian Government "considers that all misinformation are of equal weight and should not be tiered based on topics such as prevalence and virality."[24]

Social media companies' definitions and policies

With their policy of explicit differentiation between misinformation and disinformation, some platforms have separate divisions and staff assigned to deal with cases of both as they arise.[25] A digital platform expert said that under their platform's approach to misinformation, content was assessed based on "what the content says, as opposed to the user's intent," which he said was "very difficult to judge."

Hence, the company was primarily focused on fact checking to ensure the accuracy of content. And when it came to government requests to have content corrected or removed, the company's response was "based on… whether the correction is correct. So if the content is accurate, and the government is trying to promote false information, we would refuse to comply."[26]

While Facebook sees advantages in having separate divisions dealing with misinformation and disinformation, this approach can lead to problems. As previously mentioned, the same false story can be deemed both misinformation and disinformation, depending on who is spreading it and why. Dealing with misinformation separately to disinformation can also potentially delay an organisation's response times.

A disinformation specialist at one platform said the in-house disinformation team was mostly concerned with various issues including account security (accounts being misused) and transparency to prevent malign actors deploying propaganda on the site, including propaganda from state-controlled media.

> The primary thing that we (disinformation team members) do is protect our platform and our users against influence operations. (But) we don't look at content, we look at behaviour.[27]

Amid the spread of false information and bogus remedies surrounding COVID-19, digital platforms have recently acknowledged that well-meaning misinformation can also cause great harm. Facebook has consequently developed a "misinformation and harm" policy, allowing it to remove misinformation with the potential to cause harm to users.[28] The platform has another harm-related policy surrounding hate speech, which allows for removal of any discriminatory content based on personal characteristics including race and religion.[29]

At the time of interviews for this project in August and September 2020, platforms maintained an exemption for political communications from their "malicious actors" category of content to be removed if it involved politicians.[30] One rationale for this exemption was that politicians were not considered malicious actors.[31]

> Malicious to us mean you're trying to lie, misrepresent yourself to someone. Politicians don't misrepresent themselves. They may misrepresent their positions. That's not a problem (for us). We don't think that's inauthentic. That's authentic. If they are lying politicians, they're authentically lying.[32]

The company position meant that "really blatant" falsehoods or misleading content in political speeches were exempt from the platform's fact checking policy.[33]

The platform policy expert said the platform did not allow politicians to spread misinformation that could lead to harm, such as harmful COVID misinformation, or misinformation that could lead to violence. "We do not allow politicians to share such misinfo and have removed a number of politicians' content under the policy."[34]

Since the interviews were conducted (and at the time of writing), both Facebook and Twitter have adopted proactive stances on alleged false content surrounding the 2020 US Presidential election, with both platforms placing warnings on some political content.

The most notable examples were labels added to tweets by President Donald Trump claiming voter fraud. Twitter added the words, "This claim about election fraud is disputed," and provided a link to information discounting the President's claim (see Figure 5.2 on the next page).[35]

---

22   Interview 4
23   Facebook. *Fake Accounts.* (Facebook, 2020). https://transparency.facebook.com/community-standards-enforcement#fake-accounts
24   Interview 9, interview with Andrea Carson, 8 September 2020
25   Interview 9
26   Interview 1
27   Interview 4
28   Interview 9
29   Interview 1
30   Interview 1; Interview 4
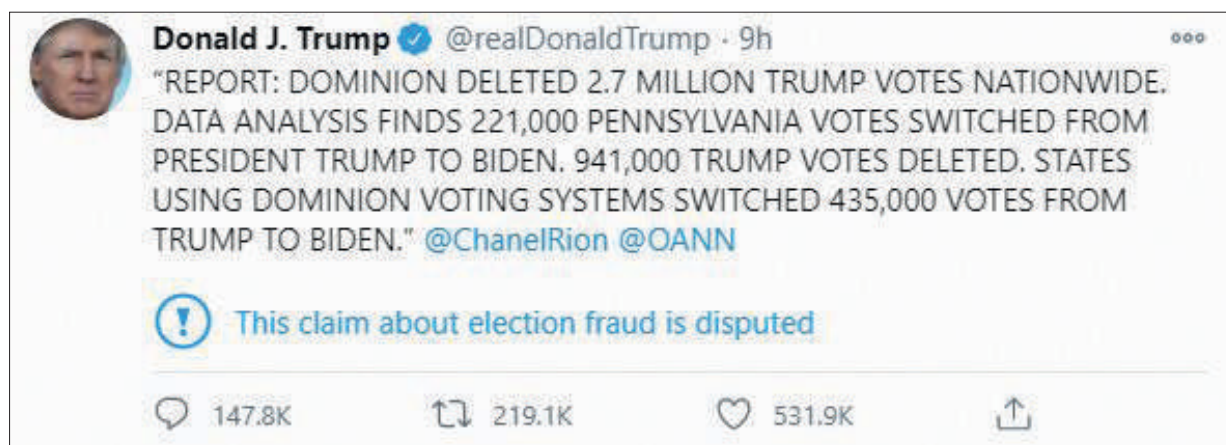31   Interview 4
32   Interview 4
33   Interview 1
34   Interview 4
35   Twitter. *Voter fraud of any kind is exceedingly rare in the US, election experts confirm* (Twitter, 2020) https://twitter.com/i/events/1308626736066617344

Figure 5.2: Donald Trump's contested Tweets

Source: Twitter, Donald Trump account 12 November 2020

Civil society organisations and academic perspectives on definitions

Community-based actors such as non-government organisations and volunteers tend to adopt definitions of misinformation used by academics and/or multinational organisations such as the United Nations. The Chair of MAFINDO, a civic organisation that tackles online hoaxes in Indonesia, Septiaji Eko Nugroho, said his group embraced First Draft's three-category schema, entailing "misinformation, disinformation and malinformation". This was also embraced by UNESCO.

Identifying the scale and effects of online misinformation

Interviewees for this project were equivocal on whether the problem of online misinformation in Singapore and Indonesia had been curbed, or was getting worse. Part of the problem was that the quantum of misinformation was so difficult to measure and compare over time. It was also dependent on country context.

A digital platform expert acknowledged the difficulty:

> That is actually hard to answer because our capability has been expanding. So we're detecting more. But that might be because we're now more capable, or it may be because there's more misinformation and disinformation. We don't have a whole picture.[36]

In Indonesia, Facebook removed 170 items between July and December 2019 in response to requests by the Communications and Informatics Ministry (KOMINFO) and the Indonesian National Police over alleged violations of laws related to treason and separatism, unlawful assembly, manipulated images, promotion of regulated wildlife products, and extremism.[37]

During the same period in Singapore, 16 items were removed, including 10 allegedly containing material inciting racial hatred, strife and intolerance. Restrictions were also placed on five items reported by the Health Sciences Authority as breaching laws on regulated goods. Restricted access was applied to one item relating to alleged defamation.[38]

While Facebook reports twice a year on removals or restrictions on misinformation and disinformation based on local laws, misinformation is generally not reported for individual nations. As a company employee explained:

> We're not doing it because it is actually quite difficult. Content that is in English language is used in various countries. One item could be posted in one country, consumed in other countries and reported from another country.[39]

---

36   Interview 4
37   Facebook. *Restrictions by Product: Indonesia*. (Facebook. 2020), https://transparency.facebook.com/content-restrictions/country/ID
38   Facebook. *Restrictions by Product: Singapore*. (Facebook. 2020), https://transparency.facebook.com/content-restrictions/country/SG
39   Interview 1

However, for languages confined largely to one nation: "I do think there could be a way to release more information or to be more transparent … But that's a work in progress."[40]

One platform expert in Singapore believed online misinformation seemed less prevalent in the city-state in late 2020 compared to other times:

> I think it's been a bit quieter lately. I would like to think it's at least partly because of our work with the fact checkers… We [are] able to get to at least the most viral, the most potentially harmful misinformation.[41]

Facebook's strategy to deal with "false news" is three-fold[42] involving removing, reducing and checking quality of information:

- Remove accounts and content that violate its *Community Standards* or *ad policies*
- Reduce the distribution of false news and other inauthentic content like clickbait by altering algorithmic flows
- Extensive fact checking
- Adding context to news posts.

In some jurisdictions, Facebook has added a circular information or context button with an "i" in it on the bottom right corner of shared news stories to enable users to make judgements about the veracity of news stories (see Figure 5.3). When clicked the button provides information about what a publisher has previously posted, its Wikipedia page and where the post has been shared. It also provides the user an opportunity to follow that news outlet to add "quality" news to their feed.

None of the digital platform experts interviewed for this project believed that the problem of online misinformation had been adequately tamed – yet. One platform expert cited the technical and temporal difficulties in addressing false content quickly:

Figure 5.3: Facebook provides context to news posts using the info button

Source: Author

> If a video is watched by 20 million people and it contains harmful misinformation… The fact that we were able to remove it after six hours, to me, shows that we're getting better at these things because before it might have taken us a lot longer. But if it was already watched by 20 million people after six hours, clearly we have to do a lot better.[43]

The sheer volume and rapid spread of false information about COVID-19 underlined the broader potential of online misinformation for global harm. A digital platform expert said the pandemic presented new and difficult challenges for technology and social media companies, with global conspiracy theories, misinformation and sometimes state propaganda "all mixed in," while the platforms were still trying to deal with other sources of false information as well:

> COVID-19 is a new topic that is bringing a lot of this out. That doesn't mean that the other kind of disinformation networks have stopped. They're still going on, and we need to prioritise COVID-19 but work on them too.[44]

He said the problem was particularly acute in Asia. "The way this information works in APAC is slightly different than the way it works out in Europe or the USA. There [in Europe and US] the actors tend to be much more organised."

The Chair of MAFINDO, Septiaji Eko Nugroho, hoped that fact checking and media literacy initiatives spreading across Indonesia would help mitigate online misinformation. However, there was still much progress to be made on media literacy, which would enable Indonesians to more readily identify false news and avoid sharing it:

> Even some people with high education still share misinformation, so it is quite complex. It's not only related to the level of education; people still don't understand how to read online information correctly.[45]

---

40   Interview 1
41   Interview 1
42   Facebook. *Hard Questions: What's Facebook's Strategy for Stopping False News?* (Facebook, 2018, 23 May) https://about.fb.com/news/2018/05/hard-questions-false-news/
43   Interview 1
44   Interview 4
45   Septiaji Eko Nugroho, interview with Andrea Carson, 26 August 2020

Common forms of misinformation

Political misinformation and hate speech are considered among the most prevalent and problematic forms of online misinformation in both Singapore and Indonesia. One platform expert said that if misinformation from "hate groups" was placed under the banner of political misinformation, "then politics would be the most common form of misinformation."[46] He highlighted the potentially dire consequences of hate speech mixed with politics:

> I think there's more misinformation in this APAC region that leads to real world harm in the sense of physical violence, as we've seen in Myanmar and Sri Lanka, and Indonesia to a certain extent.[47]

Damar Juniarto observed that political misinformation tended to focus on individuals rather than parties' policies. Politicians and candidates were common targets for misinformation "hoaxes" and rumour.[48]

The next most common type of false news was the "mischievous" variety, such as conspiracy theories and related hate group content.[49] False and misleading content created to make money was also becoming more common, according to a technology platform expert. These types of false content align with Wardle's typology in Figure 5.1.

Misinformation about health issues such as COVID-19 was also prominent, and in Indonesia was sometimes blended with political conspiracy theories (see example below).[50]

Box 5.1 Indonesia: combining political and health misinformation

Pro-Prabowo netizens usually produce a lot of hate speech on how Indonesian President Joko Widodo (known as Jokowi) handled COVID. Like they accuse Jokowi of creating the conspiracy theory on COVID, that COVID is not real, COVID is about [a] money arrangement between Indonesian government [and the] World Health Organisation.[51]

While Facebook has been widely used in both Indonesia and Singapore to spread misinformation, the Facebook-owned and encrypted WhatsApp has also been a popular platform for misinformation spreaders in Indonesia.

> It's particularly bad because of the number of WhatsApp users in Indonesia. One person tends to have more than one (account) and so the approach to tackle misinformation has to be different because it's end-to-end encrypted.

Facebook's misinformation strategy on WhatsApp has included limiting the number of times that messages can be forwarded: "You can only forward a message to up to five people – this is now a global feature, not just in Singapore and Indonesia,"[52] a Facebook expert confirmed.

In Singapore, much of the content targeted under the Government's Protection from Online Falsehoods and Manipulation Act (POFMA) has focused on statements by political opponents of the ruling party, and sometimes journalists and digital platforms.[53]

From its enactment in May 2019 up until October 2020, POFMA was used 71 times to prosecute cases of alleged online misinformation. Most orders under POFMA have been "correction directions" requiring a correction notice and a link to the facts alongside a statement about why the content has been deemed false. Other orders require the removal of content and blocking websites. Facebook had received more than 20 of these orders, including orders to post correction notices and to disable access to web pages at the time of writing. Twenty orders were posted during Indonesia's general election period from 23 June and 10 July 2020. Many of these related to questions around government policy,[54] raising concerns that POFMA was being used by the ruling party to shut down political debate and dissent. As one academic observed:

> I think the fear now is this is a slippery slope kind of situation where POFMA will be used as a tool for politically motivated censorship. During the elections, there were instances where it bordered on politically motivated censorship.[55]

---

46   Interview 4
47   Interview 1
48   Author interview with Damar Juniarto, Executive Director SAFEnet, Southeast Asia Freedom of Expression, 31 August 2020
49   Interview 4
50   Interview 11, Interview with Andrea Carson, 20 August 2020
51   Interview 7, Interview with Andrea Carson, 19 August 2020
52   Interview 1
53   Interview 11, Interview 3, Interview PJ Thum
54   Aqill Haziq Mahmud "IN FOCUS: Has POFMA been effective? A look at the fake news law, 1 year since it kicked in," *Channel NewsAsia*, 2020, 3 October, https://www.channelnewsasia.com/news/singapore/singapore-pofma-fake-news-law-1-year-kicked-in-13163404
55   Interview 11

Negative consequences of online misinformation

Participants in this project identified a wide spectrum of negative consequences attributed to the spread of online misinformation in Indonesia and Singapore. These included emotional harm to members of targeted minority and vulnerable groups such as the LGBTI community and women (in the case of misogyny); physical harm arising out of misinformation that incites violence; racial and religious based vilification; and public confusion and distrust resulting from citizens being unable to distinguish misinformation from fact.

Emotional and physical harm

Real world harm is more often associated with online disinformation rather than misinformation. But misinformation can also cause distress – for example, through online harassment and bullying – and physical harm through misinformation that incites violence, or adverse health outcomes due to false information about COVID-19 treatments or other diseases. Septiaji Eko Nugroho cited a video clip online featuring a celebrity with 3 million followers who interviewed a purported professor offering medicine to treat COVID-19. "But actually he's not a professor, and it is not really medicine. It's like herbal remedies."

Andreas Harsono of Human Rights Watch for Indonesia agreed that misinformation could be dangerous and deadly. He cited the example of controversy and tension surrounding the re-election bid of former Jakarta governor Basuki Tjahaja Purnama (known as Ahok). He believed the public enmity toward Ahok – fed by the false claim that Ahok had blasphemed Islam – could have escalated: "To some extent, we were lucky the Islamists won (the election). If not, things might have been very ugly."

A digital platform policymaker also saw first-hand how misinformation surrounding the 2019 general election in Indonesia could trigger violence[56] (see case study 5.2 on the next page).

Impacts on election campaigns, political vilification

The potential of misinformation to interfere with election campaigns and political communication was a significant concern among participants in this project. While decades of research findings are mixed on the impact that the media, including social media, can have on voters' decision making, respondents expressed strong views on the subject.

Although Facebook has historically removed posts deemed to be disinformation, it was only relatively recently that it adopted a similar option for misinformation – specifically for cases where there is the potential for harm. A platform expert explained:

> We saw that misinformation around the Rohingya crisis in Myanmar, and the Easter bombing crisis in Sri Lanka really led to people attacking other people. And we didn't have the policy at the time to remove misinformation. And we don't want to just remove content, you know, without a principled policy, so we created that policy, misinformation harm.

At the time of writing, the policy's activation was confined to countries in Asia Pacific, Africa and the Middle East because of their specific requirements and limited digital literacy.

> Misinformation in this region [APAC] is unique because, while obviously there are a lot of really bad things going on in the US related to misinformation, over here when people hear some rumours or a completely false story that has been debunked in many cases, people have lower digital literacy. Immediately, I think it could result in violence.[57]

In Indonesia, the prevalence of political misinformation online tends to be highest around election times, with the risks and problems particularly acute in regional and local contexts. Technology platforms have found that working with trusted community-based organisations can help them detect early signs of trouble or the potential for misinformation campaigns to circulate. However, this can be difficult to achieve in remote and rural areas:

---

56   Interview 9
57   Interview 1

Box 5.2 Ahok Case Study

After giving a speech in September 2016, Jakarta governor Basuki Tjahaja Purnama, known as Ahok, faced allegations of blasphemy against the Qur'an. Ahok, a Christian and ethnic Chinese, was claimed to have stated: "You don't have to vote for me and you probably won't, if you've been misled by those using Surat Al Maidah 51 (Verse 51) of the Qur'an in a misleading way."[58] This verse holds that Muslims should not let Christians or Jews be their *auliya*, often interpreted as "leader."[59]

While initial responses to the speech were muted, footage of the speech was uploaded to YouTube where it became viral. Crucially, the man who uploaded the video was eventually found to have incorrectly transcribed what Ahok had said, making it appear as though his remarks were critical of the Qur'an itself and not his political opponents who were allegedly using the Quranic verse to marginalise non-Muslim leaders.[60]

Alok's comments led to massive and occasionally violent public demonstrations in Jakarta in the following months, where hundreds of thousands of Muslims called for his arrest for insulting Islam.[61] In May 2017, Ahok was sentenced to two years jail and thus could not complete his term as governor. Since his release in 2019 Ahok has declared his career in government over.[62]

In several ways this case encapsulates the political, legal, social and misinformation challenges that exist in Indonesia today. In legal terms, that Ahok was ultimately convicted for blasphemy, despite prosecutors opting to pursue the lesser charge of hate speech, raises doubts about the fairness of the judiciary and one's capacity to access even basic legal protections.[63]

The video supporting his conviction was initially not found to have been doctored by the court. The video was used as the primary evidence against Ahok to convict him of Blasphemy. Later in the year, however, the video uploader was found to have incorrectly transcribed the video of Ahok, misleading the public, and incriminating Ahok. The man was convicted under the ITE law for the act of tampering with the footage.[64] The example illustrates the possibility that manipulated content can be used to prosecute and convict.

While it is difficult to confirm whether Ahok's conviction was politically motivated, as some have argued,[65] the vehemence of public outrage against him is seen to have caused Jokowi, his former gubernatorial running mate, to grow wary of the political threat posed by Islamist groups, leading Jokowi to increasingly quash opposition through the ITE law and further align with mainstream conservative Islamic organisations.[66] As such, a "political mainstreaming" of conservative Islamism has occurred, furthering Indonesia's perceived shift toward illiberalism.[67]

When it comes to sub-regional elections we don't have partners there on the ground to flag misinformation that could potentially turn into real world harm. So these conversations need to be initiated.[68]

Recognising this issue, Facebook has in recent years worked to develop partnerships with community groups in conflict-prone areas to cement its presence in lesser-developed provinces, strengthen its election integrity activities and to overcome the challenges of operating in a country with hundreds of languages, and where artificial intelligence technologies may not pick up early signs of disinformation and misinformation:

We select conflict-prone areas that intersect with regional elections in places like Papua or Ambon Island, which have a history of conflict, and we set up a smaller team of trusted partners and academics that we could potentially work with that could potentially flag to us early on misinformation that could surface. When we go to different parts, the misinformation is very much localised – it's very thick on local context. That would not normally surface for someone that sits in Jakarta.[69]

58 Butt, Simon, "Why is Ahok in prison? A legal analysis of the decision", *Indonesia at Melbourne,* 6 June 2017, https://indonesiaatmelbourne.unimelb.edu.au/why-is-ahok-in-prison-a-legal-analysis-of-the-decision/
59 "Why is Ahok in prison?.
60 Soeriaatmadja, Wahyudi, "Man who uploaded controversial video of ex-Jakarta governor Ahok sentenced to jail", *The Straits Times,* 14 November 2017, https://www.straitstimes.com/asia/se-asia/man-who-uploaded-controversial-ahok-video-sentenced-to-jail
61 Agence France-Presse, "Jakarta protests: Muslims turn out in force against Christian governor Ahok", *The Guardian,* 2 December 2016, https://www.theguardian.com/world/2016/dec/02/jakarta-protests-muslims-against-christian-governor-ahok
62 Bhwana, Petir Garda, "Ahok reflects on never becoming a government official again", *Tempo.co*, 22 October 2019, https://en.tempo.co/read/1262677/ahok-reflects-on-never-becoming-a-government-official-again
63 Butt, Simon, "Why is Ahok in prison? A legal analysis of the decision", *Indonesia at Melbourne,* 6 June 2017.
64 "Man who uploaded controversial video of ex-Jakarta governor Ahok sentenced to jail".
65 Butt, Simon, "Why is Ahok in prison?"
66 Warburton, Eve and Aspinall, Edward, "Explaining Indonesia's democratic regression: Structure, agency and popular opinion", *Contemporary Southeast Asia* 41(2), 2019, p. 271.
67 Ibid., p. 260.
68 Interview 9
69 Interview 9

A particular concern among interviewees was the tendency for politically-motivated misinformation to be weaponised against individual opposition candidates and their supporters, particularly in Indonesia.

> They are attacking the candidate, not attacking the program… even attacking the belief of the people who support the candidate, like saying that this person is not Islam enough to be our leader or, as in the Ahok case in 2017, this person is 'kafir'. So that means if you are like him, you are not following the rules of Islam… The use of political identity as a way of propaganda is something that's more effectively used than criticising the political program.[70]

Damar Juniarto observed this phenomenon in the actions of the "cyber armies" and "militias" who engaged in trolling and "doxing" (posting private information with malicious intent) of political opponents.

> There's so many people being targeted. So we are working together with other organisations, we cannot do this by ourselves. That's why we are forming our national coalition against persecution to protect the people and ask the police to investigate and to (find the) organisations behind the attacks.

Political misinformation during election campaigns is frequently shared through informal and personal networks such as WhatsApp – the Facebook-owned platform that is very popular among Indonesians, and particularly prone to misuse. "In the context of the presidential election in Indonesia last year, the friendship groups (on WhatsApp) became a key source of political hoaxes," said one researcher.[71]

Tackling misinformation shared on WhatsApp is difficult because of end-to-end encryption of the shared content. Facebook has tried to overcome the problem by limiting the number of times individuals can share the same information. But this has had the unintended consequence of disadvantaging small business owners who have used WhatsApp to promote their goods and services. As a Facebook expert explained:

> We want to support the Indonesian Government to address misinformation. But one community that shouted the loudest when we actually made those adjustments are the small and medium businesses that thrive on WhatsApp. You can win in one area and lose in the other.[72]

In Singapore, the prevalence of alleged online misinformation during election campaigns has raised different issues. Some observers have accused the Singapore Government of overreach in its attempts to combat misinformation in the lead-up to national elections in July 2020. While acknowledging that misinformation relating to elections is problematic, one academic said the Government was conflicted in its self-appointed role of overseeing and regulating election-related misinformation:

> There should be an independent group set up to evaluate false information in that election period, and then it should be disbanded. And that's it.[73]

Similarly, for other forms of misinformation with the potential to cause harm (such as COVID-19 related false content), he recommended following the model spawned by Britain's Leveson inquiry – appointing a committee of experts from different sectors (such as medicine and academia) at arm's length from government to regulate the online space, and with the authority to order the removal of misinformation after it has been assessed.

Misleading the public

It is self-evident that online misinformation can mislead the public. But how much harm can it cause, and how effective are measures to mitigate it? As Pew Research Centre studies have confirmed, misinformation can make it difficult for citizens to determine real news from false information, affecting their capacity to make informed choices, particularly at the ballot box.[74]

But as explained in the example below, correcting even harmless fake news can create confusion by reiterating the false information. This is sometimes called the "backfire effect".

Box 5.3 Singapore: "plastic rice"

In Singapore there is kind of a famous fake news, and it happens every now and then, of plastic rice, and the news will go around that, "hey, this rice is plastic, looks like real rice but plastic. It's being sold in the supermarket. Don't buy the rice from the supermarket because they are selling this plastic rice." So if you look at that, then the harm is not so serious. But, the thing about trying to correct information is that you have to tell people what the false information was. And I think the research in this space has shown that when you do that, some people believe the false information.[75]

Racial and religious vilification

The case of former Jakarta governor Basuki Tjahaja Purnama (Ahok) provides a high-profile example of how online misinformation can be used to vilify individuals and groups on racial and religious grounds, sometimes for political purposes. Ahok's Christian faith made him a target of hostile online misinformation during his last election campaign – and Andreas Harsono believes this was central to his defeat. More broadly, Septiaji Eko Nugroho says Indonesia's ethnic and religious diversity, and related polarisation in political affiliations, is a significant contributing factor to the proliferation of online misinformation.

---

70   Author interview with Damar Juniarto
71   Interview 7
72   Interview 9
73   Interview 3
74   Michael Barthel, Amy Mitchell and Jesse Holcomb. *Many Americans believe Fake News is sowing confusion.* (*Pew Research Centre,* 15 December 2016. https://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/
75   Interview 3

Targets: Civil activists, women and minority groups

Community-based activists and marginalised groups – including women and people who identify as LGBTI – have been frequent targets for online attacks in Indonesia and Singapore. Damar Juniarto identified a number of "high risk groups" in Indonesia for online misinformation with the potential for harm. Most prominent among these were:

- Journalists
- Human rights defenders
- Anti-corruption activists
- Ethnic group defenders
- Women
- LGBTI community members.

SAFEnet recorded almost 40 reports of online attacks on members of these groups over a recent 12-month period. Juniarto said it was critical for civic groups to have direct lines of communication to digital platforms like Twitter, Facebook and YouTube to report online abuses, and to find timely ways to strengthen and protect targeted groups.

> Direct reporting helps a lot. It is also very important if you know how things work inside the company. They have a long, long process to deal with misinformation, but they are willing to help to escalate our report.

Online hoaxes in Indonesia are frequently not just political, but disinformation and misinformation often is targeted against women. According to one expert, sexual harassment of females is prevalent on WhatsApp.[76] To mitigate gender-based online harm, academic researchers have been working with women across four cities to identify and try to improve their media and digital literacy. The program aimed to train women to teach other women about how to recognise and deal with online misinformation, as well as hate speech and disinformation. Due to the pandemic and postponement of local elections in 2020, the face-to-face "train the trainer" sessions were conducted online: "We choose women who are already active, not only in the WhatsApp groups, but also active in their communities. So they become an engine of change," the researcher said.

Country-specific problems

Despite their geographic proximity, Indonesia and Singapore are vastly different countries in so many ways – including in how online misinformation manifests online. Journalist Kirsten Han observed that while "big level disinformation campaigns" were common in Indonesia, the bigger problem in Singapore concerned freedom of political expression.

In Singapore, the key demographic characteristic in the context of online misinformation is not religion, but the nation's relatively large migrant population. This has manifested most recently in online campaigns that exaggerated the role of migrants in COVID-19 outbreaks.[78]

Geographic, cultural and religious diversity

With its sprawling archipelago spread across five time zones, and its enormous cultural, ethnic, linguistic and religious diversity, Indonesia is an uncommonly challenging environment for technology platforms and governments seeking to deal with online misinformation.

Islam, the dominant religion, also has an important place in the nation's wider cultural, social and legal fabric. This extends to the Government's upholding of blasphemy laws and other Islamic tenets such as *kafir,* which effectively impose limitations on some types of online content and freedom of expression. As one Indonesian academic explained, this creates inevitable

tensions between local and international community standards about acceptable content on issues such as pornography.

> There is a tension between government and the international social media platforms because social media has their standards or community guidelines, but it's produced for international needs. In some cases Indonesians have specific needs that have to be contextualised with the local conditions. In Indonesia the definition of pornography is very different.[77]

Democratic deficits: Restrictions on freedom of speech

Identification and management of undesirable content are key areas of tension between government authorities and social media companies. Demands by the Indonesian Government for content removal have sometimes created friction with social media companies, which have a range of alternative options for dealing with misinformation, depending on the perceived level of potential harm.[79]

In some situations – often involving political tension and/or threats of violence – the Indonesian Government has acted to slow down or selectively shut down the internet on the grounds that certain content may "ruin the general

---

76   Interview 7
77   Ibid
78   Interview 3
79   Interview 7

purpose of the society."[80] An example of this was when the Government blocked the internet in Papua in 2019 following days of protests against Indonesian rule of the province.[81]

SAFEnet's Damar Juniarto said his organisation closely watched governments in Southeast Asia that sought to interfere with citizens' internet access, or to use misinformation as a reason to shut down or slow down the internet. However, he said SAFEnet's vision for freedom of expression online to improve democratic participation needed to be balanced against the need for people to feel safe online. To help achieve this, SAFEnet had worked with Facebook and Google to monitor and report hate speech, with a particular focus on gender-based harassment and violence.

Andreas Harsono was also concerned about curbs on freedom of expression in Indonesia. "We are seeing the rise of Islamism in Indonesia, and we are also seeing the re-emergence of military and police roles in civilian life." In this environment, religious and political issues were very sensitive, said Septiaji Eko Nugroho. One academic noted the prevalence of hate speech before, during and after elections.[82]

Media and digital literacy

Media training and teaching digital literacy are considered important tools to help mitigate the harm caused by misinformation. However, given low levels of general literacy in Indonesia, it is difficult to increase media literacy to help citizens detect fake news, said Septiaji Eko Nugroho, Chair of fact-checking group MAFINDO.

Singapore, by contrast, has relatively high rates of both general and digital literacy, though less so among older citizens, said journalist Kirsten Han:

Younger Singaporeans are much better at this because they are digital natives and they grew up with this. They seem to ask more questions about what they're reading, (which) the older Singaporeans don't do.

Han noted, however, that due to government controls over the media, high levels of general literacy did not necessarily equate with media literacy. "Local mainstream media is seen as controlled by the Government," she said. This limited the media's "fourth estate" function of holding the Government to account. Indeed, Han said that since Prime Minister Lee Kuan Yew's time (1959-1990) there was an explicit rejection of the idea of the media being a "fourth estate", because he said that an unelected media can't have that sort of power over the government.

---

80   Interview 7
81   Helen Davidson, "Indonesia arrests dozens of West Papuans over claim flag was thrown in sewer," *The Gaurdian,* August 18, 2019, https://www.theguardian.com/world/2019/aug/18/indonesia-arrests-dozens-of-west-papuans-over-claim-flag-was-thrown-in-sewer
82   Interview 7

She said it was also "hard to teach media literacy when the country has only one main newspaper. And you're supposed to take that as truth."[83]

Government employees are "beholden" to the Official Secrets Act, which precludes them from sharing information without authorisation, Han said. Hence, the tools needed to establish the truth were often held exclusively by the state, she said.[84]

Internet use and preferences

In Indonesia, somewhere between 50 and 60 per cent of citizens have internet access, with about 95 per cent of the connected population having Facebook accounts.[85] However, younger and urban Indonesians tend to prefer Instagram over Facebook. Other popular platforms include WhatsApp, Twitter, Netflix, YouTube and TikTok. COVID-19 prompted an increase of about 40 per cent in internet and social media use in Indonesia, according to one academic.[86] And with more use comes more misinformation, said Septiaji Eko Nugroho. "We see misinformation on Instagram and also on TikTok."

Apart from issues with encryption, some unique ways in which private messaging platforms are used in Indonesia make it more difficult to control, according

to Andreas Harsono. Indonesian users tended to have more than one account, and WhatsApp groups could be as large as 250 people,[87] presenting additional challenges for those trying to deal with online misinformation, Nugroho said.

> The difficulty for us is that it is like a private communication. So we don't really exactly understand the numbers. For Facebook, most of the contents are in a public space. So Facebook, Twitter and Instagram, I think are much easier for us to get some knowledge about their use.[88]

Similar platform usage trends were observed in Singapore. One academic said about 40 per cent of recent survey respondents said that they used WhatsApp to get news, just short of the 50 per cent who relied on Facebook.[89] While Chinese-speaking Singaporeans favoured WeChat and Weibo,[90] younger Singaporeans were more drawn to Instagram, Twitter and Telegram.

According to Kirsten Han, it is said (in jest) that you get more politics on Facebook than in Singapore's

Parliament, because even the politicians rely on Facebook:

> It's quite common to see a government agency put their press statement on Facebook before they even put it on their website. Because that's how it gets seen. And that's how it gets shared, and ministers will openly rebut people on Facebook. The local press pick it up and just quote him off his Facebook post rather than in a press conference or interview. And so everyone uses Facebook. It is an important way to kind of reach people and see what they are talking about.

Han said Telegram was a favoured platform for political mobilisation, given government restrictions on public assemblies and other offline political activities.

83   Author interview with Kirsten Han
84   Kirsten Han, "WTC Long Read: A mother's concerns in a time of POFMA," *We The Citizens,* 9 November 2020, https://wethecitizens.substack.com/p/wtc-long-read-a-mothers-concerns
85   Interview 1
86   Interview 1
87   Interview 1
88   Author interview with Septiaji Eko Nugroho, Chairman of MAFINDO, 26 August 2020
89   Interview 11
90   Interview 11

Conclusion

The definition of misinformation is contested. While it is often understood in opposition to disinformation, this distinction is not always clear. Some have posited a simple distinction – misinformation being a falsehood spread with innocent intent, and disinformation involving deliberate ill-intent. Yet social media platforms say it is impossible to divine the intent of the person posting content. So, when managing and categorising problematic content, their focus tends to be more on its factual veracity, and its relative potential to cause harm.

Governments in Indonesia and Singapore, on the other hand, while also strongly focused on potential harm (particularly in relation to issues like COVID-19) have been widely accused of applying self-serving political criteria when defining and identifying alleged online misinformation. This has put them in conflict with major platforms and civil society actors over what is and is not misinformation, and what should and should not be allowed online, particularly in the lead-up to political elections.

Other ambiguities and complications abound. For example, as the COVID-19 epidemic has revealed, misinformation about medical treatments can be spread without the intention to cause harm – meeting one definition of misinformation – but false cures may inflict serious physical harm. Likewise, true information can be harmful and used for political purposes, such as spreading innuendo and gossip.

These are but a few examples of the lack of clarity and consensus on fundamental defining aspects of online misinformation. The ambiguity matters because it signifies a lack of agreement and clarity about how best to *address* the problem. This can result in fractured or "siloed" approaches by governments and digital platforms to misinformation and disinformation. While governments have tended towards overreach (sometimes criminalising citizens' inadvertent breaches of laws, and suppressing freedom of speech and dissent), platforms may have historically underestimated the harm of online misinformation and not addressed falsehoods or removed harmful content quickly enough.

Although Facebook and other platforms have refined their misinformation strategies, some changes have brought additional complications. For example,

while removing fake accounts might seem desirable, it can have the questionable effect of suppressing dissident voices in countries under non-democratic rule. Fact checking to identify false content, while objectively desirable, is not only costly and time consuming, but needs to be better customised to deal with false content on encrypted sites such as WhatsApp.

Notwithstanding the lack of consensus on how to define, measure and mitigate misinformation online, clear unanimity exists about the urgent need to curb it in both online and offline spheres to improve the quality of information vital to the health and prosperity of communities and democracies everywhere.

Tackling misinformation online and its challenges

Introduction

This chapter explores recent attempts by digital platforms and lawmakers in Singapore and Indonesia to tackle the problem of misinformation online. It considers the various issues – technological, political, demographic, geographic and legal – that surround this 21st century problem, and focuses on the effects, intended or otherwise, that measures taken to mitigate misinformation have had on civic society, democracy and the technology platforms.

We identified widespread fears that attempts to date by lawmakers to combat misinformation also hold the potential to undermine media freedom, free speech and democracy in both countries, and that governments and digital platforms face ongoing challenges in navigating this complex regulatory space. The chapter is divided into two sections. The first outlines what social media companies and governments are doing to manage online misinformation, according to interviewees. The second section examines ongoing challenges that both platforms and governments face tackling this endemic problem. We specifically examine the stated problems with the laws that deal with misinformation, including how these laws are perceived to be misused for purposes other than reducing online misinformation.

Section 1
Measures to tackle misinformation

Digital platform measures to deal with misinformation

Social media platforms have introduced a variety of measures in recent years to try to tackle online misinformation. In interviews for this project, digital platform experts involved in addressing misinformation detailed various approaches ranging from top-down to community-led, technical and social, restrictive and corrective, and human and non-human strategies. For Facebook, these community standards revolve around the areas of "Authenticity", ensuring content on Facebook is authentic; "Safety", ensuring users can participate in a safe online environment free of threats and intimidation; "Privacy", the platform's commitment to protecting personal information and privacy; and "Dignity".[1]

There are at least 26 areas of concern that fit beneath these broad objectives of which false news is one and the issue most closely aligned with misinformation – the subject of this study. Under this section heading, Facebook outlines its three-pronged strategy to: "Remove" accounts that violate its policies; "Reduce" inauthentic content and the spread of false news, and to "Inform" or help online users make informed decisions about "what to read, trust and share."[2] To paraphrase, Facebook defines "inauthentic" as the use of its platforms to mislead others about the identity, purpose, popularity or origin of their online presence. It includes users who may engage in coordinated activities and who do not comply with the platforms'

Community Standards (see below), or who engage (or claim to participate) in behaviours involving fake accounts or foreign or government interference.[3]

The measures discussed in more detail below, in alphabetical order, fit within Facebook's three-pronged approach and were the most visible or known measures that digital platforms were using in Singapore and Indonesia to tackle misinformation as identified by the expert respondents.

Community standards

"Community standards" adopted by digital platforms, and agreed to by users, have been a primary resource to help platforms combat misinformation. By declaring types of content and behaviours that are admissible on platforms, community standards help people determine what constitutes misinformation, and how to distinguish it from illegal information and material that is simply contrary to the agenda of individuals or groups that oppose it.[4] Facebook works with community service organisations (CSO) to convey its community standards: "We continue to train CSOs on how we look at our community standards and how our community standards look at misinformation," but conceded that more "outreach" was needed, "especially for Indonesia," to ensure the public and government understand how misinformation is regarded by the organisation.[5]

However, Kirsten Han, a journalist based in Singapore, said community standards on platforms sometimes lacked clarity. "When you get taken down [from using

a platform] for violating community standards, no one actually knows why," she said. "So, I think the platforms should be more transparent and work with local civil society more about these policies."[6]

Artificial intelligence

Artificial intelligence (AI) is considered an indispensable tool in platforms' efforts to detect misleading content that has the potential to be both harmful (such as false information about COVID-19) and to be disseminated rapidly and widely. AI is valued primarily for its ability to identify misinformation quickly. According to one digital platform expert, for any tool to be able to match the virality of misinformation, it "needs to be" AI.[7] While effective AI systems are already in use[8] there was still a "need to be a lot faster" in tracking and tackling misinformation.[9]

The chairman and founder of the Indonesian civil society group tackling online misinformation MAFINDO, Septiaji Eko Nugroho, said a limitation of AI was local context and culture:

> Sometimes what we see is the machine doesn't really know the local context, especially for Indonesia where we have more than 700 languages, local languages, and some word meanings could be very different. A word could be very polite in one area, but very insulting in another.[10]

1 Facebook, "Community Standards," *Facebook*, 2020, https://www.facebook.com/communitystandards/
2 Facebook, "Hard Questions: What's Facebook's Strategy for Stopping False News," *Facebook,* 23 May 2020, https://about.fb.com/news/2018/05/hard-questions-false-news/
3 Facebook, "Inauthentic Behaviour," *Facebook,* 2020, https://m.facebook.com/communitystandards/inauthentic_behavior/
4 Interview 9, interview with Andrea Carson, 8 September 2020; Interview 4, interviewed with Andrea Carson, 7 August 2020
5 Interview 9
6 Interview with Kirsten Han, interview with Andrea Carson, 25 August 2020
7 Interview 1, interview with Andrea Carson, 7 August 2020
8 Interview 9
9 Interview 1
10 Author interview with Septiaji Eko Nugroho, Chairman of MAFINDO, 26 August 2020

For this reason, human analysis of misinformation and inauthentic content remains essential, argued an Indonesia academic.[11]

Content removal, platform bans and feature limits

Academics and the technology platforms cited various tools that can be used to tackle online misinformation. These include the removal of content,[12] fact checks (along with statements about false claims) and, in the most extreme cases, banning users who have repeatedly spread misinformation from a platform.[13] However, only misinformation that risked causing "real world harm" tended to be removed quickly.[14] For example, in reference to recent riots in Indonesia, one platform expert said:

> The basis of what happened with those riots was actually misinformation… that led to real world harm. That's why we could actually instantly remove the content… We don't (usually) remove on the go… we would normally consult with our trusted partners on the ground.[15]

Misinformation relating to serious public health issues such as COVID-19 and vaccinations tends to be deemed harmful, as does racial and religious hate speech.[16] One academic said that while platforms preferred less severe measures than content removal, the Government sometimes saw removal as "the best solution."[17] A digital platform expert said platforms reserved user bans for "the worst actors."[18]

Tension between local norms and customs and broader considerations of human rights can also cause conflict between platforms and governments about what is misinformation and how to respond to it. A digital platform expert said:

> It's a difficult conversation to have with the Government… they get a lot of pressure [about the platform] not adhering to the local norms and traditions.[19]

Editor-in-Chief of *Tempo* magazine, Wahyu Dhyatmika, said it was not uncommon for the Indonesian Government to demand hoaxes be taken down from the platform or otherwise threaten measures such as revoking their licence to operate in Indonesia or legal action. This made the issue of "take downs" and user bans a complex one. He explained:

> The tech platforms also get pushback from civil society if Government asked them to take down content that's not necessarily misinformation but criticism towards the government. So they are really working on a thin line if they want to keep being an open platform for all voices. But, I suppose, they need to also obey the law and follow the government's line. So it's a very complex issue.[20]

Added to this complexity is the mixed quality of reports of misinformation sent to platforms by the Government. According to one digital platform expert it was hard to act on misinformation when the reporting is poor or the misinformation not well defined.[21] Another issue is disagreements between platforms and governments over what constitutes misinformation.[22] A possible solution to this was more independent fact checking.[23]

Platforms can also restrict features that have been used to spread information, or just "turn off" certain functions to

prevent people abusing these features.[24] But such measures can have unintended consequences for other users and uses, such as small business marketing (see Chapter 5 for more details regarding WhatsApp forwarding features).[25]

Digital literacy

Several interviewees identified teaching digital literacy to the general community as essential to combating misinformation in Singapore and Indonesia. One platform expert said:

> For a country to be successful in clamping down on misinformation, they need to put digital literacy and ways to recognise misinformation in the curriculum. I think the answer is in people's awareness… it's like wearing a seatbelt so that everyone in the country will grow up knowing that… there's a risk that you will find misinformation and be misled… if you use the internet.[26]

Recent campaigns aimed at educating Indonesian citizens on how to detect online misinformation were "very successful," said another platform expert.[27] Other measures included publicity campaigns to "teach people to think critically when they use the internet before they share anything," and "train the trainer" programs, where the platform provides training to organisations, which in turn train other people in their communities.[28] Another platform policy expert said the key was to teach people that not everything they see online is authentic. One way to do this was a general public education campaign in Indonesia:

11   Interview 7, interview with Andrea Carson, 19 August 2020
12   Interview 1; Interview 7; Interview 9
13   Interview 4, interview with Andrea Carson, 7 August 2020
14   Interview 9
15   Interview 9
16   Interview 1
17   Interview 7
18   Interview 4
19   Interview 9
20   Author interview with Wahyu Dhyatmika, Editor-in-Chief of *Tempo magazine,* 24 August 2020
21   Interview 9
22   Interview 9
23   Interview 9
24   Interview 4
25   Interview 9
26   Interview 1
27   Interview 9
28   Interview 1

We tried to educate the public on how they need to look at misinformation. We built partnerships with Siberkreasi, a consortium of CSOs, academics and private sector that care about digital literacy, and delivered programs such as "Asah Digital", aimed to educate students, parents and teachers to better identify misinformation using critical thinking and empathy. In the lead up to election we also ran campaigns on our platforms to tackle misinformation and had stickers around the city buses, all over Jakarta. And I hope [we] can continue these public education campaigns.[29]

Anti-misinformation activist Septiaji Eko Nugroho endorsed a "multi-pronged approach" to digital literacy involving not just platforms, but governmental and community organisations involved in training the public.[30] He said MAFINDO collaborated with more than 100 organisations including civil society groups and government agencies to improve the public's digital literacy through various targeted campaigns.

Fact checking

Technology platforms have initiated extensive third-party fact checking operations, which in Indonesia include the Indonesian civil society organisation (CSO) and fact-checking outlet, MAFINDO, and media organisations such as *Tempo*.[31] In some cases, the platforms use other external experts, such as the World Health Organisation and other health experts for consultations regarding harmful COVID-19 misinformation.

Fact checking in Indonesia is dynamic, with independent media and CSOs collaborating with and receiving support from technology platforms (seven of which are signatories to the International Fact-Checking Network (IFCN) – a unit of the Poynter Institute dedicated to bringing together fact checkers worldwide), and government agencies.[32] Platforms have also performed fact checking in Singapore, with a particular focus on election campaigns.[33]

One advantage of fact checking compared to other anti-misinformation measures is that it allows platforms to correct false content while respecting users' rights to publication. As one platform expert said, a correction allows the continued right to share content while "everyone has the right to know also that it's been fact checked as false."[34]

However, fact checking is resource-intensive and expensive. Wahyu Dhyatmika, editor of Indonesian media company *Tempo*, described the challenges:

> Reporters can do five to seven news items per day, and our editors can get through 15 articles per day. But fact checkers sometimes only produce one fact checked article per day... it's very resource intensive.[35]

Another digital platform expert, noting the large volumes of misinformation online, said of third-party fact checkers: "They need to be very strategic in the type of misinformation that they want to debunk, because it does take a lot of work."[36]

Others said fact checking, though valuable, needed to be used in conjunction with other measures. Singapore-based journalist Kirsten Han said fact checking alone would not stamp out misinformation. But she believed more fact checking would help to shift accepted norms and remind people that they need to look out for misinformation.[37] In this way, fact checking may also serve as an educational tool for social media users and should be used in conjunction with digital literacy education.

False content warning labels

Platforms have also taken to using warning labels to alert users to content deemed to be false or unreliable.[38] One social media expert said labelling of misinformation and the "promotion" of correct information had been particularly focused on serious public health issues such as COVID-19 and vaccination.[39] With COVID-19, algorithms are used to highlight and prioritise credible information from bodies like the World Health Organisation and the Government.

Investing in quality journalism

Platform initiatives to support journalism communities such as Facebook's Journalism Project and Google News Initiative and Twitter grants to media outlets were welcomed by respondents who thought the platforms had a role to play in supporting quality news online.

One academic said: "These projects where companies invest in helping journalism to survive are the kinds of models that should be replicated in this misinformation arena."[40]

Others valued the contributions and commitment platform companies had made to third-party fact checking. These outsourced roles also provided another stream of revenue for media outlets in difficult times for the business model of legacy media.

Public reporting measures and proof of accounts

Asking social media users to provide proof of identification aims to ensure transparency and accountability, said one digital platform expert.[41]

Providing features and avenues for users to report misinformation to platform regulators can also help with the detection and management of online misinformation.[42] This can be particularly useful when dealing with private messaging applications such as WhatsApp, over which content regulation is made difficult by privacy and encryption controls.

29   Interview 9
30   Author interview with Septiaji Eko Nugroho, Author interview with Andrea Carson, 26 August 2020
31   Interview 1
32   Author interview with Septiaji Eko Nugroho
33   Interview 11, interview with Andrea Carson, 20 August 2020
34   Interview 4
35   Author interview with Wahyu Dhyatmika
36   Interview 9
37   Author interview with Kirsten Han
38   Interview 1
39   Interview 1
40   Interview 11
41   Interview 4
42   Interview 1

Relationships between technology platforms

Technology platforms acknowledge and embrace their central role in combatting online misinformation. However, one social media expert expressed a desire for more transparency by platforms about their interventions and policies.[43] And while there was general agreement on the need for co-operation between platforms, there were mixed views on the extent to which it occurs.

One platform expert said:

> If we investigated and found certain bad actors that are pushing propaganda across our platform, we would share some of what we found with our partners, so that they can then further their own investigation and try to take down the network on their site as well.[44]

Community organisations strongly support co-operation and information sharing between platforms. Damar Juniarto of SAFEnet recalled how he had shared a model of reporting misinformation introduced by one platform with other platforms. "It helps a lot," he said.[45]

Trusted partners and collaboration

Digital platform experts stressed the importance of collaboration with community organisations, local media, academics and governments to tackle misinformation. One said they would normally consult with "trusted partners" to validate what type of information is worth removing immediately: "We don't really want to be the arbiter of truth."[46]

Trusted partners could reduce platforms' burden of responsibility in the task of deciding which content to manage through fact checking activities.[47] One platform interviewee said it was important that fact checking partners operated independently: "Ultimately it's up to them… to validate whether that specific information is true or not."[48]

Another digital platform expert stressed the importance of collaboration between platforms:

> I think collaboration and trust needs to be developed, and there needs to be proper information sharing across platforms because this information is not just on any (one) network.[49]

Partner organisations also advocated a proactive role for platforms. The Indonesia-based head of the Southeast Asia Freedom of Expression Network (SAFEnet) Damar Juniarto said civil society groups could not tackle the problem of misinformation alone and that they had "asked the social media platforms to take responsibility as well."[50] Juniarto highlighted the potential for civil society organisations (CSOs) and platforms to work together to hold the government accountable for perceived regulatory overreach that could threaten freedom of expression and political discourse. This highlights how the agendas of platforms and CSOs (which are otherwise called non-government organisations, or NGOs, in Australia and some other countries) may intersect.

In Indonesia, social media platforms provide resources to media organisations for measures such as fact checking operations.[51] An example of this is the fact checking coalition *CekFakta,* comprising 22 media companies, numerous CSOs such as MAFINDO, and is financially supported by the Google News Initiative, anti-misinformation NGOs Internews and First Draft. The coalition aims to create almost 100 "master trainers" among journalists, and a curriculum to train another 4000 fact checkers, said MAFINDO head Septiaji Eko Nugroho.

Tempo, one of the media companies involved in *CekFakta,* through a separate partnership, had also established a team of health experts to help tackle misinformation related to COVID-19, according to editor-in-chief Wahyu Dhyatmika.

Despite these positives, one digital platform expert lamented the lack of consultation between the Indonesian Government and CSOs, compared to the "quite regular" consultation by the Ministry of Communications and Informatics with platforms.

> To ensure that the conversation continues to develop in the right direction, maybe we should start holding public consultation… with the CSO communities as well.[52]

> The Indonesian Government has also been accused of asking platforms to remove content simply because they "don't like" it, said Damar Juniarto.[53]

The major platform companies also fund academic research to further knowledge about the nature of the problem and ways to mitigate it. Global funding rounds call for academics to submit proposals on particular themes. The companies also commission academics and research units for specific projects, including this report.

43   Interview 1
44   Interview 4
45   Author interview with Damar Juniarto, SAFEnet, Southeast Asia Freedom of Expression, Executive Director, 8 September 2020
46   Interview 9
47   Interview 9
48   Interview 9
49   Interview 4
50   Author interview with Damar Juniarto
51   Author interview with Wahyu Dhyatmika, Author interview with Andrea Carson, 24 August 2020.
52   Interview 9
53   Author interview with Damar Juniarto, Author interview with Andrea Carson, 31 August 2020.

Government measures to deal with misinformation

The governments of Indonesia and Singapore have both enacted laws specifically to combat misinformation online (see chapters 1 and 2 for more details). Pre-existing laws are also used to tackle the problem. While there is broad agreement about the need for government regulation of harmful online content, critics in both countries question the effectiveness of the existing laws and the ways in which governments have applied them.

Indonesia

There are several laws and proposed laws that attempt to deal with misinformation and disinformation in Indonesia. Below are the laws that interviewees referenced in their responses.

Revised Criminal Code

Proposed revisions to Indonesia's near-century old Criminal Code – aimed in part at curbing the spread of online misinformation – have prompted widespread public outcry, including street protests in September 2019 (see chapter 1). Human rights activist Andreas Harsono said the revisions would lead to an expansion of government powers, and a "much more draconian" and discriminatory law.[54] Plans for a vote in Parliament on the draft Bill have been stalled at the time of writing following the protests amid pressure on the Government to resubmit a revised plan. Harsono was particularly concerned about what a revision would mean for religiosity and politics in Indonesia:

> The blasphemy law in the existing criminal code has only one article. In the draft law, the draft penal code, it will be expanded into six articles. You know, blasphemy is nonsense, that it is going to be expanded, slander and libel will also be expanded with longer jail terms. That's why we

are worried in the current climate. If Indonesia is to revise the Criminal Code, what is the current situation? We are already seeing the rise of Islamism in Indonesia. We are also seeing the re-emergence of military and police role in civilian life.[55]

Within the existing Criminal Code is an article pertaining to treason with the provision to jail alleged offenders for up to 20 years.[56] Harsono said the article is used unjustly as a tool of the state to arrest and jail Papuan separatists. Amnesty International has recorded at least 77 prisoners of conscience detained on treason charges in Papua and Indonesia, including at least 20 people under city arrest.[57]

> Papuans want to be independent of Indonesia or ethnic Moluccan who also want to be independent from Indonesia. They were sentenced between three and 20 years in prison for raising their flags. Now this draconian Criminal Code article is extended into the internet law (ITE), because, of course, in 1918 the internet did not exist. In 1918 it was mostly print and radio broadcasts, with broadcast TV also covered under broadcast.[58]

Information and Electronic Transactions Law

Indonesia's Information and Electronic Transactions Law (ITE) was introduced in 2008 and revised in 2016. Harsono said the law is "basically an extension" of the Criminal Code as it applies to hate speech, slander, defamation and blasphemy to include online material. "Both of them are pretty ugly laws," he said.[59]

SAFEnet's Damar Juniarto said the ITE law is "misused" during election campaigns, especially to undermine rival political candidates by reporting them to police for allegedly breaching the law. This was hurting freedom of expression and democratic participation, he argued: "The misuse of internet laws is always increasing during the election time… freedom of expression in Indonesia is decreasing."

A digital platform policy expert said the ITE law was problematic because:

> It contains a vague article that says something that could disrupt the harmony or stability in the community is illegal essentially. And so the Government has used that law to prosecute people for you know, all kinds of things that they post on social media.[60]

Editor-in-Chief of *Tempo* magazine, Wahyu Dhyatmika, said the main problem with the ITE law was a lack of transparency about how it is used and that it tended to be used in favour of government officials, not civil society. He argued:

> There's problem with transparency [of ITE] and also about the effectiveness of its legal methods to deal with misinformation. If it's misinformation – the distributors may not knowingly distribute contents with regards to the impact or with its accuracy – then using laws just creates polarisation, it creates other problems in the society. It doesn't really deal with the core issue that we are dealing with, which is the low rate of media literacy. And, you know, low trust in the government.[61]

54   Author interview with Andreas Harsono, Human Rights activist and Researcher at Amnesty International Indonesia, 20 August 2020
55   Ibid
56   Ibid
57   Epa, K. "Rights groups demand end to Indonesian treason laws," UCAnews. 2020, 13 March, https://www.ucanews.com/news/rights-groups-demand-end-to-indonesian-treason-laws/87448#
58   Author interview with Andreas Harsono
59   Ibid
60   Interview 1
61   Author interview with Wahyu Dhyatmika

Further, defamation – alongside libel, slander and blasphemy – is also covered by the Criminal Code and ITE law.[62] As part of the general attack against online content deemed harmful, lawmakers and enforcers in Indonesia have also sought to limit and criminalise pornography.

Personal Data Protection (PDP) Draft Bill

SAFEnet is also concerned about a Cybersecurity Draft Bill before the Indonesian House of Representatives at the time of writing that ostensibly aims to enforce data protection and to punish data breaches with fines up to $A20million for corporations and seven years jail for individuals. It is said to be modelled on aspects of the General Data Protection Regulation 2016/679 (GDPR) issued by the European Parliament and Council of the European Union. However, Juniarto said the proposed laws (known as RUU KKS) contain provisions that would enable the government to suppress the spread of information by cutting data connections. It also threatened to sanction public opinion if deemed a cyber threat, without any judicial oversight. "I'm a little bit worried because they [the Indonesian Government] are not involving enough stakeholders to think together about this law. It is one-sided for the sake of the Government… not for the people," Juniarto said.

The Indonesian Government's Communications and Informatics (KOMINFO) Ministry also counters alleged hoaxes and misinformation on its website. KOMINFO issued a statement on 4 November 2019 that a new regulation GR71 would fill a regulatory vacuum until the PDP was passed.[63] This regulation provides measures to prevent the circulation and use of prohibited content including what the government deems as "negative content", among other uses. This includes online information that may "cause public disquiet and disturb public order."[64]

A digital platform expert said this proposed regulation on electronic system operators (ESO)[65] if passed will force platforms to meet short turnarounds to remove content if deemed inappropriate by the government.

> The Government has taken the most conservative approach which is that if it's misinformation that could potentially be a threat to the country, then it should be removed. I think what has been missing from this discussion, with regards to content moderation regulation, has been our friends from the CSO community. Not only are they the ones who will be impacted, CSOs will be able to provide a substantial input to the draft on trends and common issues.[66]

Singapore

The law that respondents found most problematic in Singapore was the new 2019 law relating to misinformation and online falsehoods, best known as POFMA.

Protection from Online Falsehoods and Manipulation Act

The Protection from Online Falsehoods and Manipulation Act (POFMA) has been the subject of vocal opposition from many Singaporeans since it took effect in September 2019. Critics claim the law is ambiguous, has inadequate appeal mechanisms and can be used arbitrarily by the government to censor or silence its opponents.

Observers say POFMA was enacted in response to platforms' unwillingness to remove some types of alleged misinformation at the request of the Government.[67] The Government had previously been unable to convince social media platforms to remove content they considered unharmful, such as opposition criticism.[68]

One academic criticised the Singapore Government's treatment of POFMA as "a panacea" to tackle misinformation online.[69] While there was "a place for legislation and regulation," he argued "it should be a multi-pronged approach."[70] However, he conceded that POFMA has been useful in mitigating misinformation relating to COVID-19 and hate speech.

Freelance journalist Kirsten Han said POFMA had increased the vulnerability of freelance journalists. She said that getting "POFMA-ed" or getting sued for defamation could disrupt the work of freelancers like her who lacked the resources to fight charges. "I wouldn't have the benefit of legal counsel that a company will pay for," she said.[71] Her situation contrasted with journalists in mainstream Singapore media outlets, which were mostly government-aligned and rarely sued for defamation.

Other Singaporean laws used against misinformation

Other laws used in Singapore in the name of fighting misinformation include sedition laws designed to prevent citizens or others displaying or enacting hatred, contempt or disaffection against the Government. Under this old 1938 law (updated in 1985), the intention of the offender is irrelevant. It has been used in the past to criminalise actions that were said to have a "seditious tendency" and may attract fines or a jail term of up to three years. One critic said it added "another layer of problems in the implementation of regulations" to deal with misinformation.[72]

62   Author interview with Andreas Harsono
63   DataGuidance. "Indonesia: New GR 71 enters into force and 'proves more legal certainty'. OneTrust *DataGuidance,* 2019, 7 November, https://corporate.dataguidance.com/indonesia-new-gr-71-enters-into-force-and-provides-more-legal-certainty/
64   ABNR, "Indonesia Issues Important New Regulation on Electronic (Network and Information Systems" *ABRN.* 2019, 30 October, https://www.lexology.com/library/detail.aspx?g=cd6e5251-6dd7-4b46-b6be-759c78c9bf7b
65   Draft of Ministerial Regulation for Private ESO (Registration and Content Moderation)
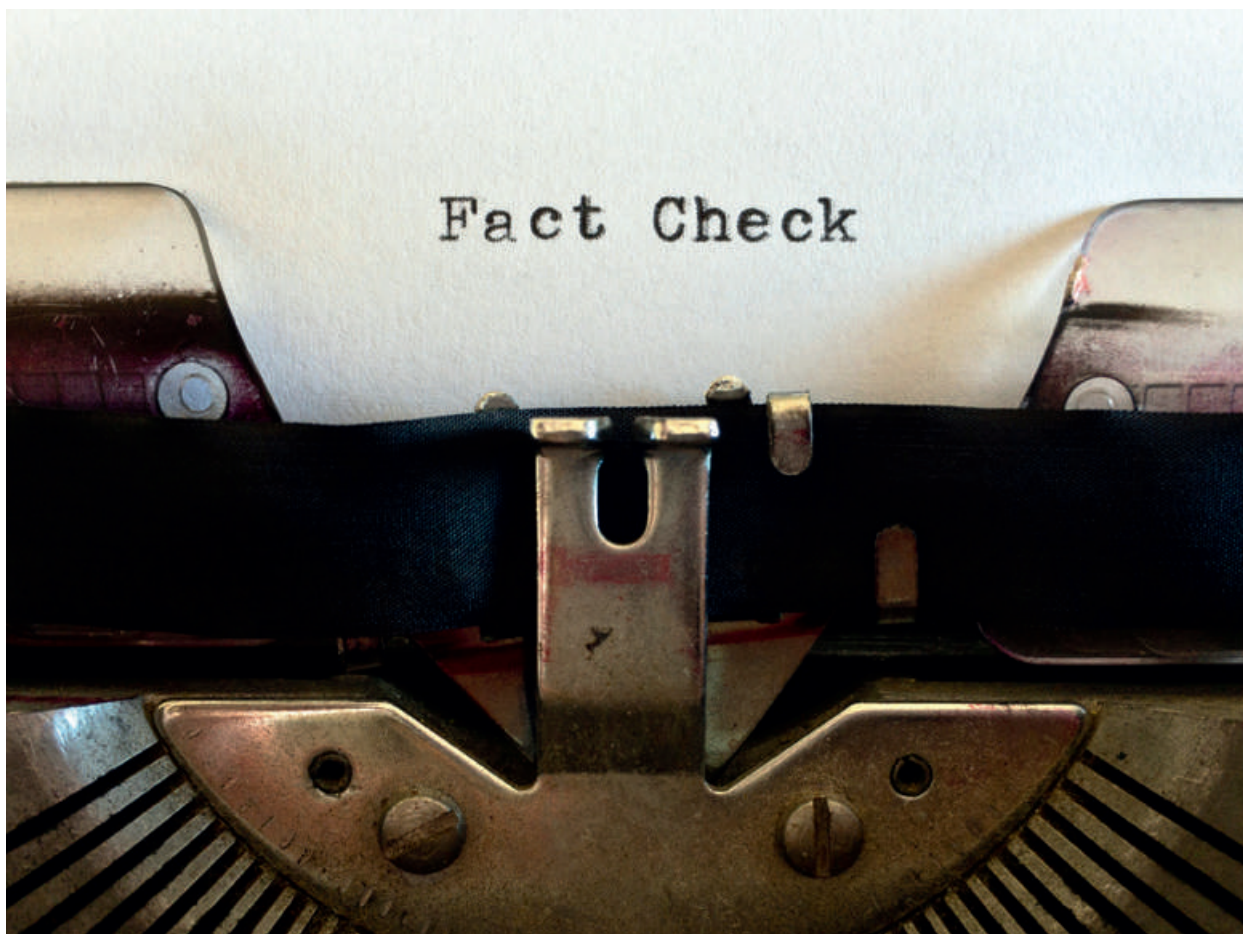66   Interview 9
67   Interview 1
68   Interview 1
69   Author interview with Kirsten Han
70   Interview 11
71   Author interview with Kirsten Han
72   Author interview with Damar Juniarto

An academic said Singaporean politicians also still "resort to civil and criminal defamation" against certain commentary.[73] Singapore's Broadcasting Act has also been used against perceived misinformation. According to one academic, the Act is among the laws used by the Government to censor political dissent.[74]

Penalties and legal appeals

Critics of POFMA have raised alarm about the large costs faced by people who defy orders to remove misinformation, or who want to challenge such orders.

Historian and activist PJ Thum said mounting an appeal against a POFMA charge of spreading misinformation would cost around $1000 for a company. "The Government says it would be fast and cheap to appeal. A thousand dollars is not cheap to us."[75]

One platform expert said the appeals process has proven to take at least two weeks, which was particularly problematic because election campaigns in Singapore run for ten days.[76] So, a successful appeal against a POFMA order about election-related material usually took longer than that and could not be resolved during an election campaign.

Kirsten Han took a similar view on POFMA:

> There's value in appealing just for the sake of showing that you don't agree. But... they use POFMA during the election campaigns. None of those appeals would have gone through fast enough to be in time for the election.[77]

However, Han also acknowledged POFMA has had some unintended benefits. The ever-present threat of her reporting being challenged under POFMA (or "POFMA-ed," as critics call it) has forced journalists to always keep in mind the need for evidence to support a story.

"It pushes you to find more evidence to support the story," she said. An academic also said POFMA had been useful in managing COVID-19 misinformation and hate speech.[78]

However, such positive angles about the various misinformation laws in Singapore and Indonesia were rare in interviews conducted for this project.

Observers in Indonesia questioned the usefulness of strong fines and other penalties as a weapon against misinformation. One academic said the penalties had not had a significant deterrent effect. Despite a high number of cases in courts, there was still a lot of misinformation in social media, suggesting law enforcement is "not easy to bring."[79]

---

73   Interview 11
74   Interview 11
75   Author interview with PJ Thum
76   Interview 1
77   Author interview with Kirsten Han
78   Interview 11
79   Interview 7

Section 2
Ongoing challenges

Challenges for platforms

Digital platforms face various technical, cultural, political and legal challenges in their efforts to mitigate misinformation. Observers from within and outside the platforms provide insights into these challenges in the following section.

Agnostic and cross platform misinformation spread

The relatively free movement of content between platforms adds to the task of trying to mitigate misinformation and disinformation. One observer said the movement of content between platforms meant legislation or voluntary regulation needed to be "platform agnostic," rather than targeted at certain platforms or platform functions, and focused "more on behaviours as opposed to content."[80]

> When Governments talk about disinformation and influence operation, they will try to read into the motive of the people doing it. And we think that's really hard, right? Like as a platform, users are users, we don't know which ones are out to get people and if governments just simply tell us, "we believe these people are trying to interfere in our local discussion and civic discussion" and tell us to block these people. Then, that's not straightforward.[81]

Collaboration, trust and information sharing between platforms were also needed to deal with this cross-platform problem.

Geography, culture and language

The location of most of Indonesia's social media companies' headquarters in Jakarta presents problems when misinformation comes from other regions across the vast Indonesian archipelago, according to Andreas Harsono. The "Java-centrism," due in part to the Indonesian Government barring platforms from opening offices in places such as Papua, meant platforms were not well placed to deal with misinformation issues in other regions.

One digital platform expert said that because misinformation can be "very much localised," it might not be readily recognisable as misinformation to "someone that sits in Jakarta."[82] He said platforms needed to make greater efforts to bridge the geography gap:

> When it comes to sub-regional elections… We don't have CSO partners there on the ground to flag misinformation that could potentially turn into real world harm… So these conversations need to be initiated.[83]

Differences between Indonesian cultural values and internationally-influenced "community standards" of platforms also create ongoing problems, according to one academic.[84] For example, pornographic images considered acceptable in Western cultures were regarded as contraband in Indonesia due to its socially conservative values – highlighting the potential tensions between the values of digital platforms and the local populations they serve.

Language diversity – both between and within countries – is another major challenge for platforms – particularly in Indonesia, where hundreds of indigenous languages are spoken across the country. One academic said the use of local languages on social media made it difficult for platforms to quickly detect problems such as hate speech, misinformation, radicalism, pornography and even indications of intent to suicide.[85] Another observer lamented the lack of fact checking of regional media.[86]

Damar Juniarto commended the platforms for supporting translation of SAFEnet's fact checking work. He also noted that SAFEnet's content was able to be widely translated and read using ClaimReview, the global tagging system. Fact checkers use it to identify their articles for search engines and social media platforms to use to promote and highlight fact checked articles. However, the continuing challenges presented by language diversity highlighted the value of platforms having partnerships with local actors.

Legal repercussions

Platforms can face potential legal repercussions resulting from their measures against misinformation and disinformation. One digital platform expert said the company had been threatened with lawsuits and, in one case, actively pursued over alleged reputational harm after labelling a group as a disinformation network.[87] But such lawsuits were rare "because our process is very rigorous."

Social media influencers

Platforms face unique challenges when high-profile users promote misinformation to their thousands or millions of followers. One digital platform expert said attempts to crack down on social media influencers can backfire when the influencer "cries foul" and attracts more sympathy from followers.[88]

---

80   Interview 4
81   Interview 4
82   Interview 9
83   Interview 9
84   Interview 7
85   Interview 7
86   Author interview with Wahyu Dhyatmika
87   Interview 4
88   Interview 1

Timeliness

Platforms say they face sometimes unrealistic demands from governments seeking quick responses to cases of alleged online misinformation. One platform expert says demands for quick action conflict with the platform's need to ensure thorough and fair processes.[89]

> We have a very rigorous process that usually takes several days, if not weeks, and in some cases, months, depending on the size, and the nefariousness of these networks.[90]

The digital platform expert expressed frustration at the eagerness of governments to "shut down those accounts in 24 hours" without trying alternative mitigation mechanisms first.

Another platform expert agreed:

> There's still a high expectation for us to remove (misinformation) very instantly. And that's something that I feel like the regulator doesn't understand. It can't be as straightforward as that.[91]

Media and community group representatives sympathised with the platforms on the issue of time pressure. While wishing for a "fast response" to his requests for action, Damar Juniarto of SAFEnet acknowledged that "it takes time."[92] MAFINDO's Septiaji Eko Nugroho said platforms had been "quick enough" in their responses to potentially harmful content, particularly during the pandemic.[93] However, he said this had been made possible in part due to the active role of other groups such as MAFINDO in detecting and reporting online misinformation.

Challenges for governments

Laws being relied upon by the Indonesian and Singaporean governments to tackle online misinformation are beset with practical issues and obstacles to their enforcement – not least globalisation versus national sovereignty and unresolved debates over what defines misinformation.

Globalisation

Globalisation presents a major challenge to the effective implementation of national laws against misinformation – particularly when there is disagreement between countries on what constitutes legitimate content. The international reach of online misinformation limits the effectiveness of one country's legal jurisdiction acting alone. And when there is disagreement across national borders about the nature of the content, this can raise potential diplomatic issues not only for governments, but for the platforms given the task of resolving them.

Journalist Kirsten Han questioned whether Singapore's POFMA law could be used to prosecute foreign-sourced misinformation and disinformation:

> POFMA is very effective if you're using it against a local activist who has limited resources, and who is in Singapore and has to comply. But if you are actually talking about a foreign state launching a disinformation campaign… like what they say Russia is doing in the US, how would you use POFMA against that?[94]

Han cites the case of political dissident Alex Tan, the subject of several orders under POFMA, to illustrate the limitations of laws that seek to prosecute alleged misinformation coming from outside the country (see chapter 2 for details).

Law enforcement

Interviewees criticised the tendency of governments to prioritise law enforcement ahead of alternative, less drastic mechanisms to deal with online misinformation. Septiaji Eko Nugroho of MAFINDO suggested there were more effective measures that could be tried first.[95] He supported the use of "restorative justice," including local "social sanctions" and mediation as a "more persuasive and educational" approach than law enforcement, which he said should be a last resort.

A notable feature of the POFMA law in Singapore is its preference for corrections over content removals. This attracts mixed views. One digital platform expert, while generally concerned about POFMA, supported the Government's approach of informing platform users that a post contains misinformation, rather than removing it.[96]

But an academic argued that the harmful potential of misinformation, particularly on an issue such as COVID-19, requires more stringent measures.[97] He said:

> It is not censorship if you remove or delete false information on health… The impact can be exponential… it should not be left on. And that is why I'm against the use of the POFMA.[98]

Critics also said the claimed intent of POFMA was at odds with the way it had been used by the Government to date. PJ Thum said definition of what constitutes a falsehood had been blurred:

> It became very clear from almost the very first use of POFMA that it was about interpretations of statements, and that the Attorney-General's chambers held the position that as long as any interpretation of a statement could be construed as false, the Government was entitled to use POFMA.[99]

---

89   Interview 4
90   Interview 4
91   Interview 9
92   Author interview with Damar Juniarto
93   Author interview with Septiaji Eko Nugroho
94   Author interview with Kirsten Han
95   Author interview with Septiaji Eko Nugroho
96   Interview 1
97   Interview 3
98   Inteview 3
99   Author interview with PJ Thum

Political use of misinformation laws

Online industry insiders and other observers say the governments of both Indonesia and Singapore have used misinformation laws to censor or silence a wide spectrum of critics, with major implications for freedom of speech, media freedom and political democracy.

In Singapore, interviewees for this project raised concerns about the targeting of opposition politicians, activists, journalists and bloggers under the POFMA law.[100] Activist PJ Thum said POFMA had enabled the arbitrary use of government power against many groups and individuals: "Because the definitions and the discretion is entirely controlled by ministers, it's impossible to appeal against this or push back against this," he said.

In Indonesia, the ITE law was of particular concern. Damar Juniarto of SAFEnet said "misuse" of internet laws was particularly prevalent around election time. He also lamented a general rise in the influence of online misinformation on Indonesia's political process dating back to 2012.

Septiaji Eko Nugroho of MAFINDO said that before the coronavirus pandemic, legal cases against misinformation were mainly about political issues, particularly around elections, and hate speech. However, he added that the laws were not just used against government critics: "Sometimes even big supporters of the President go to jail because of... misbehaviour issues in social media," he said.

Others noted recent examples to illustrate the Indonesian Government's use of the ITE law and Criminal Code to limit political expression. Andreas Harsono said Papuans and ethnic Moluccans were threatened with the law over their struggle for sovereignty, while an academic cited two instances in 2019 – the post-election riots and unrest in Papua – when the Government either slowed down or blanketed internet access for citizens as a way to mitigate the unrest.[101]

Targeting the media

Journalists have been key targets of misinformation laws in Indonesia and Singapore. One interviewee said journalists faced the risk of significant jail terms for their reporting in Indonesia.[102] While noting that the Singaporean Government had not jailed anyone under misinformation laws, PJ Thum, who runs the independent media company *New Naratif,* said:

> The Government can simply ban us. They can block access to our site. And because I'm a Singaporean, they can come after me and haul me into court and charge me with whatever they want under the law... And then they can come after *New Naratif* for up to half a million dollars. So these are the things hanging over our heads.[103]

Suggesting independent media organisations had received particular scrutiny, PJ Thum cited an example from the recent Singapore election campaign involving a statement by Chairman of the Singapore Democratic Party, Professor Paul Tambyah to which the ruling party (PAP) objected.

> (The PAP) were very careful about it... they did not hit the Singapore Democratic Party or Paul Tambyah himself with POFMA, even though he was the source of the statement. They hit the outlets which reported his statement, which means he had no standing to appeal. Only the media outlets could challenge it. And given the very short election period... by the time that (media outlets) appealed, the election was pretty much over. So I do feel that this did sway the results against Tambyah.[104]

The ruling party has used a number of regulatory measures to rein in Singapore media companies and journalists. Kirsten Han said the party's presumption of control over what constitutes a falsehood, combined with the lack of freedom of information, made it hard for journalists to circumvent POFMA orders. And the costs of appealing against such orders could be prohibitive for freelance journalists and independent media companies.

Critics say the ruling party has also tried to censor media organisations by "gazetting" them as political organisations, which means they are banned from accepting money from foreigners and forced to declare all donations. Thum said *New Naratif* had sought to circumvent these issues by registering offshore.

Han has worked around the "gazetting" problem *because* she works independently and writes for international publications. This allows her "to write a report about Singapore outside of government control."[105]

In Indonesia, Wahyu Dhyatmika said *Tempo* had been on the receiving end of multiple complaints to the Press Councils and sometime lawsuits from government ministers.[106] In another instance, after publication of a critical investigation into the Indonesian Government, Wahyu Dhyatmika said his site was attacked and "bullied by bots" in an orchestrated cyber-attack. While he couldn't prove the Government was involved, he said the timing of the attack soon after publication was suspicious.

Censorship, self-censorship and freedom of expression

Critics say the introduction of laws such as POFMA has had what one called a "chilling effect" on public discourse in Singapore. One academic feared self-censorship will increase as POFMA is deployed to censor political dissent and alternative views.[107]

PJ Thum said the fear of POFMA orders was already affecting media practice. He cited the typical example of an editor wanting to print something in the public interest, but the author resisting because they don't want to get "POFMA'ed."[108]

Thum said regulations that pre-date POFMA in Singapore had already acted as a deterrent, particularly for

---

100 Interview 1
101 Interview 1
102 Author interview with Andreas Harsono
103 Author interview with PJ Thum
104 Author interview with PJ Thum
105 Author interview with Kirsten Han
106 Author interview with Wahyu Dhyatmika
107 Interview 11
108 Author interview with PJ Thum

independent media. "Even if POFMA disappeared, you'd see no new media start-ups for social-political issues because of the fear (of) the regulations."[109] The main problem with POFMA, he said, was its contribution to a culture of self-censorship:

> A lot of these laws create fear so that people end up self-censoring. So the Government can say that they didn't do anything. They didn't actually apply the law.[110]

Kirsten Han said of her own practice: "There is definitely kind of more apprehension and hesitation… I definitely have found myself hesitating on some stories."

In Indonesia, Wahyu Dhyatmika observed more caution among people engaging in online discussions:

> You can see it from chats, response or comments that we have for our content on social media. The commenters, the users will remind each other, "careful with your comment. Don't post anything that's sensitive, because who knows what will happen."[111]

Interviewees in both countries cited anti-misinformation laws as a restraint on freedom of expression and democratic discourse more broadly. The use of POFMA during the 2020 Singapore elections was a case in point. One academic said:

> The Government used laws, and sometimes quite bluntly, to coerce the technology companies… to remove posts… during the elections.[112]

The Government had also invoked POFMA to pressure political parties to remove or retract what they had said about the government planning policies.[113]

In Indonesia, activists fear proposed changes to the Criminal Code will increase the Government's powers to suppress free speech. Another civic rights activist, Damar Juniarto of SAFEnet, cited proposed limits on criticising the Government, saying the Bill was designed to benefit the powerful over the people.[114]

But one academic believed the public also need to appreciate their responsibilities when it came to free speech:

> There is a grey area between freedom of expression… (and) how to be an active and also ethical digital media user or digital citizen. Sometimes people interpret freedom of expression to mean freedom to say anything, but they forget that it should be in an ethical manner.[115]

Declining quality of debate

Interviewees blamed the use of misinformation laws, and the resulting restrictions on free speech, for a general deterioration in the quality of public and political debate in both countries. One Singapore academic sensed the Government wanted to use POFMA to "stop debate," leading to the loss of a democratic contest of ideas.[116]

PJ Thum said the Singapore ruling party "hates" foundational elements of a functioning democracy such as "a critical citizenry (that) asks questions of the Government…they prefer to write laws which just give them vast sweeping amounts of power, and just tell people to just blindly listen."[117]

Interviewees also lamented a decline in the standard of public debate in Indonesia, which they blamed in part on the use of misinformation laws to persecute journalists and to control the free flow of information online.[118]

Lack of transparency

Critics also cite a lack of transparency surrounding the use of misinformation laws. Central to this issue is unequal access to information, favouring governments over their populations. Kirsten Han said:

> In Singapore… there's no freedom of information laws. So the Government holds pretty much all the cards in terms of data. So I can say something, and they go, "that's not actually true, because our data shows this," and then I can't do anything.[119]

One academic also questioned the transparency of the appeals process under POFMA, despite it being portrayed by the Government as inexpensive and accessible.[120]

Similar concerns have been raised about Indonesia's ITE law. Wahyu Dhyatmika of *Tempo* said, "the problem is sometimes… there's no transparency about how it's being used." While action is often taken when government officials allege misinformation and disinformation, members of the public lack the clout to get such action taken on their behalf.

The backfire effect

Some observers believe Singapore's ruling party has damaged its standing with the public by appointing itself the arbiter of truth under POFMA. PJ Thum points to the PAP's poor election result in 2020 as evidence that the Singapore public "are not going to put up with" the use of laws such as POFMA to suppress democratic rights. He hoped its relatively poor poll result for a party in power since 1959 would encourage the Government to restrain its actions in future.[121]

Critics believe the use of POFMA to combat misinformation on private messaging platforms may also have backfired on the ruling party. Kirsten Han said that to issue a POFMA order against such content appeared not only impractical, but counter-productive

109   Ibid
110   Author interview with PJ Thum, Historian and Managing Director of the *New Naratif,* 19 August 2020
111   Author interview with Wahyu Dhyatmika
112   Interview 11
113   Interview 11
114   Author interview with Damar Juniarto
115   Interview 7
116   Interview 3
117   Author interview with PJ Thum
118   Author interview with Andreas Harsono; Interview 7
119   Author interview with Kirsten Han
120   Interview 11
121   Author interview with PJ Thum

"because that means you're actually going to be amplifying the falsehood that you're supposed to fight."[122]

One digital platform expert said "the vast majority" of POFMA corrections during the election campaign were issued in response to criticism of either the Government or government policy.[123]

Kirsten Han said:

> It didn't seem like POFMA orders were taken that seriously... it feels like people see POFMA not as a fact checking tool but as a political tool... It's definitely not escaped notice that no PAP politicians have been POFMA'ed. It's always opposition politicians, and its mainly independent news sites.[124]

PJ Thum agreed that this approach may have backfired on the Government:

> I think people have reached a point where they realise POFMA is really a tool by the Government to silence its opponents and to make sure its version of narratives gets perpetuated.[125]

In both Singapore and Indonesia, a perceived lack of transparency around misinformation laws was seen to have contributed to decreasing trust in governments.[126] As PJ Thum argued:

> If we don't trust the Government to regulate appropriately, if we don't... have trust in their motives, then any regulation is greeted with hostility and seen as... the Government trying to interfere with our freedom of speech.[127]

One Singapore academic said the continued use of other laws against misinformation alongside POFMA had bred distrust. It suggested that POFMA was "not strictly necessary" – and raised questions about the Government's justification for its introduction.[128]

Religious vilification

The central role of religion in public and political life in Indonesia is claimed by critics to have added to the discriminatory nature of misinformation laws. Andreas Harsono cited the case of a Christian politician who complained about discriminatory regulations made "in the name of Islamic Sharia," and who was subsequently reported to the police by an Islamist group for alleged blasphemy.[129]

Another well-known case of blasphemy law being used against a religious minority involved the former Jakarta governor Ahok (see chapter 5). Harsono believes the use of the law against Ahok in 2017 caused his election defeat. In this context, Harsono held grave concerns about changes proposed to Indonesia's Criminal Code: "The current draft [of] the Criminal Code is made in compliance with the Islamic Sharia. It will discriminate against minorities."

122 Author interview with Kirsten Han
123 Interview 1
124 Author interview with Kirsten Han
125 Author interview with PJ Thum
126 Author interview with Kirsten Han; Author interview with Wahyu Dhyatmika
127 Author interview with PJ Thum
128 Interview 3
129 Author interview with Andreas Harsono

Conclusion

This chapter examined recent measures that social media and governments have taken to deal with misinformation online. Notwithstanding some vexed questions about definitions of misinformation and disinformation, as explored throughout this document, interviewees identified a range of platform measures and laws that have been enacted to deal with this harmful social problem that impacts on democratic health.

For platform companies, these measures range from removing harmful actors and their content and fake accounts; reducing repeat offenders' access to platform features and platform users' exposure to low-quality content; and informing users of unreliable content (not suggestive of causing real-world harm) by using independent fact checkers to label it as false and downgrade its spread. Also in the arsenal of tools was using non-human (AI) and human partners, such as trusted civil society groups, to detect and forewarn the platforms of emerging misinformation campaigns. The public also plays an important role in reporting online misinformation with mechanisms to alert the platforms of content that deviate from its policies and community standards. These documented community standards enable social media companies to articulate their expectations of online behaviour and content to users.

These measures highlight the multi-pronged approach needed to tackle a complex problem and they underscore the importance of working in partnership with users and civil society. Clearly, there is also a need to work cooperatively with governments and other platform companies if the endemic problem of misinformation is to be mitigated. As this chapter has shown, there are still mighty challenges for platforms to work through to make progress in the battle against misinformation. These include physical hurdles such as working across political jurisdictions, vast geographies and different languages. Different government definitions and expectations of timely responses to mis- and disinformation are often at odds with the platform companies' capacities and understandings. One possible solution is working more closely with other technology companies and different in-house divisions to deal with transnational

and cross-platform misinformation. This again raises important questions about the need for clear definitions, and how to deal with different types of false and misleading content.

Even harsh critics acknowledge governments have an indispensable role to play in combatting online misinformation. But the experts interviewed expressed less confidence in governments' ability to be both the arbiter and enforcer. This chapter has shown that the legislated approach to tackling misinformation in Indonesia and Singapore has prompted widespread concern that the mandated "solutions" can produce similar effects to the original problem by undermining media and political trust and free speech in both countries. As has been discussed, some of these consequences, such as suppressing political dissent, can serve government interests; while other adversities such as criminalising those who inadvertently spread misinformation, may be unintended. In any case, the limitations of the legislated response to tackle online misinformation highlights important considerations for Australian law and policymakers to consider in their pursuit of regulating misinformation online. Chief among these questions is how to balance responsible speech with free expression without overreaching and damaging a vibrant democracy.

Potential remedies

Introduction

Policy makers seeking solutions to the rampant spread of online misinformation face formidable challenges. The starting point for any plan to deal with online misinformation must be recognition of the need for a multi pronged approach – and for cooperation between key stakeholders.

The multiple layers of complexity that define this global problem defy simple answers.

These are among the main conclusions to be drawn from extensive interviews conducted for this project with digital industry experts, academics, media professionals and others with specialist knowledge of the online environments of Indonesia and Singapore. While individual ideas for how to tackle the issue vary significantly, broad consensus exists on the need for multi-faceted strategies involving all interested parties, including government, the technology industry, the media, and community-based organisations. The scope of suggested initiatives was extensive – from active programs to enhance digital literacy and journalism standards, to increased collaboration between digital platforms, more transparent and inclusive government policy-making and, crucially, a quest for consensus on the vexed issue of how to define online misinformation. Some of the suggestions are already active or are being developed. This chapter outlines some of the main proposed remedies from the perspective of those interviewed.

Common definitions

Ambiguity about what defines misinformation, and how this relates to considerations of free speech, is a recurring theme among those seeking and proposing solutions to the scourge of online misinformation.

Some observers see the resolution of this confusion as a necessary pre-requisite to tackling the issue. Singapore-based journalist Kirsten Han believed digital platforms needed to take more of a lead, saying they "should be clearer about their content standards," which in turn would clarify behavioural expectations on users.[1] Han said the platforms could do this by adopting uniform international standards on human rights and free speech rather than arriving at their own definitions.

One Singaporean academic said the Singaporean government, like other nations including those in the European Union, were still unclear about what is "deemed as a falsehood or as misinformation and disinformation." Part of this uncertainty, the academic noted, was a function of the newness of regulating online misinformation and disinformation, and ideas were evolving.[2]

A social media expert said journalists, policy-makers and regulators, including the EU Code, often conflate misinformation with disinformation:

> When they start conflating all these different issues, it makes it really difficult for anyone to be able to then decide on what the actual issue is. So in order to come up with a solution, we try to have very clear definitions about what we are talking about. So when it comes to talking about any kind of misinformation regulation we really fight for clarity as to what problem we are trying to address before we can even start developing any kind of regulation.[3]

Facebook's approach is to deal with disinformation by focusing on actors, behaviours and content. Disinformation involves actors and behaviours and what it also calls "coordinated inauthentic behaviours" (CIB). Tackling misinformation focuses on content, to remove false claims online working with third-party fact checkers and comparing how content sits alongside its community standards and policies.

However, the company concedes that misinformation and disinformation can involve the same content. A problem with content-based approaches is that it is not systemic but a "whack-a-mole" approach. The social media expert said the company was more effective when it examined actors and behaviours because then it could see breaches against platform policies and remove pages, their contents, and networks.

---

1   Interview with Kirsten Han, interview with Andrea Carson, 25 August 2020.
2   Interview 11, interview with Andrea Carson, 20 August 2020.
3   Interview 13, interview with Andrea Carson, 16 September 2020.

When we're taking down these pages and networks, we feel that it's a greater impact. And it's more scalable than just taking down one piece of content at a time. This is why we look at these three individual pillars, because it then allows us to kind of look at the problem more holistically, but then also carve out different solutions to address different areas.[4]

If policy-makers, platforms and journalists had the same understanding of the definitions of misinformation and disinformation there would be less confusion about measures needed to combat electoral interference and foreign interference, according to the social media policy expert:

We're trying to educate policymakers on these differences, because I think it does make a huge difference in terms of the types of regulation that needs to be put in place, the types of policies that companies put in place, and mitigation approaches that need to be put in place.[5]

However, definitions also needed to be mindful of local norms, as one Indonesian academic observed. The use of the term hoax instead of disinformation was one example. Another was what content was considered harmful:

There is a tension between government and the international platforms because social media platforms have community standard or community guidelines, but it's produced for international needs. Indonesians have specific needs that have to be contextualised with the local conditions, especially in terms of for example pornography. In Indonesia, the definition of pornography is different in terms of community standards from international social media platform guidelines.[6]

Digital literacy

Improving citizens' media and digital literacy was advocated by all groups and individuals involved in this project. Education was pinned as being at "the centre" of any multi-pronged approach, with "incentives to educate the public and get the various stakeholders involved about disinformation, misinformation and fake news."[7]

Digital literacy was seen as a valuable bulwark against misinformation because it encouraged people to "use critical thinking before they share a specific type of content," as one digital platform expert put it.[8] In this way the problem could sometimes be mitigated in advance. Indonesian activist and head of anti-misinformation group MAFINDO Septiaji Eko Nugroho likened education in this context to "immunisation" and "inoculation."[9] This approach would focus on the "the psychological aspects" of preparing people in advance to avoid being "misled by misinformation." The approach,

which he said was still in development, would seek to "fight misinformation with information" and could be particularly applicable to situations such as the COVID-19 "infodemic."

Singapore-based academic and activist PJ Thum said that Singapore had always proceeded on the "impossible" premise that, "we can regulate anything, if we just write the laws well enough and if we are given enough power and if you trust enough in our benevolence and our intelligence."[10] He believed the development of more "critical minds" among citizens through media literacy would reduce the need and

scope for governments to claim sole responsibility for regulating the problem, and therefore make it more difficult for them to justify some of their more contentious measures.

Amid broad agreement about the value of digital literacy, different suggestions emerged on how it should be pursued. One academic suggested all stakeholders, including technology platforms, should be given incentives to invest resources in education of "the masses."[11] Another academic with experience in conducting digital literacy programs in Indonesia proposed a nuanced approach. "I always say that you have to be not only smart using the digital media, but you have to be wise and also ethical. And it's not easy to ask people to be ethical."[12] For these reasons she said the design and implementation of digital literacy programs needed to consider a variety of contextual factors beyond the education itself.

4   Interview 13.
5   Interview 13.
6   Interview 7, interview with Andrea Carson, 19 August 2020.
7   Interview 11, interview with Andrea Carson, 20 August 2020.
8   Interview 9, interview with Andrea Carson, 8 September 2020.
9   Author Interview with Septiaji Eko Nugroho, interview with Andrea Carson, 26 August 2020.
10   Author interview with PJ Thum, Historian and Managing Director of the *New Naratif,* 19 August 2020
11   Interview 11.
12   Interview 7, interview with Andrea Carson, 19 August 2020.

A digital platform expert with experience in digital literacy programs in Indonesia criticised approaches that had so far focused only on "niche markets."[13] What was needed, he said, was "a massive campaign and to really educate the masses." While acknowledging the success of initiatives in which he had been involved, he said they were expensive and largely deployed during election campaigns. "I feel like we need a program that is much more sustainable, that continues to surface whether there is an election or not."[14]

Another observer, Septiaji Eko Nugroho, proposed a "curriculum" to guide future educational efforts. This would include

teaching citizens "lateral reading" – a self-sufficient verification method as outlined in one of Stanford University's free online curriculum resources. Researchers worked with classroom teachers to produce a curriculum aimed at civic online reasoning skills (COR). These skills enable students to search for, evaluate and verify information. The materials are free online at https://cor.stanford.edu/.[15] Similar approaches, including "train the trainer" programs that give adult citizens the tools to educate others, were also supported.[16] A difficulty with this approach is low levels of general literacy and dealing with different languages,

including within the one country such as in Indonesia. Notwithstanding the challenges, Septiaji Eko Nugroho saw merit in teaching digital literacy through the school system.

A Singaporean academic argued that more government and platform resources needed to be committed to public education about low-quality online information and incentives put in place to encourage the platforms to run these education campaigns: "I don't think there is incentive enough for the platform companies to invest in more tools in educating the masses. I would like to see more resources devoted to education from all stakeholders."[17]

Transparency

Interviewees advocated more transparency – not just by policy and law makers but also news organisations, journalists and digital platforms to assist the fight against online misinformation. One Singapore-based academic argued that governments needed to more "clearly and transparently" communicate their laws to the public.[18]

Others said it was also incumbent upon non-government actors to be transparent. PJ Thum argued that since "everyone who reports has an agenda," it was important that "you yourself are aware of that agenda, of your own biases as a human being, as an organisation, as a platform, whether you're honest

to yourself about your blind spots, your subjectivity, but also whether you're transparent about that with others." A high level of transparency may help prevent citizens from being misled by misinformation disguised as objective fact, he said.

Damar Juniarto of SAFEnet, said digital platforms' transparency reports such as Facebook's twice-yearly reports[19] were an important step for civil society groups to check on government demands to take down online information that "they don't like." He said, "This is something we need to look deeply and closely at." He said the platforms' transparency reports revealed when the government applied a "forceful approach" to the technology platforms to remove content, allowing his organisation to scrutinise such actions.

13   Interview 9.
14   Interview 9.
15   The university's history education group collaborated with the Poynter Institute and Local Media Association to create MediaWise, an initiative supported by Google.
      For details see: https://news.stanford.edu/thedish/2019/12/09/stanford-education-researchers-create-free-lessons-to-teach-digital-literacy/
16   Interview 1, interview with Andrea Carson, 7 August 2020; Interview 7; Interview 9
17   Interview 11.
18   Interview 11.
19   These reports are published on the platform's website at: https://transparency.facebook.com/content-restrictions

Inclusive process

Several contributors to this project recommended more involvement of non-government actors and civil society in the policy-making process.[20] PJ Thum argued that a lack of public consultation in law making would inevitably result in "imperfect" laws that would be open to exploitation by government for political purposes.

Public input could not only help remedy these flaws, but improve public confidence in institutions:

> What you need is a robust way of creating those laws and regulations which is open to scrutiny, which seeks to encompass as many different voices as possible, which has people who are accountable, which is representative, and which is transparent in how it's made. And once you have a very robust way of creating these laws and regulations, and that encourages people to participate in their creation (and) ensures that all these different viewpoints are heard, that itself... makes the law as robust as possible... it gives people more faith in the intent of the law, in the intent of the people behind it.[21]

For Thum, the key to resolving the "crisis of faith" in governments, their intentions and "the system itself" is "to make sure that everyone feels like their voice is heard." A flow-on effect of a more inclusive law-making process would be the public educating themselves on regulatory challenges and taking on greater responsibility for their resolution. This in turn would help governments, as the public would not be "so quick to get angry or point fingers when things go wrong... but instead say, 'okay, we need to go back and participate in the reformulation and rethinking of new regulations' and find ways to then improve these laws."

One social media expert said 'continuous public consultation' has often been the missing link in Indonesia.[22] However, Septiaji Eko Nugroho said efforts to correct this deficit were underway. He endorsed collaborative partnerships between civil society organisations (CSOs), government agencies, media organisations and digital platforms, such as those MAFINDO had established to improve fact checking, deliver digital literacy and monitor elections, among other activities. "We need to tackle [misinformation] with what we call comprehensive efforts or a multi-pronged approach," Nugroho said.

Working with civil society and academics

Several participants advocated governments and digital platforms develop more collaborative working relationships with civil society groups. While recognising that "different contexts around the world" would complicate this task for digital platforms, Kirsten Han said this should not stop them being more transparent with local communities about their content policies. This was particularly necessary when governments exploited platforms' policies to sideline civil society organisations (CSOs) from participating in public debates online.

She cited a case in which a social media platform's new "accountability policies about who can share and boost political content" inadvertently led to the exclusion of civil society groups. Han explained that social media platforms did not quite take into consideration the local context when they rolled out their policy:

> So there was this policy that you would have to be a locally registered group to boost political content — but this only works in an environment where registration is democratic, which it isn't in Singapore because the government can choose to disallow particular groups from registering.[23]

20   Author Interview with PJ Thum; Interview 11; Interview with Septiaji Eko Nugroho; Interview 9
21   Author Interview with PJ Thum
22   Interview 9.
23   Author interview with Kirsten Han

This policy was also problematic for media outlets and journalists. Han explained:

> I was an editor-in-chief of a Southeast Asian platform that was founded by Singaporeans, but we were not allowed to register in Singapore because (the Government) claimed that we were foreign interference… And this happens a lot in Southeast Asia, that human rights and activist groups are not registered because the Government for political reasons do not allow us to register.[24]

Platforms have acknowledged the need to work more closely and productively with civil society groups. A digital platform expert said he valued "having a trusted partner ecosystem, where I feel confident enough that they can report things directly to me or my team… before

bad things can happen."[25] While the trusted partner ecosystem was still "a work in progress," he felt his platform and CSOs "we're in a much better position now" than two to three years ago.

Septiaji Eko Nugroho believed civil society's contribution could be particularly valuable in a "hierarchical" country like Indonesia, where authority figures such as religious leaders or celebrities had "more power to spread the message." Civil society groups could facilitate networks between influential people such as local leaders, journalists and academics, "so that if there is possible disinformation then they can help us."[26]

He related his experience in 2018 during the West Kalimantan regional elections, when MAFINDO set up a "hoax crisis centre" and a related website, bringing together people from the Government, religious leaders, journalists and police, "and then we educated them (about what) we needed to do… when there is misinformation coming before or after the elections." The centre provided clarifications on suspected misinformation, including about religious and ethnic issues. Nugroho asserted

that "nobody" could have achieved this without the help of MAFINDO.

Tempo editor-in-chief Wahyu Dhyatmika expressed similar sentiments, saying "we need a road map that everyone can agree on."[27] He said efforts at collaboration to date had been disjointed, with civil society creating its "own ecosystem" comprised of "mostly media and civil society and not connected to the Government or law enforcement."

Independent civil society groups were also seen to have an important role in helping to identify and remedy unintended consequences of either government or platform-generated misinformation policies.[28] Kirsten Han cited the example of Google's recent decision in Singapore to ban political advertising. She said the decision disproportionately impacted on smaller political parties that relied relatively heavily on online advertising. In another case of unintended consequences in Indonesia, small and medium business groups alerted WhatsApp to problems with its new limits on forwarding messages, which had negatively affected the ability of businesses to market their products.[29]

Public interest journalism

Improving journalism standards and providing the public with access to credible news online was advocated as a potentially valuable tool in combatting online misinformation.

Wahyu Dhyatmika said *Tempo's* international reporting collaborations had "strengthened our credibility and reputation," which had improved engagement with audiences and, in turn, would lead to more people alerting them to suspected misinformation as audience size and audience trust increased:

> I think it comes down to how engaged your audience (is) with you in the newsroom. Because then

you will be able to detect any misinformation early and try to counter it early. And that's better than waiting for it to become viral.[30]

Dhyatmika also highlighted the value of fact checking operations in media companies as a part of the fight against misinformation, while digital platforms that supported fact checking were commended by one academic for

their apparent willingness to tackle the problem.[31] Dhyatmika advocated the introduction of fact checking at more media outlets, particularly local outlets where it was "not that widespread yet," to enable more detection and countering of misinformation "early on."

Platforms' investments in journalism projects such as Google News Initiative and Facebook's Journalism Project were commended by respondents. One academic said these projects help quality journalism survive and would like to see these models replicated by other technology companies.[32]

24   Author interview with Kirsten Han
25   Interview 9
26   Author interview with Septiaji Eko Nugroho
27   Interview with Dhyatmika, interview with the author, 24 August 2020
28   Interview 6, interview with Andrea Carson, 25 August 2020; Interview 9
29   Interview 9
30   Author interview with Wahyu Dhyatmika
31   Interview 11
32   Interview 11

Collaboration between technology platforms

Greater collaboration and information sharing between technology platforms is seen by some industry figures as a necessity in the fight against online misinformation, given the ubiquity of the problem. A digital platform expert suggested more cooperation would require a shift in attitudes by some platforms towards others. While platforms might be competitors in business, in the information space they were "friends."[33] He proposed legislation to facilitate collaboration, saying: "Legislation should focus on… how civic society, journalists and platform and tech industries could work together to develop best practice."[34]

However, a social media expert said cooperation was more common than what might be known by the public. When one digital platform unearths a disinformation campaign they share it with the others. "There's constant engagement that takes place between us and all the other industry partners in this space of disinformation."[35] The expert said Europe was the most advanced in information sharing with intelligence authorities and between the technology platforms such as Google, Twitter, Facebook, Microsoft and Reddit. This coordination included annual conferences to share intelligence about disinformation threats and to exchange information:

In this way we can then tackle the problem together because we know that collaboration with our industry, partners, governments, civil society, and even academia is really key to solving the problem.[36] Less clear was how coordinated communications between industry and other allies were in the Asia Pacific. As another digital platform expert in the region stated:

It's very seldom that we partner with other social media platforms. It's almost as if we just have to own the problem ourselves and address it head on, whether it's directly with the regulator or in partnership with the CSOs. But, I think the key is not so much partnering with the folks in the industry but partnering with the CSO partners… that's the approach that we have taken so far.[37]

Conclusion

Central to the recommendations to manage online misinformation is the need for agreement on definitions, so that those trying to find remedies are actually addressing the same problem. It is not clear that this has been the case to date. From the interviews it was also clear that mitigating misinformation requires a multi-pronged approach.

Digital education programs cannot be done in isolation without efforts to reduce false information and remove harmful content. The experts also agreed that such a complex problem requires the involvement and cooperation of different actors, ranging from civil society organisations, academia, journalism, digital platforms, government and policy-makers. Likewise, any regulatory initiative to address misinformation online needed to include those with grass-roots experience about the forms in which it appears, as well as those with specialist knowledge such as policy-makers and academics. Inherent in the duplication of recommendations was the need for the different parties to communicate to the public about what they are already doing about false news online and why.

---

33   Interview 4
34   Interview 4
35   Interview 14. Correspondence with Andrea Carson, 18 November 2020.
36   Interview 13.
37   Interview 4.

Concluding analysis

Concluding **analysis**

The globalisation of digital communication technologies in the 21st century has delivered unprecedented opportunities and challenges. It promised a more inclusive digital public sphere, with the internet playing a democratising role to enable citizens from around the globe to come together. It also changed the ways in which we think about news. As New York academic Jay Rosen famously wrote, "the people formerly known as the audience" are now both *consumers* and *producers* of content.[1]

The rise of the digital technology giants has overshadowed the cultural power of legacy media. Facebook, Twitter, YouTube and others have provided the means for anyone with an internet connection and a keyboard, smartphone, camera or voice-activated software to participate in creating and exchanging news and information.

This report deliberately focuses largely on the challenges, not the opportunities, of these profound developments. Supported by detailed case studies of the experiences of Indonesia and Singapore, we have examined how global communication networks have facilitated the prolific spread of online falsehoods – primarily misinformation and disinformation – to create what academic Claire Wardle describes as a world-wide phenomenon of "information disorder".[2] We have explored the potentially far-reaching consequences of the spread of online misinformation, and how governments and technology platforms have responded with various measures to tackle the problem.

The report finds that misinformation, even when transmitted innocently, can have detrimental consequences, ranging from undermining democratic processes and public health and safety, to inciting violence against minorities and other vulnerable groups and individuals. In cases when it leads to harm, misinformation can overlap with disinformation, which for the purposes of this study is regarded as false or manipulated content that causes political, personal or financial harms.[3]

Misinformation's pernicious spread has made it a top-level policy concern for governments around the world. In Australia, the Morrison Government, acting on the recommendations of an inquiry, has instructed the digital technology platforms to implement a voluntary Code of Disinformation by 2021. The findings of this study aim to assist public debate surrounding the development of the code.

In pursuing remedies to the spread of online misinformation, governments in liberal democracies like Australia face the considerable challenge of trying to strike a balance between mitigating harm, and preserving basic democratic tenets such as pluralism, freedom of expression and media freedom.

Governments have choices in how to respond. This report highlights the mixed and sometimes negative experiences of two Asia-Pacific countries that have chosen a legislative pathway. Others, such as the European Commission, have so far opted for voluntary regulation. The benefits and drawbacks of Europe's approach feature in chapter three.

These choices come at a critical time – when media and political freedoms once taken for granted appear to be under threat across the globe. Both illiberal and liberal governments have presided over 14 years of what the democracy activist group Freedom House describes as an "assault" on democracy and pluralism. The group warns that digital platforms and social media are the new frontier in this world-wide attack on freedoms.[4] The majority of countries that have opted for fake news laws already restrict their citizens' political rights and civil liberties, and are considered "partly free" or "not free" on a democracy scorecard. Singapore (with a score of 50 out of 100) and Indonesia (61) are lowly ranked compared with Australia's score of 97.[5] However, Australia scores less well on internet freedom (76 out of 100) due to existing "limits on content, violations of user rights and obstacles to access".[6]

These indicators serve as a warning as countries pursue regulatory and legislative pathways to tackle online misinformation. The key findings of this report highlight worrying effects of government over-reach through legislative responses to misinformation. The governments of both Singapore and Indonesia have been accused of misusing their anti-misinformation laws to censor or silence a wide spectrum of critics, including journalists, political dissidents and human rights

---

1   Jay Rosen, "The people formerly known as the audience," in *Participation and Media Production: Critical Reflections on Content Creation*, eds. Nico Carpentier & Benjamin DeCleen (Newcastle upon Tyne, UK: Cambridge Scientific Publishers Ltd, 2008), 163-165.
2   Claire Wardle, "The Need for Smarter Definitions and Practical, Timely Empirical Research on Information Disorder." *Digital Journalism,* 6, 2018 no. 8: 953.
3   James Meese, J and Edward Hurcombe, Regulating Misinformation: Policy Brief (Melbourne, Analysis & Policy Observatory, RMIT University, 2020), https://apo.org.au/node/309357
4   Sarah Repucci, "A Leaderless Struggle for Democracy: Democracy and Pluralism are under assault", *Freedom House,* 2020, https://freedomhouse.org/report/freedom-world/2020/leaderless-struggle-democracy
5   Ibid
6   Freedom House, "Freedom of the Net 2020", (Freedom House, 2020), https://freedomhouse.org/country/australia/freedom-net/2020#C

campaigners, as well as religious leaders. Experts criticised the tendency of these governments to prioritise law enforcement over alternative, less drastic mechanisms to deal with online misinformation. Academics observe that fake news laws addressing misinformation can only be successfully implemented without damaging political and civil rights in robust democracies like France, which have added checks and balances to their legislative measures.[7]

Empirical data highlights some positive results for non-regulatory measures already being employed by digital platforms and others to tackle online misinformation. These include:

- Tools and campaigns to improve digital literacy
- Third-party fact checking of content and use of false information warning labels
- Requiring proof of identity to improve account transparency
- Removing harmful content or limiting its algorithmic spread
- Reducing services to users who breach community standards
- Supporting journalism by providing resources and financial support to news media organisations.

However, public recognition of this work appears to be limited. Platforms would serve themselves and the public well to improve the visibility of existing measures, and to more widely publicise the role the public can play in limiting the spread of misinformation.

Certainly, more work is needed to curb the scourge of online falsehoods, perhaps starting with a greater

sense of shared responsibility by governments, digital platforms and users. Non-government organisations, academia, and traditional media also have vital roles to play in the promotion and development of digital literacy education and sustaining a culture of reliable and trustworthy information. As already happens in Europe, these key players could generate considerable benefits by holding regular meetings to communicate and share knowledge of known online risks and strategies to mitigate misinformation including being mindful not to inadvertently, or otherwise, amplify it.

The development of a successful voluntary code requires input from diverse stakeholders. But first there needs to be consensus on the meaning of key terms such as misinformation, disinformation and fake news so that everyone knows they are addressing the same problems. The present lack of definitional clarity across the globe is a key barrier to progress.

Misinformation on global platforms was also difficult to measure at a national level, as it is not confined to country borders. Adding further complexity to detecting and measuring misinformation, are country-specific issues such as Indonesia' hundreds of spoken languages, many with different meanings for similar words that confound artificial intelligence techniques.

Potential remedies identified in the report include further developing trusted partnerships with civic leaders; expanding digital literacy education campaigns; expanding resources for public interest journalism; more

cooperation between platforms; continuing to fund academic research; and greater data transparency for researchers to engender understanding about the scale of the problem and methods to mitigate it.

The findings also highlight the importance of a multi-pronged response to this complex problem, with input needed from a multitude of actors ranging from policy makers and regulators to on-the-ground fact checkers, educators and the organisations that work with victims of online misinformation campaigns. Traditional media also have a role to play as misinformation can be amplified in news reporting and distributed on its digital networks.

The case studies examining Indonesia and Singapore highlight the need for regulatory responses to be customised to national contexts, but to also incorporate international principles such as universal human rights. Expert participants in this project agreed that there was, as yet, no gold standard for regulating misinformation. While the EU code is often referenced and seen as adaptable to the Australian context, experts warned it was not flawless, and cautioned against its wholesale adoption.

Despite the lack of consensus on how to define, measure and mitigate misinformation online, clear unanimity exists about the urgent need to curb it to improve the quality of information in the public sphere, which is vital to a healthy democracy.

---

7   James Meese, J and Edward Hurcombe, Regulating Misinformation: Policy Brief (Melbourne, Analysis & Policy Observatory, RMIT University), https://apo.org.au/node/309357

Acknowledgements

Reference list

About Hungary. "Coronavirus update: Bill on rescinding the government's emergency powers submitted to parliament today." Published May 26, 2020. http://abouthungary.hu/news-in-brief/coronavirus-update-bill-on-rescinding-the-governments-emergency-powers-submitted-to-parliament-today/

Abu Baker, Jalelah. "Exemption of Government from being sued under POHA amendments a 'glaring omission': Pritam Singh." *Channel News Asia,* May 7, 2019. https://www.channelnewsasia.com/news/singapore/exemption-government-sued-under-poha-amendments-pritam-singh-11511118

Abu Baker, Jalelah. "Tan Wu Meng's opinion piece on Pritam Singh was 'serious' and 'thoughtful': Shanmugam." *Channel News Asia,* June 21, 2020. https://www.channelnewsasia.com/news/singapore/tan-wu-meng-pritam-singh-aflian-shanmugam-12856406

Academics Against Misinformation. "POFMA: Letter to Education Minister." Published April 11, 2019. http://www.academia.sg/pofma-letter/

Academics Against Misinformation. "POFMA: Media release." Published April 14, 2019. http://www.academia.sg/pofma-media-release/

Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act). Bundestag. July 12, 2017. https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

Al Jazeera. "Indonesia passes controversial anti-terror laws to fight ISIL." May 26, 2018. https://www.aljazeera.com/news/2018/05/indonesia-passes-controversial-anti-terror-laws-fight-isil-180525055635674.html

Amnesty International. "Open letter on the increasing use of makar charges against Papuan activists to stifle freedom of expression." Published October 2, 2019. https://www.amnesty.id/open-letter-on-the-increasing-use-of-makar-charges-against-papuan-activists-to-stifle-freedom-of-expression/

Aravindan, Aradhana. "Google says Singapore's fake news law could hamper innovation." *Reuters,* May 9, 2019. https://www.reuters.com/article/us-singapore-politics-google/google-says-singapores-fake-news-law-could-hamper-innovation-idUSKCN1SF08X

Aris, Kieren and Rachel Fielden. "Tackling online disinformation in Indonesia through media literacy: The redirect method." Paper presented at Fake News and Elections in Asia Conference. Bangkok, Thailand, 10-12 July, 2019. Accessed November 13, 2020, https://asiacentre.org/wp-content/uploads/2019/09/Fake-News-Conference-Proceeding.pdf

Article 19 and Aliansi Jurnalis Independen. *Freedom of Expression and the Media in Indonesia.* London and Jakarta: Article 19 and Aliansi Jurnalis Independen, 2005. https://www.refworld.org/pdfid/4754185f0.pdf

ASEAN Parliamentarians for Human Rights. "Singapore: Amend the 'fake news' bill." Published May 7, 2019. https://aseanmp.org/2019/05/07/singapore-fake-news-bill/?fbclid=IwAR114nescHaE8VQ5NDYlV8YxxTcKi_6ogBLXROZFR-8C5Uf5OnwCVjePQZ8.

Association of Women for Action and Research. *No new restrictions needed: AWARE submission to Select Committee on Deliberate Online Falsehoods.* Association of Women for Action and Research, 2018. http://d2t1lspzrjtif2.cloudfront.net/wp-content/uploads/AWARE-submission-to-Select-Committee-on-Deliberate-Online-Falsehoods-1.pdf.

Au Waipang, Alex. "Singapore bloggers wary of news site licence scheme." Committee to Protect Journalists. Published June 4, 2013. https://cpj.org/2013/06/singapores-news-site-license-plan-raises-questions/

Australian Communications and Media Authority. *Misinformation and News Quality on Digital Platforms in Australia: A Position Paper to Guide Code Development.* Canberra: ACMA, 2020. https://www.acma.gov.au/sites/default/files/2020-06/Misinformation%20and%20news%20quality%20position%20paper.pdf

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

Australian Government. *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry.* Canberra: Commonwealth of Australia, 2019. https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf

Barthel, Michael, Amy Mitchell and Jesse Holcomb. "Many Americans believe fake news is sowing confusion." Pew Research Centre. Published December 15, 2016. https://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/

BBC. "Singapore ruling PAP party wins elections, but support falls." July 10, 2020. https://www.bbc.com/news/world-asia-53358650

Bertrand, Jacques. *Nationalism and Ethnic Conflict in Indonesia.* Cambridge: Cambridge University Press, 2003. DOI:10.1017/CBO9780511559341

Bhwana, Petir Garda. "Ahok reflects on never becoming a government official again." *Tempo,* October 22, 2019. https://en.tempo.co/read/1262677/ahok-reflects-on-never-becoming-a-government-official-again

Bhwana, Petir Garda. "Coronavirus-crackdown aimed at anti-President smears, hoaxes." *Tempo*, April 6, 2020. https://en.tempo.co/read/1328272/coronavirus-crackdown-aimed-at-anti-president-smears-hoaxes

Board, Jack. "Inside Indonesia's 'fake news' war room, fighting political hoaxes in election season." *Channel News Asia*, April 13, 2019. https://www.channelnewsasia.com/news/asia/indonesia-election-fake-news-war-room-fighting-political-hoaxes-11439398

Bothwell, Ellie. "Fake news laws may 'catch on' during coronavirus." Times Higher Education. Published April 6, 2020. https://www.timeshighereducation.com/news/fake-news-laws-may-catch-during-coronavirus

Bowie, Nile. "The changing face of Singapore democracy." *Asia Times*. September 10, 2020. https://asiatimes.com/2020/09/the-changing-face-of-singapore-democracy/

Britannica. "Pancasila." Accessed August 20, 2020. https://www.britannica.com/topic/Pancasila.

Bruns, Axel, Stephen Harrington, and Edward Hurcombe. "'Corona? 5G? Or Both?': The dynamics of COVID-19/5G conspiracy theories on Facebook." *Media International Australia* 177, no. 1 (November 2020): 12–29. https://doi.org/10.1177/1329878X20946113.

Butt, Simon. "Why is Ahok in prison? A legal analysis of the decision." *Indonesia at Melbourne,* June 6, 2017. https://indonesiaatmelbourne.unimelb.edu.au/why-is-ahok-in-prison-a-legal-analysis-of-the-decision/

Carson, Andrea. *Investigative Journalism, Democracy and the Digital Age*. New York: Routledge, 2020.

Central Intelligence Agency. "The world factbook: Indonesia." Accessed August 19, 2020. https://www.cia.gov/library/publications/the-world-factbook/geos/id.html

Chairil, Tangguh. "Indonesia's intelligence service is coming out to counter COVID-19." *The Diplomat,* June 19, 2020. https://thediplomat.com/2020/06/indonesias-intelligence-service-is-coming-out-to-counter-covid-19/

Chang, Nicole. "Judge dismisses The Online Citizen's POFMA challenge." *Channel News Asia,* February 19, 2020. https://www.channelnewsasia.com/news/singapore/the-online-citizen-toc-pofma-challenge-appeal-dismiss-12449826

Charlton, Emma. "How Finland is fighting fake news – in the classroom." World Economic Forum. Published May 21, 2019. https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom/

Chauvel, Richard and Ikrar Nusa Bhakti. *The Papua Conflict: Jakarta's Perceptions and Policies*. Washington, D.C: East-West Center Washington, Policy Studies 5, 2004.

Chen, Siyuan and Chia Chen Wei. "Singapore's latest efforts at regulating online hate speech." *Research Collection School of Law* (2019): n.p. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4879&context=sol_research

Chew, Amy. "'Chinese army uniforms' in Indonesia: Another hoax to discredit Beijing, Widodo." *South China Morning Post*, July 29, 2020. https://www.scmp.com/week-asia/politics/article/3095217/chinese-army-uniforms-indonesia-another-hoax-discredit-beijing

Coconuts Jakarta. "Indonesian gov't justifies maintaining internet block in Papua despite officials declaring security restored." August 28, 2019. https://coconuts.co/jakarta/news/indonesian-govt-justifies-maintaining-internet-block-in-papua-despite-officials-declaring-security-restored/

Coconuts Jakarta. "RKUHP Explainer: All the controversial articles in Indonesia's criminal code overhaul." September 19, 2019. https://coconuts.co/bali/features/rkuhp-explainer-all-the-controversial-articles-in-indonesias-criminal-code-overhaul-2/

Coconuts Jakarta. "Senior Indonesian minister suggests anti-terrorism law be used against election hoax spreaders." March 21, 2019. https://coconuts.co/jakarta/news/senior-indonesian-minister-suggest-anti-terrorism-law-used-election-hoax-spreaders/

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

Committee to Protect Journalists. "Singaporean authorities shut down *The Real Singapore* news website." Published May 5, 2015. https://cpj.org/2015/05/singaporean-authorities-shut-down-the-real-singapo/

Courthouse News Service. "Hundreds arrested for 'fake news' in Asia." April 10, 2020. https://www.courthousenews.com/asia-arrests-hundreds-for-fake-news-on-virus/.

Criminal Code [KUHP] (Indonesia). Government of Indonesia, 1946. https://www.unodc.org/res/cld/document/idn/indonesian_penal_code_html/I.1_Criminal_Code.pdf

Crowther, Craig. "Viktor Orban and Hungarian Government poised to give up unrestrained powers." *Euronews,* May 27, 2020. https://www.euronews.com/2020/05/26/viktor-orban-and-hungarian-government-poised-to-give-up-unrestrained-powers

Dahlgren, Paul. "Media, knowledge and trust: The deepening epistemic crisis of democracy." *Journal of the European Institute for Communication and Culture* 25, no. 1-2 (2018): 20-27. DOI: 10.1080/13183222.2018.1418819

Daskal, Jennifer. "This 'fake news' law threatens free speech. But it doesn't stop there." *New York Times,,* May 30, 2019. https://www.nytimes.com/2019/05/30/opinion/hate-speech-law-singapore.html

DDCMS. *The Cairncross Review: A Sustainable Future for Journalism*. London: Department for Digital, Culture, Media & Sport, February 12, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf

Defamation Act (Singapore). Parliament of Singapore, 1965. https://sso.agc.gov.sg/Act/DA1957

Digital Industry Group Inc. *Australian Code of Practice on Disinformation: Draft for Public Consultation.* DIGI, October 16, 2020. https://digi.org.au/wp-content/uploads/2020/10/Disinformation-Code-draft-for-public-consultaion-.pdf

Dittrich, Paul-Jasper. *Tackling the Spread of Disinformation: Why a Co-regulatory Approach is the Right Way Forward for the EU.* Berlin: Jacques Delors Centre, December 12, 2019. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/ GrauePublikationen/EZ_JDI_BST_Policy_Paper_Disinformation_Dittrich_2019_ENG.pdf.

Draft Revised Criminal Code [RKUHP] (Indonesia). Government of Indonesia, 2019. https://www.hukumonline.com/pusatdata/detail/17797/rancangan-undang-undang-2019#

Drake, Christine. *National Integration in Indonesia: Patterns and Policies.* Honolulu: University of Hawaii Press, 2019.

Dursin, Kanis. "Hoax stories hamper Indonesia's COVID-19 fight." *Bangkok Post*, July 6, 2020 https://www.bangkokpost.com/opinion/opinion/1946480/hoax-stories-hamper-indonesias-covid-19-fight

East StratCom Task Force. *Action Plan on Strategic Communication.* Brussels: European Commission, June 22, 2015. http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf

Eddyono, Supriyadi Widodo, Zainal Abidin, Arsil and Emerson Yuntho. *Brief Notes on the Proposed Discussion of 2015 Criminal Code Bill.* National Alliance for Criminal Code Reform, March 26, 2015. https://elsam.or.id/wp-content/uploads/2015/08/Brief-Notes-on-the-Proposed-Discussion-of-2015-Criminal-Code-Bill.pdf

Elections Department Singapore. "Parliamentary elections." Accessed November 13, 2020. https://www.eld.gov.sg/elections_parliamentary.html

European Commission. "A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council." Published June 14, 2019. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2914

European Commission. "First baseline reports – Fighting COVID-19 disinformation monitoring program." Published September 10, 2020. https://ec.europa.eu/digital-single-market/en/news/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme.

European Commission. "Protecting European democracy from interference and manipulation – European Democracy Action Plan." Accessed November 19, 2020. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12506-European-Democracy-Action-Plan

European Commission. "The Digital Services Act package." Last updated June 22, 2020. https://ec.europa.eu/digital-single-market/en/digital-services-act-package

European Commission. *Action Plan against Disinformation.* Brussels: European Commission, December 5, 2018 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0036&qid=1583456906698&from=EN

European Commission. *Assessment of the Code of Practice on Disinformation – Achievements and Areas for Further Improvement.* Brussels: European Commission, September 10, 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212

European Commission. *Code of Practice on Disinformation: First Annual Reports.* Brussels: European Commission, October 2019. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62698.

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

European Commission. *Joint Framework on Countering Hybrid Threats*. Brussels: European Commission, April 6, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

European Commission. *Joint Framework on Countering Hybrid Threats from July 2017 to June 2018.* Brussels: European Union, June 13, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0014&from=EN.

European Commission. *Report on the Implementation of the Action Plan against Disinformation.* Brussels: European Commission, June 14, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

European Commission. *Tackling COVID-19 Disinformation – Getting the Facts Right.* Brussels: European Commission, June 10, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0008&from=EN

European Commission. *Tackling Online Disinformation: A European Approach.* Brussels: European Commission, April 26, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&qid=1583456906698&from=EN

European Committee of the Regions. *Opinion of the European Committee of the Regions on "Tackling Online Disinformation: A European Approach".* Brussels: Official Journal of the European Union, May 16, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018IR3908&qid=1583456906698&from=EN

European Council. *European Council Meeting (19 and 20 March 2015) – Conclusions.* Brussels: European Council, March 20, 2015. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

European Court of Human Rights. *European Convention on Human Rights.* Brussels: European Court of Human Rights, 2010. https://www.echr.coe.int/Documents/Convention_ENG.pdf

European Economic and Social Committee. *Opinion on Action Plan against Disinformation.* Brussels: European Commission, March 20, 2019. https://webapi2016.eesc.europa.eu/v1/documents/EESC-2018-06302-00-00-AC-TRA-EN.docx/content

European Parliament and the Council. *Directive (EU) 2018/1808 of the European Parliament and of the Council.* Brussels: European Parliament, November 14, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN

European Parliament. *Charter of Fundamental Human Rights of the European Union (2000/c 364/01).* Brussels: European Parliament, December 18, 2000. https://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Regulators Group for Audiovisual Media Services. *ERGA Report on Disinformation: Assessment of the Implementation of the Code of Practice.* Brussels: European Commission, May 2020. https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf

European Union External Action Service. "Questions and Answers about the East StratCom Task Force." Published December 5, 2018. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en

EUvsDisinfo. "About." Accessed November 17, 2020. https://euvsdisinfo.eu/about/

EUvsDisinfo. "Removal of three cases further to complaints by Dutch media." Published March 8, 2018. https://euvsdisinfo.eu/removal-of-three-cases-further-to-complaints-by-dutch-media/

Fathurohman, Irfan. "ICJR urges parliament and government to not need to hurry to pass the Criminal Code bill." IDNTimes. Published July 11, 2020. https://www.idntimes.com/news/indonesia/irfanfathurohman/icjr-desak-pemerintah-dpr-tidak-buru-buru-sahkan-ruu-kuhp/4

Fiorentino, Michael-Ross. "France passes controversial 'fake news' law." *Euronews,* May 9, 2019. https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law

Fisher, Caroline. "Australia." In *Reuters Institute Digital News Report 2019,* edited by Nic Newman, Richard Fletcher, Antonis Kalogeropoulos and Rasmus Kleis Nielsen, 132-133. Oxford: Reuters Institute for the Study of Journalism, 2019. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/inline-files/DNR_2019_FINAL.pdf

Foreign Correspondents Association of Singapore. "The Foreign Correspondents Association of Singapore is deeply concerned about the Singapore government's passing of a bill…" Facebook. May 9, 2019. https://www.facebook.com/FCASG.org/posts/2358487210882553

Formichi, Chiara. "Violence, sectarianism, and the politics or religion: Articulations of anti-Shi'a discourses in Indonesia." *Indonesia,* no. 98 (2014): 1-27.

FORUM-ASIA. "Singapore: Use of anti-fake news law reveals institutional framework that undermines the promotion and protection of human rights." Published February 11, 2020. https://www.forum-asia.org/?p=30931

Francois, Camille. *Actors, Behaviours, Content: A Disinformation ABC: Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses.* The Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, September 20, 2019. https://science.house.gov/imo/media/doc/Francois%20Addendum%20to%20Testimony%20-%20ABC_Framework_2019_Sept_2019.pdf

Freedom House. "Freedom in the World 2020: Indonesia." Accessed November 13, 2020. https://freedomhouse.org/country/indonesia/freedom-world/2020

Freedom House. "Freedom on the Net 2019: Indonesia." Accessed November 13, 2020. https://freedomhouse.org/country/indonesia/freedom-net/2019

Freedom House. "Freedom on the Net 2020: Australia." Accessed November 20, 2020. https://freedomhouse.org/country/australia/freedom-net/2020#C

Freedom House. *Freedom of the Press 2017.* Freedom House, 2017. https://freedomhouse.org/report/freedom-press/freedom-press-2017

Freedom House. *Freedom on the Net 2016.* Freedom House, 2016. https://freedomhouse.org/sites/default/files/2020-02/Freedom_on_the_Net_2016_complete_book.pdf

Freedom House. *Freedom on the Net 2017: Indonesia.* Freedom House, 2017. https://www.justice.gov/eoir/page/file/1026001/download

Freedom House. *Special Report 2018: Attacks on the Record – The State of Global Press Freedom, 2017-2018.* Freedom House, 2018. https://freedomhouse.org/report/special-report/2018/attacks-record.

Freischlad, Nadine. "Controversial 'right to be forgotten' finds its way into Indonesian law." Tech in Asia. Published December 1, 2016. https://www.techinasia.com/indonesia-recognizes-right-to-be-forgotten

Function 8. "Submission to the Parliamentary Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures." Facebook. February 28, 2018. ttps://m.facebook.com/story.php?story_fbid=911516705691971&id=350013055175675

Funke, Daniel and Daniela Flamini. "A guide to anti-misinformation actions around the world." Poynter. Accessed November 14, 2020. https://www.poynter.org/ifcn/anti-misinformation-actions/#indonesia

Funke, Daniel. "Italians can now report fake news to the police. Here's why that's problematic." Poynter. Published January 19, 2018. https://www.poynter.org/fact-checking/2018/italians-can-now-report-fake-news-to-the-police-heres-why-thats-problematic/

Funke, Daniel. "Three publications are suing the EU over fake news allegations." Poynter. Published February 28, 2018 https://www.poynter.org/fact-checking/2018/three-publications-are-suing-the-eu-over-fake-news-allegations/

George, Cherian. "Online falsehoods bill: Will words in legislation mean whatever S'pore govt chooses them to mean?" Mothership. Published April 6, 2019. https://mothership.sg/2019/04/online-falsehoods-cherian-george/

Guillaume, Marine. *Combating the Manipulation of Information – A French Case.* Helsinki: Hybrid CoE, 2019. https://www.hybridcoe.fi/wp-content/uploads/2019/05/HybridCoE_SA_Combating-the-manipulation-of-information.pdf

Gunawan, Budi and Barito Mulyo Ratmono. "Social media, cyberhoaxes and national security: Threats and protection in Indonesian cyberspace." *International Journal of Network Security* 22, no 1. (2020): 93-101.

Gunia, Amy. "Singapore's prime minister threatens website editor with libel." *Time,* September 2, 2019. https://time.com/5666835/singapore-prime-minister-lee-hsien-loong-libel/

Hamid, Usman. "Indonesia's Information Law has threatened free speech for more than a decade. This must stop." *The Conversation,* November 25, 2019. https://theconversation.com/indonesias-information-law-has-threatened-free-speech-for-more-than-a-decade-this-must-stop-127446

Han, Kirsten. "Big Brother's regional ripple effect." *Index on Censorship* 48, no. 2 (2019): 67–69.

Han, Kirsten. "Coronavirus: How effective is Singapore's anti-fake news law?" *The News Lens*, April 8, 2020. https://international.thenewslens.com/article/133521.

Han, Kirsten. "WTC Long Read: A mother's concerns in a time of POFMA." We The Citizens. Published November 9, 2020. https://wethecitizens.substack.com/p/wtc-long-read-a-mothers-concerns

Harsono, Andreas. "Indonesia's journalists grapple with Islamism." Human Rights Watch. Published August 21, 2019 https://www.hrw.org/news/2019/08/21/indonesias-journalists-grapple-islamism

Harsono, Andreas. "Indonesia's president urges delay on Criminal Code vote." Human Rights Watch. Published September 23, 2019. https://www.hrw.org/news/2019/09/23/indonesias-president-urges-delay-criminal-code-vote

Hasani, Ismail. "The decreasing space for non-religious expression in Indonesia." In *Religion, Law and Intolerance in Indonesia*, edited by Tim Lindsey and Helen Pausacker, Chapter 9. London and New York: Routledge, 2016.

Hatta, Muhammad. "The spread of hoaxes and its legal consequences." *International Journal of Psychosocial Rehabilitation* 24, no. 3, (2020): 1750-1760.

Howe, Lee Kay. "True or false or misleading: [A]dequate judicial oversight over Part 3 directions under the Protection from Online Falsehoods and Manipulation Act." *Singapore Comparative Law Review*, (2019): 239-247.

Human Rights Watch. "Indonesia: Repeal new intelligence law." Published October 26, 2011. https://www.hrw.org/news/2011/10/26/indonesia-repeal-new-intelligence-law

Human Rights Watch. *Kill the Chicken to Scare the Monkeys: Suppression of Free Expression and Assembly in Singapore.* Human Rights Watch, 2017. https://www.hrw.org/sites/default/files/report_pdf/singapore1217_web.pdf

Human Rights Watch. *World Report 2020*. Human Rights Watch, 2020. https://www.hrw.org/sites/default/files/world_report_download/hrw_world_report_2020_0.pdf

Indonesia at Melbourne. "Indonesians better get ready for jail, as flawed new criminal code looks set to pass." Published September 3, 2019. https://indonesiaatmelbourne.unimelb.edu.au/indonesians-better-get-ready-for-jail-as-flawed-new-criminal-code-looks-set-to-pass/

Infocomm Media Development Authority. "Fact sheet – Online news sites to be placed on a more consistent licensing framework as traditional news platforms." Last updated June 10, 2019. https://www.imda.gov.sg/news-and-events/Media-Room/archived/mda/Media-Releases/2013/fact-sheet--online-news-sites-to-be-placed-on-a-more-consistent-licensing-framework-as-traditional-news-platforms

Infocomm Media Development Authority. *Internet Code of Practice.* Infocomm Media Development Authority, 1997. https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/Regulations/Codes-of-Practice/Codes-of-Practice-Media/PoliciesandContentGuidelinesInternetInterneCodeOfPractice.pdf

International Commission of Jurists. "Singapore: Parliament must reject internet regulation bill that threatens freedom of expression." Published April 4, 2019. https://www.icj.org/wp-content/uploads/2019/04/Singapore-fake-news-bill-News-web-story-2019-ENG.pdf

Ismail, Saifulbahri. "ASEAN lawmakers urge Indonesia to reject changes to criminal code." *Channel News Asia,* February 7, 2018. https://www.channelnewsasia.com/news/asia/asean-lawmakers-urge-indonesia-to-reject-changes-to-criminal-9935950

Jakarta Globe. "BIN budget cuts to jeopardise regional election security, says spy chief." September 10, 2015. https://jakartaglobe.id/context/bin-budget-cuts-jeopardize-regional-election-security-says-spy-chief/

Jankowicz, Nina. *Avoiding the Band-Aid Effect in Institutional Responses to Disinformation and Hybrid Threats.* Washington D.C.: The German Marshal Fund, August 12, 2019. https://www.gmfus.org/sites/default/files/publications/pdf/Jankowicz%20-%20Bandaid%20Effect%20paper.pdf

Jayakumar, Shashi, Benjamin Ang and Nur Diyanah Anwar. *Disinformation and Fake News.* Singapore: Palgrave MacMillan, 2021.

"Joint statement regarding the Protection from Online Falsehoods and Manipulation Bill [Joint statement from arts and civil society organisations]." Accessed November 20, 2020. https://docs.google.com/document/d/1yNCUHvJBOkZG_WbNt1W_8BAxzHKIjIBK1EJbMLu9Rr8/edit?fbclid=IwAR1Vu0C-CVkZbZlM7FiRdOcJiWLqWfSAYjXkdscE_1Ou6k5QMvDlElXh7bQ.

"Journalists Call for withdrawal of Singapore's 'fake news' Bill [letter to Minister of Communications and Information S Iswaran]." Published April 24, 2019. URL:https://docs.google.com/document/d/16pVee1fGx9cU6qADARrgfTtcV60-tVFpm46UGF1-j0o/edit.

Kaye, David. *Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. United Nations, 2019. https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_SGP_3_2019.pdf

Koh, Valerie. "Govt orders shutdown of *The Real Singapore*." *Today Online*, May 4, 2015. https://www.todayonline.com/singapore/mda-suspends-licence-socio-political-website-real-singapore

Krisetya, Beltsazar A. "COVID-19 exposes vulnerabilities in our cyberspace." *The Jakarta Post,* April 1, 2020. https://www.thejakartapost.com/academia/2020/04/01/covid-19-exposes-vulnerabilities-in-our-cyberspace.html

Kurohi, Rei. "Singapore GE2020: WP's Raeesah Khan apologises for posts which allegedly promoted enmity between different groups." *The Straits Times.* Updated September 1, 2020. https://www.straitstimes.com/politics/singapore-ge2020-wps-raeesah-khan-apologises-for-posts-which-allegedly-promoted-enmity

Kurnia, Novi and Astuti. "Researchers find Indonesia needs more digital literacy education." *The Conversation*, September 26, 2017. https://theconversation.com/researchers-find-indonesia-needs-more-digital-literacy-education-84570

La Batu, Safrin. "Nine social media, messaging apps agree to combat fake news." *The Jakarta Post*, January 31, 2018. https://www.thejakartapost.com/news/2018/01/31/nine-social-media-messaging-apps-agree-to-combat-fake-news.html

La Cour, Christina. "Governments countering disinformation: The case of Italy." Disinfo Portal. Accessed November 19, 2020. https://disinfoportal.org/governments-countering-disinformation-the-case-of-italy/

Lam, Lydia. "Judge dismisses SDP's POFMA challenge, says statements were false in face of statistical evidence." *Channel News Asia,* February 5, 2020. https://www.channelnewsasia.com/news/singapore/judge-dismisses-sdp-s-pofma-challenge-says-statements-were-false-12394932?cid=h3_referral_inarticlelinks_24082018_cna

Lam, Lydia. "PM Lee sues blogger Leong Sze Hian for defamation over sharing of article." *Channel News Asia,* December 7, 2018. https://www.channelnewsasia.com/news/singapore/pm-lee-sues-blogger-leong-sze-hian-defamation-libellous-article-10999710

Lamb, Kate. "Indonesian government to hold weekly 'fake news' briefings." *The Guardian*, September 27, 2018. https://www.theguardian.com/world/2018/sep/27/indonesian-government-to-hold-weekly-fake-news-briefings

Lamb, Kate. "Muslim Cyber Army: A 'fake news' operation designed to derail Indonesia's leader." *The Guardian*, March 13, 2018. https://www.theguardian.com/world/2018/mar/13/muslim-cyber-army-a-fake-news-operation-designed-to-bring-down-indonesias-leader.

Lamb, Kate. "Outcry as Indonesia seeks to arrest renowned West Papua rights lawyer." *The Guardian*, September 5, 2019. https://www.theguardian.com/world/2019/sep/05/outcry-as-indonesia-seeks-to-arrest-renowned-west-papua-rights-lawyer

Lamb, Kate. "Sulawesi tsunami: Indonesia battles fake news as hoaxers spread panic." *The Guardian*, October 4, 2018. https://www.theguardian.com/world/2018/oct/04/sulawesi-tsunami-indonesia-battles-fake-news-as-hoaxers-spread-panic

Law No. 11 of 2008 on Information and Electronic Transactions [UU ITE] (Indonesia), 2008 [revised 2016]. Accessed November 13, 2020. https://www.hukumonline.com/pusatdata/detail/lt584a7363785c8/node/lt56b97e5c627c5/uu-no-19-tahun-2016-perubahan-atas-undang-undang-nomor-11-tahun-2008-tentang-informasi-dan-transaksi-elektronik

Law No. 17 of 2011 on State Intelligence (Indonesia). Accessed November 13, 2020 https://www.icj.org/wp-content/uploads/2011/01/Indonesia-intelligence-law-draft-2011-eng.pdf

Law No. 40 of 2008 on Elimination of Racial and Ethnic Discrimination (Indonesia): 2008. Accessed November 13, 2020. https://www.hukumonline.com/pusatdata/detail/28539/node/1011/uu-no-40-tahun-2008-penghapusan-diskriminasi-ras-dan-etnis

Lee, Howard and Terence Lee. "From contempt of court to fake news: public legitimisation and governance in mediated Singapore." *Media International Australia* 173, no. 1 (2019): 81-92.

Lee, Howard and Terence Lee. "Polarising dissent: The constructed narrative of Singapore's new 'fake news' law." *The Asia Dialogue,* June 10, 2019. https://theasiadialogue.com/2019/06/10/polarising-dissent-the-constructed-narrative-of-singapores-new-fake-news-law/

Lee, Pearl. "TRS co-founder Yang Kaiheng jailed 8 months for sedition." *The Straits Times,* June 28, 2016. https://www.straitstimes.com/singapore/courts-crime/trs-co-founder-yang-kaiheng-jailed-8-months-for-sedition.

Lee, Tse Yin. "Analysis: How effective was Indonesia's war on fake news in its election?" *BBC Monitoring*, May 16, 2019. https://monitoring.bbc.co.uk/product/c200tf1l

Lee, Vernon. "Fake news law is ploy by government to hold on to 'absolute power': Workers' Party MP Low Thia Khiang." *Yahoo News Singapore,* May 8, 2019. https://sg.news.yahoo.com/fake-news-law-is-ploy-by-government-to-hold-absolute-power-low-thia-khiang-155910029.html

Library of Congress. "Laws protecting journalists from online harassment: Singapore." Accessed November 20, 2020, https://www.loc.gov/law/help/protecting-journalists/singapore.php

Lim, Adrian. "Parliament: Fake news law covers closed platforms like chat groups and social media groups, says Edwin Tong." *The Straits Times.* May 7, 2019. https://www.straitstimes.com/politics/parliament-fake-news-law-covers-closed-platforms-like-chat-groups-and-social-media-groups

Llewellyn, Aisyah. "Punitive measures: Indonesia's new draft criminal code." Lowy Institute. Published February 9, 2018. https://www.lowyinstitute.org/the-interpreter/punitive-measures-indonesias-new-draft-criminal-code

Lomas, Natasha. "TikTok joins the EU's Code of Practice on Disinformation." *TechCrunch,* June 22, 2020. https://techcrunch.com/2020/06/22/tiktok-joins-the-eus-code-of-practice-on-disinformation/

Luger, Jason. "Planetary illiberalism and the cybercity-state: in and beyond territory." *Territory, Politics, Governance* 8, no. 1 (2020): 1-17. DOI: 10.1080/21622671.2019.1627906

Lukman, Enricko. "How Indonesia's problematic internet law will impede freedom of expression." SAFEnet. Published September 10, 2014. https://safenet.or.id/2014/09/how-indonesias-problematic-internet-law-will-impede-freedom-of-expression/

Macron, Emmanuel, Gitanas Nauseda and Arturs Krisjanis Karins. *Joint Statement by the Presidents of France And Lithuania, and Prime Minister of Latvia on Protection of Democracies.* Paris: Palais de l'Elysee, September 28, 2020. https://static.lsm.lv/documents/z5.pdf

MAFINDO. "About." Accessed August 10, 2020. https://www.mafindo.or.id/about/

Mahtani, Shibani. "Singapore introduced tough laws against fake news. Coronavirus has put them to the test." *Washington Post,* March 16, 2020. https://www.washingtonpost.com/world/asia_pacific/exploiting-fake-news-laws-singapore-targets-tech-firms-over-coronavirus-falsehoods/2020/03/16/a49d6aa0-5f8f-11ea-ac50-18701e14e06d_story.html

Marsden, Chris, Trisha Meyer, and Ian Brown. "Platform values and democratic elections: How can the law regulate digital disinformation?" *Computer Law and Security Review* 36, (2020): 1-18.

Mchangama, Jacob and Joelle Fiss. *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Citizenship.* Copenhagen: Justitia, November 2019. https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf

Meese, James and Edward Hurcombe. *Regulating Misinformation: Policy Brief.* Melbourne: RMIT University, November 12, 2020. https://apo.org.au/sites/default/files/resource-files/2020-11/apo-nid309357.pdf

Meyer, Paul. "Singapore's first election under the fake news law." *The Diplomat,* July 7, 2020. https://thediplomat.com/2020/07/singapores-first-election-under-the-fake-news-law/

Mid-Day. "Indonesian man arrested for Facebook post allegedly insulting Islam." Published May 1, 2018 https://www.mid-day.com/articles/indonesian-man-arrested-for-facebook-post-allegedly-insulting-islam/19374167

Ministry of Communications and Information and Ministry of Law. *Deliberate and Online Falsehoods: Challenges and Implications.* Singapore: Parliament of Singapore, 2018. https://www.nas.gov.sg/archivesonline/government_records/Flipviewer/grid_publish/6/6797717d-f25b-11e7-bafc-001a4a5ba61b-06012018Misc.10of2018/web/html5/index.html?launchlogo=tablet/GovernmentRecords_brandingLogo_.png&pn=1

Ministry of Communications and Information. "The 'Singapore States Times' and Alex Tan's Facebook pages declared as declared online locations under POFMA." Published May 6, 2020. https://www.pofmaoffice.gov.sg/documents/media-releases/2020/May/pofma-pr-mci-06may2020-01.pdf

Ministry of Health and Ministry of Manpower. "Joint MOM-MOH statement on the issuance of correction directions under the Protection from Online Falsehoods and Manipulation Act (POFMA) against National University of Singapore Society (NUSS), The Online Citizen Asia (TOC), CNA and *New Naratif*." POFMA Office. Published July 5, 2020 https://www.pofmaoffice.gov.sg/documents/media-releases/2020/July/pofma-pr-mom-05jul2020-01.pdf

Ministry of Law. *Enhancements to the Protection from Online Harassment Act ('POHA').* Singapore: Ministry of Law, April 1, 2019. https://www.mlaw.gov.sg/news/press-releases/enhancements-to-the-protection-from-harassment-act-poha

National Library of Singapore. "Combating fake news." Last updated October 29, 2020. https://sure.nlb.gov.sg/resources/audience/adults/combating-fake-news

Nenadic, Iva. "Unpacking the 'European approach' to tackling challenges of disinformation and political manipulation." *Internet Policy Review* 8, no. 4 (2019): 1-22.

Neo, Ric. "The securitisation of fake news in Singapore." *International Politics* 57 (2019): 724-740. DOI:10.1057/s41311-019-00198-4.

Neubronner, Stephanie. "Bill to protect from online falsehoods: Refinements needed." *RSIS Commentary* 85, (April 30, 2019): n.p.

New Mandala. "Q&A: Sandiaga Uno on economic policy." Published March 4, 2019. https://www.newmandala.org/qa-sandiaga-uno-on-economic-policy/

Nijeboer, Arjen. "Why the EU must close EUvsDisinfo." *Euobserver,* March 27, 2018. https://euobserver.com/opinion/141458

NL Times. "Dutch Government to launch anti-fake news campaign." December 13, 2018. https://nltimes.nl/2018/12/13/dutch-government-launch-anti-fake-news-campaign

Novak, Benjamin. "Hungary moves to end rule by decree, but Orban's powers may stay." *New York Times,* June 16, 2020. https://www.nytimes.com/2020/06/16/world/europe/hungary-coronavirus-orban.html

Nugroho, Agung. "Comparative study on hoax handling policies in Indonesia and Singapore." *Advances in Social Science, Education and Humanities Research* 343, (2019): 358-363.

Nugroho, Fiska Maulidian. "Study of fake news dissemination articles on Criminal Code regulations, Law of Information and Electronic Technology, and also Law of Terrorism Criminal Act eradication." Paper presented at Fake News and Elections in Asia Conference, Bangkok, Thailand, July 10-12, 2019. Accessed November 13, 2020. https://asiacentre.org/wp-content/uploads/2019/09/Fake-News-Conference-Proceeding.pdf

Nurita, Dewi. "Fadli Zon urge National Cyber Agency hit the brake." *Tempo,* January 8, 2018. https://en.tempo.co/read/914656/fadli-zon-urge-national-cyber-agency-hit-the-brake

Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation. "National political stability under control: Home ministry." Cabinet Secretariat of the Republic of Indonesia. Published September 26, 2019. https://setkab.go.id/en/national-political-stability-under-control-home-ministry/

Oktavianti, Tri Indah. "National Police detail tightened measures to combat COVID-19, support government policy." *The Jakarta Post*, April 8, 2020. https://www.thejakartapost.com/news/2020/04/08/national-police-detail-tightened-measures-to-combat-covid-19-support-government-policy.html

Ong, Benjamin Joshua. "Looking beyond the vague terms in Singapore's fake news laws." *TodayOnline*, May 14, 2019. https://www.todayonline.com/commentary/looking-beyond-vague-terms-fake-news-laws

Ong, Benjamin Joshua. "Symposium on POFMA: Parliamentary debates about POFMA – Hansard beyond statutory interpretation?" *Research Collection School of Law* (November 2019): 1-5. https://ink.library.smu.edu.sg/sol_research/2968

Pamment, James. *The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission.* Washington: Carnegie Endowment for International Peace, March 2020. https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187.

Pamment, James. *The EU's Role in Fighting Disinformation: Taking Back the Initiative*. Washington: Carnegie Endowment for International Peace, June 2020. https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf.

Parliament of Singapore. "Members of parliament." Accessed November 13, 2020. https://www.parliament.gov.sg/about-us/structure/members-of-parliament

Parliament of Singapore. "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill." Published May 8, 2019. Vol. 94, Part 1. https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-366

Parliament of Singapore. "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill." Published May 8, 2019. Vol. 94, Part 2. https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-367

Parliament of Singapore. *Report of the Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures*. Singapore: Parliament of Singapore, 2018. https://sprs.parl.gov.sg/selectcommittee/selectcommittee/download?id=1&type=subReport

Parlina, Ina. "Jokowi declares fight against disseminators of fake news." *The Jakarta Post*, December 30, 2016. https://www.thejakartapost.com/news/2016/12/30/jokowi-declares-fight-against-disseminators-of-fake-news.html

Pausacker, Helen. "Ahok: Loved and hated governor of Jakarta." *Indonesia at Melbourne*, August 4, 2015. https://indonesiaatmelbourne.unimelb.edu.au/ahok-loved-and-hated-governor-of-jakarta/

Penal Code (Singapore). Parliament of Singapore. 1972. https://sso.agc.gov.sg/Act/PC1871?ProvIds=pr499-

Potkin, Fanny and Augustinus Beo Da Costa. "Fact-checkers vs. hoax peddlers: A fake news battle ahead of Indonesia's election." *Reuters*, April 11, 2019. https://www.reuters.com/article/us-indonesia-election-fakenews-insight/fact-checkers-vs-hoax-peddlers-a-fake-news-battle-ahead-of-indonesias-election-idUSKCN1RM2ZE

Protection from Online Falsehoods and Manipulation Act (Singapore). Parliament of Singapore. 2019. https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625

Protection from Online Harassment Act (Singapore). Parliament of Singapore. 2014. https://sso.agc.gov.sg/Act/PHA2014

Renaldi, Adi. "Facebook Removed Hundreds of Accounts for Allegedly Spreading Propaganda in Indonesia." *VICE News*, October 10, 2019. https://www.vice.com/en_asia/article/ne8qbq/facebook-removed-hundreds-accounts-spreading-propaganda-indonesia

Renda, Andrea. *The Legal Framework to Address "Fake News": Possible Policy Actions at the EU Level*. Brussels: Policy Department for Economic, Scientific and Quality of Life Policies, June 2018. https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf

Reni, Dewi Savitri and Syarifah Reihana Fakhry. "RKUHP: What it means for criminal justice in Indonesia." SSEK. Published March 3, 2020. https://www.ssek.com/blog/rkuhp-what-it-means-for-criminal-justice-in-indonesia

Reporters Without Borders. "Indonesia used Covid-19 to silence criticism of government." April 16, 2020. https://rsf.org/en/news/indonesia-used-covid-19-silence-criticism-government

Repucci, Sarah. "A leaderless struggle for democracy: Democracy and pluralism are under assault." Freedom House. Accessed November 20, 2020. https://freedomhouse.org/report/freedom-world/2020/leaderless-struggle-democracy

Reuters. "Facebook takes down hundreds of Indonesian accounts linked to fake news syndicate." February 1, 2019. https://www.reuters.com/article/us-facebook-indonesia/facebook-takes-down-hundreds-of-indonesian-accounts-linked-to-fake-news-syndicate-idUSKCN1PQ3JS

Reza, Bhatara Ibnu. "Why strengthening anti-terror laws is not the answer." Indonesia at Melbourne. Published February 1, 2016. https://indonesiaatmelbourne.unimelb.edu.au/why-strengthening-anti-terror-laws-not-the-answer/

Rosen, Jay. "The people formerly known as the audience." In *Participation and Media Production: Critical Reflections on Content Creation*, edited by Nico Carpentier and Benjamin DeCleen, 163-165. Newcastle upon Tyne, UK: Cambridge Scientific Publishers Ltd, 2008.

Rumata, Vience Mutiara and Ashwin Sasongko Sastrosubroto. "Net-attack 2.0: Digital post-truth and its regulatory challenges in Indonesia." *Advances in Social Science, Education and Humanities Research* 165, (2018): 116-120.

SAFEnet. "[Press release] SAFEnet sends Amicus Curiae for the Saiful Mahdi case." Published February 11, 2020. https://id.safenet.or.id/2020/02/rilis-pers-safenet-kirim-amicus-curiae-untuk-kasus-saiful-mahdi/

SAFEnet. "Persoalan UU ITE dan Praktik Pelanggaran Hak Digital di Indonesia." Published November 14, 2019. https://id.safenet.or.id/wp-content/uploads/2019/11/Persoalan-UU-ITE-dan-Pelanggaran-Hak-Digital-SAFEnet-2019.pdf

SAFEnet. "The experts: The Indonesia Ministry of Communication and Informatics and the President violates human rights and state administrative law." Published March 17, 2020. https://safenet.or.id/2020/03/experts-the-ministry-of-communication-and-information-and-the-president-violates-human-rights-and-state-administrative-law/

Samios, Zoe and Lisa Visentin. "ACMA: Tech giants' code to handle fake news fails to meet expectations." *Sydney Morning Herald*, October 26, 2020. https://www.smh.com.au/politics/federal/acma-tech-giants-code-to-handle-fake-news-fails-to-meet-expectations-20201026-p568oq.html.

Saurwein, Florian and Charlotte Spencer-Smith. "Combating disinformation on social media: Multilevel governance and distributed accountability in Europe." *Digital Journalism* 8, no. 6 (2020): 820-841.

Schultheis, Emily. "The Czech Republic's fake news problem." *The Atlantic*, October 21, 2017. https://www.theatlantic.com/international/archive/2017/10/fake-news-in-the-czech-republic/543591/

Sedition Act (Singapore). Parliament of Singapore. 1948. https://sso.agc.gov.sg/Act/SA1948?ProvIds=pr3-.

Serhan, Yasmeen. "Italy scrambles to fight misinformation ahead of its elections." *The Atlantic*, February 24, 2018. https://www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/

Siberkreasi. "About Siberkreasi." Accessed November 13, 2020. https://siberkreasi.id/tentang-siberkreasi/

Sim, Fann. "Workers' Party opposes online falsehoods Bill, says Pritam Singh." *Channel News Asia*, May 7, 2019. https://www.channelnewsasia.com/news/singapore/online-falsehoods-workers-party-opposes-bill-pritam-singh-11511450

Singapore Government. "What is the licensing framework for online news sites all about?" Published June 18, 2013. https://www.gov.sg/article/what-is-the-licensing-framework-for-online-news-sites-all-about

Singapore Legal Advice. "Singapore fake news laws: Guide to POFMA (Protection from Online Falsehoods and Manipulation Act)." Published February 3, 2020. https://singaporelegaladvice.com/law-articles/singapore-fake-news-protection-online-falsehoods-manipulation/

Social Observatory for Disinformation and Media Analysis. "About us." Accessed November 19, 2020. https://www.disinfobservatory.org/about-us/.

Soeriaatmadja, Wahyudi. "Eucalyptus necklace among 'cures' raising alarm in Indonesia." *The Straits Times,* July 10, 2020. https://www.straitstimes.com/asia/se-asia/eucalyptus-necklace-among-cures-raising-alarm-in-indonesia

Soeriaatmadja, Wahyudi. "Man who uploaded controversial video of ex-Jakarta governor Ahok sentenced to jail." *The Straits Times,* November 14, 2017. https://www.straitstimes.com/asia/se-asia/man-who-uploaded-controversial-ahok-video-sentenced-to-jail

Sounding Board. *The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice.* European Commission, September 24, 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54456.

Statista. "Leading countries based on Facebook audience size as of July 2020." Published July 24, 2020. https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/

Stolton, Samuel. "EU code of practice on disinformation 'insufficient and unsuitable,' member states say." *EURACTIV.com*, June 5, 2020. https://www.euractiv.com/section/digital/news/eu-code-of-practice-on-disinformation-insufficient-and-unsuitable-member-states-say/.

Stophoax. "About Stophoax.id at a glance." Accessed November 13, 2020. https://stophoax.id/tentang-kami/

Subramanian, Samanth. "Inside the Macedonian fake-news complex." *Wired.* February 15, 2017. https://www.wired.com/2017/02/veles-macedonia-fake-news/

Sudhakar, S. "Ahmad Dhani imprisoned, Fahri Hamzah encourages revised LAW." Suara. Published January 29, 2019. https://www.suara.com/news/2019/01/29/144219/ahmad-dhani-dipenjara-fahri-hamzah-dorong-uu-ite-direvisi

Sumaktoyo, Nathaneal. "Ethnicity and Jakarta's election." New Mandala. Published February 13, 2017
 https://www.newmandala.org/ethnicity-jakartas-election/

Swan, David. "Code to rein in spread of fake data." *The Australian*, June 26, 2020.

Tambini, Damian. *Fake News: Public Policy Responses.* London: Media Policy Project, London School of Economics and Political Science, 2017. http://eprints.lse.ac.uk/73015/1/LSE%20MPP%20Policy%20Brief%2020%20-%20Fake%20news_final.pdf

Tandoc Jr., Edson. C., Wei Lim Zheng and Richard Ling. "Defining 'Fake News'." *Digital Journalism* 6, no. 2 (2018): 137-153. DOI:10.1080/21670811.2017.1360143

Tang, N. "POFMA: A song of fact and opinion." The Online Citizen. Published February 4, 2020. https://www.onlinecitizenasia.com/2020/02/04/pofma-a-song-of-fact-and-opinion/

Tapsell, Ross. "Indonesia's policing of hoax news increasingly politicised." *ISEAS,* no. 75 (2019): 1-10. https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_75.pdf

Tapsell, Ross. "Platform convergence in Indonesia: Challenges and opportunities for media freedom." *Convergence* 21, no. 2 (2014): 182-197.

Tardaguila, Cristina. "Fact-checkers are teaching Indonesian housewives how to stop misinformation." Poynter. Published December 12, 2019. https://www.poynter.org/ifcn/2019/fact-checkers-are-teaching-indonesian-women-how-to-stop-misinformation/

Tardaguila, Cristina. "Spain has a new government and its fact-checkers had an impact on the campaign." Poynter. Published May 3, 2019. https://www.poynter.org/fact-checking/2019/spain-has-a-new-government-and-its-fact-checkers-had-an-impact-on-the-campaign/

Tehusijarana, Karina M. and Jessicha Valentina. "Jakarta riot: Government temporarily limits access to social media, messaging apps." *The Jakarta Post*, May 22, 2019. https://www.thejakartapost.com/life/2019/05/22/jakarta-riot-government-temporarily-limits-access-to-social-media-messaging-apps.html

Temby, Quinton. "Disinformation, violence, and anti-Chinese sentiment in Indonesia's 2019 elections." *ISEAS,* no. 67 (2019): 1-8. https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_67.pdf

Temby, Quinton. "Indonesia's election riots offer a lesson on the perils of fake news." *South China Morning Post,* September 9, 2019. https://www.scmp.com/week-asia/politics/article/3026057/indonesias-election-riots-offer-lesson-perils-fake-news

Tempo. "Lawmakers push for amendment of electronic law." September 13, 2013. https://en.tempo.co/read/512919/lawmakers-push-for-amendment-of-electronic-law

Tham, Yuen-C. "Fake news act: Speed, cost of appeals process set out." *The Straits Times,* October 2, 2019
 https://www.straitstimes.com/politics/fake-news-act-speed-cost-of-appeals-process-set-out

Tham, Yuen-C. "Falsehoods on coronavirus show why Pofma is necessary." *The Straits Times,* February 4, 2020. https://www.straitstimes.com/politics/falsehoods-on-coronavirus-show-why-pofma-is-necessary

The Guardian. "Jakarta protests: Muslims turn out in force against Christian governor Ahok." December 2, 2016.
https://www.theguardian.com/world/2016/dec/02/jakarta-protests-muslims-against-christian-governor-ahok

The Jakarta Post. "Beware what you share: Police step up war on hoaxes." November 12, 2018.
https://www.thejakartapost.com/news/2018/11/12/beware-what-you-share-police-step-war-hoaxes-fake-news.html

The Jakarta Post. "Criminalisation code." July 18, 2019.
https://www.thejakartapost.com/academia/2019/07/18/criminalization-code.html

The Jakarta Post. "Indonesia wages war against coronavirus misinformation as hoaxes spread online." February 3, 2020. https://www.thejakartapost.com/news/2020/02/03/indonesia-wages-war-against-coronavirus-misinformation-as-hoaxes-spread-online.html

The Jakarta Post. "ITE law aims to protect, manage electronic information, transactions." October 27, 2016.
https://www.thejakartapost.com/news/2016/10/27/ite-law-aims-to-protect-manage-electronic-information-transactions.html

The Jakarta Post. "New regulation to have intelligence agency work directly under President Jokowi." July 20, 2020. https://www.thejakartapost.com/news/2020/07/20/new-regulation-to-have-intelligence-agency-work-directly-under-president-jokowi.html

The Jakarta Post. "Prabowo campaign spokesman arrested on subversion charges." May 21, 2019. https://www.thejakartapost.com/news/2019/05/21/prabowo-campaign-spokesman-arrested-on-subversioncharges.html

The Jakarta Post. "Revised ITE Law could hamper freedom of expression: Researcher." October 31, 2016.
https://www.thejakartapost.com/news/2016/10/31/revised-ite-law-could-hamper-freedom-of-expression-researcher.html

The Jakarta Post. "Right contained in ITE Law to delete negative news threatens press freedom: Activist." October 28, 2016.
https://www.thejakartapost.com/news/2016/10/28/right-contained-in-ite-law-to-delete-negative-news-threatens-press-freedom-activist.html

The Online Citizen. "Five statements of facts by Dr Thum Ping Tjin spared from POFMA correction direction – Why?' Published May 14, 2020. https://www.onlinecitizenasia.com/2020/05/14/five-statements-of-facts-by-dr-thum-ping-tjin-spared-from-pofma-correction-direction-why/

The Straits Times. "Fake news law invoked for the first time over Facebook post." November 26, 2019.
https://www.straitstimes.com/politics/fake-news-law-invoked-for-the-first-time-over-facebook-post

The Straits Times. "Indonesia court sentences administrator of 'fake news factory' Saracen to jail." January 12, 2018.
https://www.straitstimes.com/asia/se-asia/indonesia-court-sentences-administrator-of-fake-news-factory-saracen-to-jail

Thomson Reuters Foundation. "Rights group, journalists press Indonesian govt to lift internet curb in restive Papua." Published August 23, 2019. https://news.trust.org//item/20190823055418-5iy2g/

Thorington, Kanzanira. "Europe's elections: The fight against disinformation." Council on Foreign Relations. Published May 23, 2019.
https://www.cfr.org/blog/europes-elections-fight-against-disinformation.

Timur, Fitri Bintang. "Unequal power makes women brunt of cyber law." SAFEnet. Published March 11, 2017.
https://safenet.or.id/2017/03/unequal-power-makes-women-brunt-of-cyber-law/

Tribunnews.com. "Publik Lebih Takut Berbicara Politik di Era Presiden Jokowi? Berikut Hasil Survei LSI." November 5, 2019.
https://www.tribunnews.com/nasional/2019/11/05/publik-lebih-takut-berbicara-politik-di-era-presiden-jokowi-berikut-hasil-survei-lsi?page=all.

Trihermanto, Febi and Helen Brown. "Indonesia focused on cyber resilience, open to foreign cooperation." Australia Indonesia Centre. Published November 12, 2019. https://digital.australiaindonesiacentre.org/news/insights/indonesia-focused-on-cyber-resilience-open-to-foreign-cooperation/

Turner, Sarah and Pamela Allen. "Chinese Indonesians in a rapidly changing nation: Pressures of ethnicity and identity." *Asia Pacific Viewpoint* 48, no. 1 (2007): 112-127.

Ungku, Fathin. "Facebook, rights groups hit out at Singapore's fake news bill." *Reuters,* April 1, 2019. https://www.reuters.com/article/us-singapore-politics-fakenews/facebook-rights-groups-hit-out-at-singapores-fake-news-bill-idUSKCN1RD279

Ungku, Fathin. "Singapore invites rights group to fake news hearing as dispute grows." *Reuters*, March 28, 2018.
https://www.reuters.com/article/us-singapore-politics-malaysia-scandal/singapore-pm-files-defamation-suit-against-blogger-who-shared-article-on-facebook-idUSKBN1O414L.

Ungku, Fathin. "Singapore PM files defamation suit against blogger who shared article on Facebook." *Reuters,* December 5, 2018.
https://www.reuters.com/article/us-singapore-politics-malaysia-scandal/singapore-pm-files-defamation-suit-against-blogger-who-shared-article-on-facebook-idUSKBN1O414L

UTS Centre for Media Transition. *Discussion Paper on an Australian Voluntary Code of Practice for Disinformation.* DIGI, October 16, 2020. https://digi.org.au/wp-content/uploads/2020/10/Discussion-Paper-Final.pdf

Valdani, Vicari and Associates. *Study for the Assessment of the Implementation of the Code of Practice on Disinformation.* Brussels: European Commission, May 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66649.

Varagur, Krithika. "Activists: Indonesian counterterrorism law threatens civil liberties." *Voa News,* May 30, 2018.
https://www.voanews.com/east-asia-pacific/activists-indonesian-counterterrorism-law-threatens-civil-liberties

Varagur, Krithika. "Indonesia poised to pass Asia's first 'right to be forgotten' law." *Voa News*, November 7, 2016.
https://www.voanews.com/east-asia/indonesia-poised-pass-asias-first-right-be-forgotten-law

Vaswani, Karishma. "Concern over Singapore's anti-fake news law." *BBC News*, April 4, 2019.
https://www.bbc.com/news/business-47782470

Voa News. "Indonesian police intensify crackdown on fake news." November 21, 2018.
https://www.voanews.com/east-asia-pacific/indonesian-police-intensify-crackdown-fake-news

Walker, Shaun and Jennifer Rankin. "Hungary passes law that will let Orban rule by decree." *The Guardian,* March 31, 2020.
https://www.theguardian.com/world/2020/mar/30/hungary-jail-for-coronavirus-misinformation-viktor-orban

Warburton, Eve. "Indonesia's pro-democracy protests cut across deep political cleavages." *New Mandala,* October 3, 2019.
ttps://www.newmandala.org/indonesias-pro-democracy-protests/

Wardle, Clair and Hossein Derakhshan. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making.*
Council of Europe Report, September 27, 2017.
https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Wardle, Claire. "The need for smarter definitions and practical, timely empirical research on information disorder." *Digital*
Journalism 6, no. 8 (2018): 951-963. DOI: 10.1080/21670811.2018.1502047

Wargadiredja, Arzia Tivany. "Indonesia's answer to fake news is a threat to free speech." *VICE News,* February 6, 2018.
https://www.vice.com/en_asia/article/j5bq54/indonesias-answer-to-fake-news-might-be-a-threat-to-free-speech

Watin-Augouard, Marc. "Law no. 2018-1202 of 22 December 2018 on combating the manipulation of information." FIC-Observatory.
Published November 1, 2019. https://observatoire-fic.com/en/law-no-2018-1202-of-22-december-2018-on-combating-the-
manipulation-of-information-by-general-marc-watin-augouard-founder-of-the-fic/

Wei, Neo Rong. "A look at key changes to Protection from Harassment Act." *TodayOnline,* May 7, 2019.
https://www.todayonline.com/singapore/look-key-amendments-protection-harassment-bill

Wilson, Cameron. "This man's Facebook page was blocked for spreading false information about the coronavirus." *BuzzFeed
News,* February 19, 2020. https://www.buzzfeed.com/cameronwilson/singapore-facebook-fake-news-law-alex-tan-coronavirus

Wolters, Oliver W. et al. "Indonesia: Religions." Britannica. Last modified November 11, 2020.
https://www.britannica.com/place/Indonesia/Services

Wong, Tessa. "Singapore fake news law polices chats and online platforms." *BBC,* May 9, 2019.
https://www.bbc.com/news/world-asia-48196985

Xiang, Teo Kai. "About." POFMA'ed. Accessed November 13, 2020. http://pofmaed.com/

Xiang, Teo Kai. "Explainer: What is POFMA?" POFMA'ed. Published July 5, 2020. http://pofmaed.com/explainer-what-is-pofma/

Xu, Terry. "TOC's submission to Select Committee on Deliberate Online Falsehoods." The Online Citizen. Published March 7, 2018
 https://www.onlinecitizenasia.com/2018/03/07/tocs-submission-to-select-committee-on-deliberate-online-falsehoods/

Yahoo News Singapore. "Thum Ping Tjin, *New Naratif* to challenge POFMA notice despite compliance." May 15, 2020.
https://sg.news.yahoo.com/thum-ping-tjin-new-naratif-to-challenge-pofma-notice-despite-compliance-071938288.html

Yao, Wei and Kenny Chng. "Symposium on POFMA: Reflections on thinking about the POFMA." *Singapore Public Law,* (November
2019): n.p. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4944&context=sol_research

Yong, Nicholas. "GE2020: Workers' Party is not 'pulling its punches' in spite of POFMA, says Pritam Singh." *Yahoo News
Singapore.* July 7, 2020. https://sg.news.yahoo.com/ge-2020-workers-party-is-not-pulling-its-punches-in-spite-of-pofma-
says-pritam-singh-063326754.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_
sig=AQAAAIrOu4fGibE2qg0_wGysQZWxGlrMs_D4ufdDdO6OzEkNrRDGDD45KSSR9ldVhmsr66-Mvrh8dfWWIKbYwHBHci5KarXg
Rua1iR2bMVxuLWxI9cNhQYQxFivabsbiKXpcqH0JFTv89ncOn32AUssYPlQuGdUBNVyXjXRcmXF-A-5H

Yuliawati, Lis and Bayu Nugraha. "Penyebar Hoax Dijerat UU Terorisme, Polri: Tergantung Fakta Hukum." *Viva*, March 21, 2019.
https://www.viva.co.id/berita/nasional/1132456-penyebar-hoax-dijerat-uu-terorisme-polri-tergantung-fakta-hukum?

Zaini, *Khairulanwar*. "Singapore in 2019: In holding pattern." *Southeast Asian Affairs*, no. 1 (2020): 294–322.

Appendix A:
Tables of laws and regulations, **Indonesia**

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Criminal Code (KUHP)	Adopted in 1946	Article 14 refers to false information, however there doesn't appear to be a definition of what makes it so. Article 15 states that information or news that is uncertain, exaggerated or incomplete is prohibited if it causes, or has the potential to cause, public unrest. Defamation is defined as the act of "intentionally harming someone's honour or reputation by charging him with a certain fact."[1]	The Government may arrest and punish with lengthy jail terms or large fines those that are suspected of spreading misinformation, whether intentionally or not, on the grounds that it causes, or threatens to cause public unrest.	Anyone in Indonesia can come under scrutiny. Members of the public and high profile political figures alike have faced charges under Articles 14 and 15. This law does not target online activity exclusively.	The focus on public unrest in the KUHP means that it has often been used in moments of crisis, such as during natural disasters, mass riots and recently the COVID-19 pandemic. It has been used against criticism of the Government's handling of COVID-19. There is also evidence to suggest it has been used freely against political dissidents, including opposition political parties and West Papuan separatists.

1   "Criminal Code [KUHP] (Indonesia), 1946," accessed November 13, 2020, Article 310(1), https://www.unodc.org/res/cld/document/idn/indonesian_penal_code_html/I.1_Criminal_Code.pdf

Appendix A: Tables of laws and regulations, Indonesia

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Revised Criminal Code (RKUHP)	Tabled in 2018; it was scheduled to be voted on in September 2019, which was postponed.	Like the existing Criminal Code, the revised version is largely lacking an explicit definition of fake news, misinformation or disinformation. It does differentiate between knowingly spreading false information,[2] spreading information one may suspect to be false,[3] and information that is uncertain, exaggerated or incomplete[4] – each carry different penalties. Blasphemy – that which discriminates or is hostile "against the religion adopted in Indonesia" – is also prohibited.[5]	The Bill outlines added powers beyond those granted in KUHP. These include the authority to prosecute criticism of judges,[6] and defamation of the President or Vice-President.[7]	Given the broad scope of the bill, it would impact on everyone in Indonesian society. It has been said to be particularly "disastrous not only for women and religious and gender minorities, but for all Indonesians."[8]	As it hasn't been passed, there have been no outcomes except for mass demonstrations in protest of its more controversial clauses relating to freedom of speech, among other things.

2   Ibid., Article 262(1).
3   Ibid., Article 262(2).
4   Ibid., Article 263.
5   Ibid., Article 304.
6   "Draft Revised Criminal Code [RKUHP] (Indonesia), 2019," accessed November 13, 2020, Article 281, https://www.hukumonline.com/pusatdata/detail/17797/rancangan-undang-undang-2019#
7   Ibid., Article 218.
8   Andreas Harsono quoted in "RKUHP Explainer: All the controversial articles in Indonesia's criminal code overhaul," *Coconuts Jakarta,* September 19, 2019, https://coconuts.co/bali/features/rkuhp-explainer-all-the-controversial-articles-in-indonesias-criminal-code-overhaul-2/

Appendix A: Tables of laws and regulations, Indonesia

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Information and Electronic Transaction Law (UU ITE)	2008; revised in 2016	Unlike the Criminal Code, UU ITE relates directly to electronic information. "False and misleading information" here relates to "consumer loss in electronic transactions,"[9] however it has been used much more broadly than that. It prohibits information intended to incite hostility based upon ethnicity, religion and race.[10] Also illegal is the unauthorised manipulation, creation and deletion of electronic information to make it "seem to be authentic."[11] One criticism is that it doesn't properly differentiate between insults and defamation.[12]	Breaches of the law carry significant jail terms and fines for perpetrators. Suspected perpetrators are often arrested and detained prior to trial, if one ever eventuates. UU ITE has been labelled the Government's "de facto 'anti-fake news' law" for its regular use against misinformation.[13] The Government can terminate online access,[14] which it has done in targeted areas of the country in times of unrest.	Internet users are obviously impacted by the law. Ordinary Indonesians that have low levels of digital literacy have come under scrutiny for sharing misinformation unwittingly.[15] Media professionals have faced charges under the law. Self-proclaimed atheists have received scrutiny for purported hate speech against Islam.[16] Critics of the Government are regular targets of the law. Such as West Papuan separatists, who have had their access to the internet blocked.	UU ITE has had several purported outcomes, such as limited free speech and crackdowns on political dissent. Others have claimed that it has resulted in a "revenge" dynamic, where it is used flagrantly against one's enemies, and has had an overall chilling effect on Indonesia's public sphere.[17]

---

9 "Law No. 11 of 2008 on Information and Electronic Transactions [UU ITE] (Indonesia), 2008 [revised 2016]" HUKUM Online, accessed November 13, 2020, Article 28(1), https://www.hukumonline.com/pusatdata/detail/lt584a7363785c8/node/lt56b97e5c627c5/uu-no-19-tahun-2016-perubahan-atas-undang-undang-nomor-11-tahun-2008-tentang-informasi-dan-transaksi-elektronik

10 Ibid., Article 28(2).

11 Ibid., Article 35.

12 Usman Hamid, "Indonesia's Information Law has threatened free speech for more than a decade. This must stop," The Conversation, November 25, 2019, https://theconversation.com/indonesias-information-law-has-threatened-free-speech-for-more-than-a-decade-this-must-stop-127446.

13 Tapsell, Ross, "Indonesia's policing of hoax news increasingly politicised," ISEAS, no. 75 (2019), https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_75.pdf

14 UU ITE, Article 40.

15 "Indonesia's policing of hoax news increasingly politicised," 3.

16 "Indonesian man arrested for Facebook post allegedly insulting Islam," Mid-Day, May 1, 2018, https://www.mid-day.com/articles/indonesian-man-arrested-for-facebook-post-allegedly-insulting-islam/19374167.

17 "Persoalan UU ITE dan Praktik Pelanggaran Hak Digital di Indonesia," SAFEnet, published November 14, 2019, https://id.safenet.or.id/wp-content/uploads/2019/11/Persoalan-UU-ITE-dan-Pelanggaran-Hak-Digital-SAFEnet-2019.pdf

Appendix A: Tables of laws and regulations, Indonesia

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Law No. 17 of 2011 on State Intelligence	2011	The law does not define fake news, however its remit covers threats to domestic security such as information and cyber warfare.[18]	This law authorises the State Intelligence Agency (BIN) to conduct surveillance, information extraction and interception to protect against "activities that threaten national interests and security."[19] BIN has been used during elections to monitor online information. BIN reports directly to the president.	This law relates to serious criminal activity that is judged to threaten national security, such as terrorism. Nonetheless, "hoaxes" have commonly fallen under this definition as they may have the potential to cause public disorder.	A recently passed law ensures BIN works directly under President Widodo.[20] BIN has been used for its intelligence expertise to help mitigate crisis points, most recently during COVID-19.
Terrorism Act	2018	Article 1.4 in the law defines the threat of violence as "speech, writing, picture, symbol or body language, with or without electronic… form which could create widespread fear."[21] However it does not define misinformation or disinformation.[22]	The terrorism law allows the police to "detain 'terror suspects' for as long as 21 days without charge, and for another 200 days if police need time to gather evidence."[23]	While senior government officials have suggested that perpetrators of hoaxes can be caught by the Act "if there is an element of threat of violence and (they) create an atmosphere of terror and widespread fear,"[24] as of yet it has not been used to prosecute misinformation.	The Act has not been used against misinformation.

18 "Law No. 17 of 2011 on State Intelligence (Indonesia), 2011," accessed November 13, 2020, https://www.icj.org/wp-content/uploads/2011/01/Indonesia-intelligence-law-draft-2011-eng.pdf

19 Ibid., Article 31(a).

20 "New regulation to have intelligence agency work directly under President Jokowi," The Jakarta Post, July 20, 2020, https://www.thejakartapost.com/news/2020/07/20/new-regulation-to-have-intelligence-agency-work-directly-under-president-jokowi.html

21 Krithika Varagur, "Activists: Indonesian counterterrorism law threatens civil liberties," Voa News, May 30, 2018, https://www.voanews.com/east-asia-pacific/activists-indonesian-counterterrorism-law-threatens-civil-liberties

22 Fiska Maulidian Nugroho, "Study of fake news dissemination articles on Criminal Code regulations, Law of Information and Electronic Technology, and also Law of Terrorism Criminal Act eradication," (Paper presented at Fake News and Elections in Asia Conference, Bangkok, Thailand, July 10-12, 2019), 88, accessed November 13, 2020, https://asiacentre.org/wp-content/uploads/2019/09/Fake-News-Conference-Proceeding.pdf

23 "Indonesia passes controversial anti-terror laws to fight ISIL," Al Jazeera, May 26, 2018, https://www.aljazeera.com/news/2018/05/indonesia-passes-controversial-anti-terror-laws-fight-isil-180525055635674.html

24 Dedi Prasetyo quoted in Lis Yuliawati and Bayu Nugraha, "Penyebar Hoax Dijerat UU Terorisme, Polri: Tergantung Fakta Hukum," Viva, March 21, 2019, https://www.viva.co.id/berita/nasional/1132456-penyebar-hoax-dijerat-uu-terorisme-polri-tergantung-fakta-hukum?

Appendix B:
Tables of laws and regulations, **Singapore**

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Protection from Online Falsehoods and Manipulation Act (POFMA)	Legislated April 2019/enacted October 2019	(2)(a): "a statement of fact is a statement which a reasonable person seeing, hearing or otherwise perceiving it would consider to be a representation of fact; and (b): a statement is false if it is false or misleading, whether wholly or in part, and whether on its own or in the context in which it appears."[1]	POFMA enables government ministers to issue directives to correct, remove, or disable access to statements it determines to be false. They may make this judgement based on whether the statement is believed to be prejudicial to Singapore's public interest, security and international relations, or to influence elections, diminish confidence in public institutions, or "incite feelings of enmity, hatred or ill will between different groups of persons."[2] Internet intermediaries can be directed to remove or disable access to false statements hosted on their platforms.[3]	Online users. Internet intermediaries: • Social media platforms • Direct messaging platforms[4] • Internet service providers • Websites. • Technology companies. Journalists and news organisations. Election campaigners and political parties, as political ads must be monitored by internet intermediaries.[5]	Due to its brief lifespan, it is difficult to gauge its outcomes. More research is needed on purported effects such as the "chilling" of free speech and self-censorship. Various actors have continued to criticise the Government, however many have promptly received POFMA orders. Time will tell if there is a decline in such forms of public speech. Some observed changes were: • policed speech during recent election • accountability of internet intermediaries (ie. Facebook) to government directives • complication of role of judiciary vis-à-vis the Government • heavy use of POFMA against oppositional voices, such as opposition politicians and independent journalists.

1   Parliament of Singapore, *Protection from Online Falsehoods and Manipulation Act* (Parliament of Singapore, 2019), section 2, https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625
2   Ibid., Section 7.
3   Ibid., Part 4.
4   Adrian, Lim, "Parliament: Fake news law covers closed platforms like chat groups and social media groups, says Edwin Tong," *The Straits Times,* May 7, 2019, https://www.straitstimes.com/politics/parliament-fake-news-law-covers-closed-platforms-like-chat-groups-and-social-media-groups
5   *Protection from Online Falsehoods and Manipulation Act,* Section 48.

Appendix B: Tables of laws and regulations, Singapore

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Protection from Online Harassment Act (POHA)	Legislated March 2014/ enacted November 2014 [revised January 2020]	POHA[6] applies the same definition as POFMA (see above box)	Aimed to be used by "the man on the street."[7] The law's use was judged by the High Court to be available only to a "person."[8] The 2019 amendments extended the law's use to entities such as companies.[9] Breaking POHA protection orders can result in arrests. Police may arrest without a warrant, and take to court, anyone deemed to act against the provisions of the Act.[10] Penalties include up to a S$5,000 fine and/or 6-12 months jail, which is doubled for repeated offences.	Individuals and entities that are found to have committed online harassment, and communicated falsehoods about other people or entities deemed as harmful, can be ordered to stop, remove or correct such communications. Individuals, entities and internet intermediaries may face protection orders or civil lawsuits from the "victim" of said abuse. The State argued that journalists may use it against harassment.[11] Actors outside Singapore can be charged under POHA. 'Vulnerable people' and victims of intimate partner violence were given greater protections in 2019 amendments.[12] People that commit 'doxxing'	The Government says more than 3000 Magistrates Complaints were made between 2014-2019, of which 1700 prosecutions were brought and 900 convictions made. 500 applications were for protection orders, of which 200 were granted. Workplace harassment was a common reason.

6   Parliament of Singapore, *Protection from Online Harassment Act (Singapore)* (Parliament of Singapore, 2014), section 2, https://sso.agc.gov.sg/Act/PHA2014
7   "Parliamentary debates: Protection from Online Falsehoods and Manipulation bill," Parliament of Singapore, published May 8, 2019, Vol. 94 , Part 2, https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-367
8   Human Rights Watch, *Kill the Chicken to Scare the Monkeys: Suppression of Free Expression and Assembly in Singapore* (Human Rights Watch, 2017), 101, https://www.hrw.org/sites/default/files/report_pdf/singapore1217_web.pdf
9   Neo Rong Wei, "A look at key changes to Protection from Harassment Act," *TodayOnline,* May 7, 2019, https://www.todayonline.com/singapore/look-key-amendments-protection-harassment-bill
10   *Protection from Online Harassment Act,* Section 18.
11   "Laws protecting journalists from online harassment: Singapore," Library of Congress, accessed November 20, 2020, https://www.loc.gov/law/help/protecting-journalists/singapore.php
12   *Protection from Online Harassment Act,* sections 8A & 8B.

Appendix B: Tables of laws and regulations, Singapore

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Online News Licencing Scheme (under the Broadcasting Act)	June 2013	As misinformation is not explicitly targeted by this framework, it is not defined as such. Nonetheless, the publication of "deliberately fabricated articles" has been punished under this licencing framework. Content that is "against public interest, public order, national harmony, and/or offends against good taste or decency" is targeted.	The Government can order licensees to take down "prohibited"[13] material within 24 hours. They can also be directed to shut down online sites, and have their licences revoked.[14]	Websites that post on Singapore-related news at least once a week on average over a two-month period, and have at least 50,000 unique visits a month from Singaporean internet users.[15] Appears to impact "news"-based sites rather than social media sites, however there was an instance where the Government asked Google to take down a YouTube video that it deemed offensive.[16]	Sites that are required to become licensees must put up a S$50,000 performance bond to the Government. This status brings content responsibilities upon them. Websites, such as *The Real Singapore*, have been ordered to take down prohibited material and shut down their sites completely. There does not appear to be a significant number of such cases. Larger, popular online sites have been forced to abide by this licencing framework.
Defamation Act (civil defamation)	1965 [revised 2014]	Defamation is defined in relation to instances of "libel and slander and other malicious falsehoods" that may cause reputational, financial or other damage.	The Government may sue anyone that it views has defamed its reputation. Unlike other countries, Singapore's defamation legislation "does not provide a qualified privilege for criticism of government officials and other public figures. The damages awarded plaintiffs can be so high as to bankrupt defendants."[17]	Anyone who has been viewed as defaming others including government. To date, this Act has seen voices of dissent, such as independent media and individual internet users face prosecution.	Self-censorship has been reported.[18] Some state they have taken precautionary measures before speaking out, such as dissipating their assets in fear of eventually being sued.[19] Civil defamation lawsuits have been used by the Government and successive Prime Ministers against political opponents, critical and foreign media for decades.[20]

13   "Prohibited material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws" (Infocomm Media Development Authority, *Internet Code of Practice* (Singapore: IMDA, 1997), 2, https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/Regulations/Codes-of-Practice/Codes-of-Practice-Media/PoliciesandContentGuidelinesInternetInterneCodeOfPractice.pdf)
14   *Kill the Chicken to Scare the Monkeys,* 49.
15   "What is the licensing framework for online news sites all about?", Singapore Government, published June 18, 2013, https://www.gov.sg/article/what-is-the-licensing-framework-for-online-news-sites-all-about
16   Alex Au Waipang, "Singapore bloggers wary of news site licence scheme," Committee to Protect Journalists, published June 4, 2013, https://cpj.org/2013/06/singapores-news-site-license-plan-raises-questions/
17   Ibid., 96.
18   *Kill the Chicken to Scare the Monkeys,* 8-10.
19   Ibid.
20   Ibid.

Appendix B: Tables of laws and regulations, Singapore

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Penal Code section 499 (criminal defamation)	1872	"Whoever, by words either spoken or intended to be read, or by signs, or by visible representations, makes or publishes any imputation concerning any person, intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person."[21]	The Government can charge a citizen, entity or foreign entity with defamation, the penalty being a fine, up to two years jail time, or both.[22] The Government can search private locations "without a warrant and seize anything they deem relevant to an alleged offense."[23]	Political opponents. Independent media.[24] Members of the public.	In the past, the Government has allegedly used criminal defamation to make political opponents ineligible to run for parliament.[25] Used by the Government less often than civil defamation lawsuits. A recent case involving The *Online Citizen* demonstrates how it can potentially put independent media in jail.
Sedition Act	1965 [revised 2013]	As misinformation is not explicitly targeted by this legislation, it is not defined as such. However, speech or publications with a "seditious tendency" is that which inspires "hatred," "contempt" or "disaffection" toward the Government or the "administration of justice," or "promote ill-will," "hostility" or "discontent" between the citizens, races and classes of Singapore.[26] Falsehoods have fallen under this definition in practice.	The Government can charge alleged seditious actors with a fine of up to S$5,000 and up to three years jail time.[27] The law enables the Government to jail people it believes are in breach of the Act, even if the statements had no seditious intent or effects on others.[28]	Members of the public. Members of the media. Vocal religious figures have been charged with sedition for inciting enmity between different religious groups.[29]	Like the use of criminal defamation, sedition charges have seen independent media and other outspoken Singaporeans jailed for publishing purported falsehoods.

21 Parliament of Singapore, *Penal Code* (Singapore) (Parliament of Singapore, 1972), Section 499, https://sso.agc.gov.sg/Act/PC1871?ProvIds=pr499-
22 Ibid., Section 500.
23 *Kill the Chicken to Scare the Monkeys,* 9
24 "In December 2018, the executive editor Terry Xu Yuan Chen was charged with defamation, and at the time of writing is awaiting trial. If convicted, Xu will face prison time and a large monetary penalty, common punishments for such 'crimes'," (Jason Luger, "Planetary illiberalism and the cybercity-state: in and beyond territory," *Territory, Politics, Governance* 8, no. 1 (2020): 12.
25 *Kill the Chicken to Scare the Monkeys,* 16.
26 Parliament of Singapore, *Sedition Act* (Singapore) (Parliament of Singapore, 1948), Section 3, https://sso.agc.gov.sg/Act/SA1948?ProvIds=pr3-
27 Ibid., section 4(1).
28 *Kill the Chicken to Scare the Monkeys,* 44
29 Ibid., 47, 49-50.

Appendix C:
Tables of laws and regulations, **European Commission**

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Action Plan on Strategic Communication	June 22, 2015	Concerned primarily with Russian coordinated disinformation campaigns	a) Increase EU Strategic Communication capacity b) Work with partners and development of networks d) Support for freedom of the media and freedom of expression f) Capacity building for journalists and media actors h) Engagement with Civil Society i) Increase awareness, develop critical thinking and promote media literacy	European External Action Service (EEAS), Member States, Organisation for Security and Co-operation in Europe (OSCE), Council of Europe, OPEN Neighbourhood, journalists and media representatives, European Regulators Group for Audiovisual Media Services (ERGA)	Established East StratCom Task Force and the flagship project EUvsDisinfo which identifies, compiles and exposes disinformation cases. As of 2019, the database holds over 6,500 samples of pro-Kremlin disinformation.
Joint Framework on Countering Hybrid Threats: A European Union Response	April 6, 2016	Hybrid threats encompass "coercive and subversive" activities that can be economic, militaristic, technological or diplomatic. Within this falls "massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors."[1]	**Action 2** Creation of an EU Hybrid Fusion Cell, facilitating cooperation and secure communication between Member States. **Action 3** "Explore with Member States ways to update and coordinate capacities to deliver proactive strategic communications and optimise use of media monitoring and linguistic specialists."	EEAS, Member States, social media specialists, online platforms, European Strategic Communications Network.	The establishment of Communication Task Forces for the Eastern and Southern Neighbourhoods. Monitoring disinformation, awareness-raising activities in Member States about the impact of Russian disinformation. The Task Forces gained support through the contribution of military advice to help counter misinformation campaigns targeted at the EU and individual Member States.

---

1   European Commission, *Joint Framework on Countering Hybrid Threats* (Brussels: European Commission, April 6, 2016), 2, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Appendix C: Tables of laws and regulations, European Commission

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Tackling Online Disinformation: A European Approach	April 26, 2018	Concerned with large scale disinformation, which includes "misleading or outright false information."[2]	**3.1.1** Convene a multi-stakeholder forum on disinformation, to form the Code of Practice on Disinformation.	Online platforms, advertising industry, advertisers, media and civil society representatives.	The Code of Practice. Possible regulation if assessment not satisfactory.
			3.1.2 Support for the creation of an independent European network of fact checkers. Launch a secure European online platform for disinformation to support fact checker networks and academics.	Independent fact checkers, academics, Member States, civil society.	Social Observatory for Disinformation and Social Media Analysis (SOMA), launched November 2018. Organised a fact checking conference. International Fact-Checking Network created an EU specific fact checking site *FactCheckEu.info*
			3.1.3 Focus on transparency and online accountability via the identification of suppliers of information.	eIDAS Cooperation Network, online platforms, voluntary online systems, academic researchers, technology companies and fact checkers, Member States.	Commission reports to have mobilised the Cooperation Network set up under the electronic Identification and Authentication Service Regulation (eIDAS), raising awareness on how eIDAS tools and services could be relied upon to tackle disinformation by increasing accountability and encouraging more responsible behaviour online
			3.1.4 Utilise Horizon 2020 work programme to mobilise new technologies. Will also explore extra support to deploy tools to combat disinformation.	Horizon 2020, European Research Council projects, traditional media, journalists, online platforms.	Currently, under the ERC and Horizon 2020, there are several actions aimed at improving the understanding of online disinformation and developing new tools for content verification. Various projects studying automated systems and their impact on public discourse, and solutions to help traditional media better detect false narratives online.

2   European Commission, *Tackling Online Disinformation: A European Approach* (Brussels: European Commission, April 26, 2018), 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&qid=1583456906698&from=EN

Appendix C: Tables of laws and regulations, European Commission

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Tackling Online Disinformation: A European Approach	April 26, 2018		**3.2** Secure and resilient election process.	Member States, media and social media representatives, international orgs.	Commission started a constructive dialogue with Member States in 2018. Delivered a compendium on cyber security of election technology. Raising awareness and strengthening capacities to manage risks to democratic electoral process presented by cyber-attacks and disinformation.
			3.3 Fostering media literacy, including steering a Media Literacy Expert Group and supporting all EU digital education efforts. Fact-checkers to provide educational material to schools and educators.	OECD, Member States, fact-checkers.	Introduce rules for Member States and video-sharing platforms on media literacy and establish a co-regulatory system. Online disinformation and fake news to be added to OECD ICT familiarity questionnaire.
			3.4 Supports the practice of quality journalism in the EU. Member States encouraged to consider strategies to address market failures hampering the viability of quality journalism, as well as training for journalists and industry innovation. Will explore increased funding opportunities to support media freedom and pluralism, quality news media and journalism.	Member states, journalists, media representatives.	Implementing framework for greater investment and funding in innovation in quality journalism, media freedom and plurality.

Appendix C: Tables of laws and regulations, European Commission

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Joint Framework on Countering Hybrid Threats from July 2017 to June 2018	June 13, 2018		**Action 3: Strategic communications** The positive experiences of the East StratCom Task Force need to be underpinned and strengthened. Task Force set up for Western Balkans. Training for staff in Eastern Partnership countries for enhancing their strategic communications capabilities and their resilience to disinformation.	East StratCom Task Force, NATO, Commission, EEAS, Eastern Partnership (EaP) countries.	Monitoring disinformation, awareness-raising activities in EaP countries and Member States about the impact of Russian disinformation.
			Action 21: Intelligence capabilities extended "by contributing military advice to help counter misinformation campaigns targeted at the EU and individual Member States."[3]	EU Military Staff, Member States, EU Hybrid Fusion Cell, EEAS.	Enabling the enhancement of early warning.

---

3   European Commission, *Joint Framework on Countering Hybrid Threats from July 2017 to June 2018* (Brussels: European Union, June 13, 2018), 13, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0014&from=EN

Appendix C: Tables of laws and regulations, European Commission

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
EU Code of Practice on Disinformation	September 26, 2018	Citing a High-Level Expert Group paper, the Code defines disinformation as "'verifiably false or misleading information' which, cumulatively, (a) 'Is created, presented and disseminated for economic gain or to intentionally deceive the public'; and (b) 'May cause public harm,' intended as 'threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security.'" It does not include "misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary."	While specific measures of how to combat disinformation are to be decided by signatories, the five "Pillars" of focus include "scrutiny of advertisement placements to reduce revenues of the purveyors of disinformation," "transparency about political and issue-based advertising," targeting inauthentic activity and strengthen integrity of services, and empowerment of consumers and the research community. Signatories tasked with producing regular reports on actions taken and a framework for regular EU and independent assessment is established.	Digital platforms, advertising bodies, fact checkers and researchers.	Successive assessments by ERGA, independent consultant VAA and the Commission found the Code has established a framework for dialogue between relevant stakeholders, monitoring, and greater transparency and accountability of platforms' operations. Each Pillar had demonstrated improvement, yet significant shortfalls in performance of the Code and its signatories were noted – particularly regarding data sharing and the empowerment of users and the research community.
Directive (EU) 2018/1808 of the European Parliament and of the Council	November 28, 2018		**Article 33a** Member States shall promote and take measures for the development of media literacy skills.	Member States, civil society.	Decrees Member States to promote media literacy. Nearly a dozen Member States have taken up comprehensive media literacy initiatives.

Appendix C: Tables of laws and regulations, European Commission

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Action Plan against Disinformation	December 5, 2018		**Action 2** High Representative to "review the mandates of the Strategic Communications Task Force for Western Balkans and South to enable them to address disinformation in these regions." **Action 3** "Establish a Rapid Alert System for addressing disinformation campaigns." **Action 5** "Strengthen strategic communications in the Union's neighbourhood."[4]	StratCom Task Forces, online platforms, international partners, G7, NATO, Union Neighbourhoods	Increased budget to strengthen the Union's capabilities to detect, analyse and expose disinformation as well as to ensure a coordinated and speedy response – ie. Rapid Alert System. RAS however has received mixed reviews since it has not been triggered (as of June 2020), and few Member States have shared information through it.[5] Fostered closer coordination among EU institutions and national authorities.

4   European Commission, *Action Plan against Disinformation* (Brussels: European Commission, December 5, 2018), 8, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0036&qid=1583456906698&from=EN

5   James Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative* (Washington: Carnegie Endowment for International Peace, June 2020), 9, https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf

Appendix C: Tables of laws and regulations, European Commission

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Action Plan against Disinformation	December 5, 2018		**Action 6** Close monitoring of the implementation of Code of Practice, and "push for rapid and effective compliance." After 12-month assessment Commission may propose actions including regulation.	Signatories to the Code	Facebook, Google, Twitter were found to have: • improved their scrutiny of ad placements, reducing malicious click-baiting practices and advertising revenues for those posting disinformation; • focused on manipulative behaviour to make content more visible through coordinated operations, as well as the abusive use of bots and fake accounts. However the platforms did not make sufficient progress in increasing the transparency of websites hosting ads, partly due to the lack of engagement from the advertising industry. Questions remain about the effectiveness of the transparency measures taken by all signatories. All platforms should also ensure an active and working cooperation with fact checkers in all Member States and empower users to better detect disinformation.

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Action Plan against Disinformation	December 5, 2018		**Action 7** "Targeted campaigns for the public and training for media and public opinion shapers." Continue support for independent media and quality journalism and research into disinformation. **Action 8** "Support the creation of teams of multi-disciplinary independent fact-checkers and researchers." **Action 9** Media Literacy Week, cross border cooperation and the "launch of practical tools for the promotion of media literacy for the public."	European Commission, High Representative, the public, independent media and journalists, academics, Member States, fact checkers, researchers, civil society.	EU institutions launched a number of initiatives to raise public awareness of disinformation across EU Member States, including seminars, conferences and media briefings. Provided proactive and multilingual communication to millions of EU citizens through social media and through communication campaigns. The Commission worked together with the EEAS and the European Parliament to produce and distribute myth busting and awareness-raising materials, drawing on both academic and institutional expertise. European Media Literacy Week with more than 320 events in the EU18. The International Fact-Checking Network created a European branch of independent fact checkers covering 14 Member States and launched a website in 11 EU languages.

Appendix C: Tables of laws and regulations, European Commission

Legislative and non-legislative initiatives	Commencement date	How it defines the problem	Relevant actions	Stakeholders impacted	Outcomes
Communication from the Commission Europe in May 2019: Preparing for a More United, Stronger and More Democratic Union in an Increasingly Uncertain World	April 30, 2019		**Part II. 4 Acting together to fight disinformation** Outlined emphasis on scaling up independent fact checking efforts, media literacy and artificial intelligence capacities, collaboration with online platforms, and media pluralism and freedom, all aimed at improving the public's access to reliable information.	EU27 Leaders, fact checkers, the public, digital platforms and social networks.	These recommendations were aimed to guide the actions and interactions of EU leaders prior to their May 2019 meeting in Romania.
Tackling COVID-19 Disinformation – Getting the Facts Right	June 10, 2020	Acknowledged the need to expand definition of the problem from disinformation, where intent is key, to misinformation, since the COVID-19 "infodemic" demonstrated the harm that such pandemic-related misinformation can cause.	Sought to develop more robust measures to counter COVID-19 misinformation. This includes: • Improving coordination between EU institutions, including better use of the Rapid Alert System, civil society and journalists • Working with the WHO to better identify and counter "misleading and harmful narratives" • Improving public education The most notable measure was to require Code signatories to provide monthly reports on their efforts to counter the infodemic.	Member States, signatories, the public, civil society and researchers	In September 2020, the Commission released Code signatories' first baseline reports on these COVID-19-related asks. The reports demonstrated signatories had increased access to and visibility of authoritative information.[6] Notably, however, the application of these measures was not uniform across the EU.

---

6   "First baseline reports – Fighting COVID-19 disinformation monitoring program," European Commission, published September 10, 2020, https://ec.europa.eu/digital-single-market/en/news/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme

Appendix D:
Respondent profile and interview **schedule**

This appendix lists the 14 interviewees who have contributed to the report along with an indicative schedule of the types of questions asked of them. Under the La Trobe University ethics application approved for this research, some interviewees' identities were not disclosed due to potential adverse consequences. However, some interviewees felt it preferable and, in some instances, safer in their circumstances, to be named. Thus, the table below details the profiles of the respondents interviewed for this project, with more detailed information provided when explicit permission was granted.

The interview schedule also varies according to individual circumstances. The Interview Schedule is a semi-structured guide to provide an understanding of the types of questions asked of respondents. Interviews were analysed with the assistance of qualitative data analysis software, NVivo, to locate rich insights in the data, consolidate the main themes that form the findings chapters (chapters five to seven), and to produce defensible findings backed by evidence.

SINGAPORE

Interviewee Name/ Number	Position	Interview Date
Pingtjin Thum (PJ Thum)	Historian, activist and Managing Director of the *New Naratif*	19 August 2020
Kirsten Han	Freelance Journalist	25 August 2020
1	Social Media/Digital Platform Expert	7 August 2020
3	Academic	18 August 2020
4	Social Media/Digital Platform Expert	7 August 2020
11	Academic	20 August 2020

INDONESIA

Interviewee Name/ Number	Position	Interview Date
Wahyu Dhyatmika	Editor-in-Chief of *Tempo* magazine	24 August 2020
Septiaji Eko Nugroho	Chairman of MAFINDO (civil society group tackling hoaxes)	26 August 2020
Andreas Harsono	Human Rights activist and Researcher at Amnesty International Indonesia	20 August 2020
Damar Juniarto	SAFEnet, Southeast Asia Freedom of Expression, Executive Director and activist	31 August 2020
7	Academic	19 August 2020
9	Social Media/Digital Platform Expert	8 September 2020

OTHER

Interviewee Name/ Number	Position	Interview Date
13	EU Social Media/Digital Platform Expert	16 September 2020
14	The Australian Communications Media Authority (ACMA)	18 November 2020

Semi-structured interview schedule

1. What is your name?

2. What organisation do you work for?

3. What is your title?

4. What is your career background?

5. How do you define fake news: misinformation and disinformation?

    a. Any other terms that should be considered?

6. Is misinformation a problem in the region? If so, how widespread is the problem on platforms and social media across the region (APAC)?

    a. Where is it most challenging in terms of places and spaces online?

7. How have you and/or your organisation dealt with misinformation?

8. Which measures do you think have been most effective?

    a. What is the evidence for that?

9. How has your government responded to the threat of misinformation on digital platforms and social media?

    a. What laws, if any, have been passed?

    b. What penalties are associated with breaches of these laws?

10. What powers do the laws provide to the Government? Do they have limitations?

11. Are there public concerns/controversial aspects of these policy/legal changes? If so, what are they?

12. Who are the people/organisations most concerned about these changes?

13. Through the experience of your work, what do you consider are the main public consequences of 'fake news' laws?

14. Can you provide examples of any adverse impacts the fake news laws have had on: a) a person, b) organisations c) others?

15. What is the current state of the debate around misinformation on social media platforms in your country and across APAC?

16. If these laws could be improved, what changes would you like to see implemented?

17. In your experience, which country has the most useful measures to deal with fake news online? Why?

18. Is there anyone in this field who you think I should talk to?

19. Is there anything else you would like to add?