Exploring online misinformation and disinformation in Asia Pacific

July 2021

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Authors

Kenechi Okeleke, Director, Social and Regional Research
James Robinson, Lead Analyst

Contributors

Jeanette Whyte, Head of Public Policy, Asia Pacific
Natasha Jackson, Head of Public Policy and Consumer Affairs
Christiaan Segura, Director, Public Policy, Asia Pacific

Contents

Executive summary

Society has long grappled with the dissemination of false information, but the arrival of the internet has proved an accelerating factor. Online channels have shown to be efficient instruments for circulating false information for various reasons, including convenience, instantaneity and scale. Connectivity has become essential, as people rely on digital services to communicate, work, learn and much more; however, the growing volume of false information, combined with its virality, means people, particularly vulnerable groups, can become misinformed, with potentially far-reaching consequences.

The myriad themes targeted by false information online, such as politics, climate change, religion and health, make the ramifications all the more significant. In addition to negative outcomes for affected individuals and communities, 'fake news' can drive a mistrust of institutions and disrupt democratic processes, which could undermine social cohesion and inclusive economic development. False information can also hinder progress on key societal issues; for example, it has slowed the response to Covid-19 and complicated efforts to tackle climate change (an area where mobile operators are increasingly engaged), and can delay or deter network infrastructure deployment.

The mobile industry is sometimes affected by false information, even though mobile operators do not typically host content. Recently, mobile operators have been the target of misinformation around 5G and Covid-19. Mobile operators also feel the effects of the countermeasures used to address online misinformation, such as the use of blunt mechanisms (e.g. network shutdowns) to slow the spread of false information.

The impacts of false information on the internet are being acutely felt in Asia Pacific, which is home to some of the largest and fastest-growing online communities in the world – the region accounts for the majority of social media users in the world. In this report, we examine the experience of countries from the GSMA Leading Nations engagement (comprising Bangladesh, India, Indonesia and Pakistan), which have seen rapid growth in misleading or inaccurate content online across a wide range of issues, including Covid-19. In this context, addressing false information online has become a priority for stakeholders in the information ecosystem in Asia Pacific and elsewhere.

With the amount of false information online set to grow further and delivery mechanisms likely to change as technology evolves, confronting this pressing challenge requires a 'whole-of-society' approach. In some cases, governments have created dedicated units to engage with stakeholders, monitor the spread of false information and conduct digital literacy campaigns to better equip citizens to navigate around false information. Citizens have a role to remain vigilant against false information and support stakeholders in their efforts. For their part, mobile operators are complying with country-specific laws and licence conditions while assisting their customers by promoting the proper use of technology.

This report examines the efforts of stakeholders as they seek to balance the impact of false information with the impact of various countermeasures to address the spread of misinformation and disinformation online. Targeted efforts by the appropriate stakeholders, specifically tailored towards false information online, have the potential to address the problem and cultivate a safer, more enriching digital experience for all internet users and, at the same time, mitigate the effects of overbroad countermeasures.

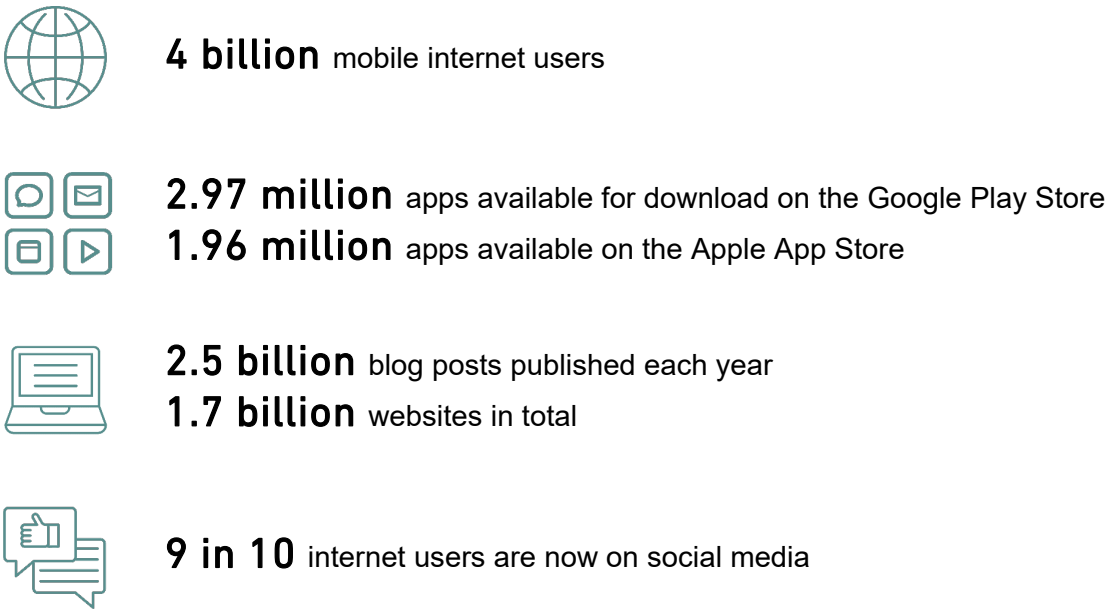
1. Misinformation and disinformation in the internet era

Society has grappled with the dissemination of misinformation and disinformation well before the arrival of the internet, with examples dating as far back as ancient Rome.[1] Although both terms involve false information and are at times used interchangeably today, there is an important distinction to make around intent. Misinformation refers to the spread of erroneous information, but not with the intention of causing harm – for example, disseminating outdated information or unproven theories about a given subject. On the other hand, disinformation generally refers to a deliberate, coordinated and malicious attempt to spread false information. This is often with the intention to harm a person, social group, organisation or country, or to gain money, power, influence or reputation.

1.1 False information spreading faster online

The arrival of the internet brought a different dimension to the spread of information, with false information at times permeating the digital world faster than real news.[2] With more people relying on online communities and platforms for social interactions, the internet has become a primary way for them to seek and validate information on a variety of subjects. A large amount of information online comes from credible sources and is generally trustworthy. Online fact-checking websites have also become more mainstream, offering people a way to check the veracity of online information. However, a sizeable and growing volume of false information online means that people, particularly impressionable or less tech-savvy users, can easily become misinformed, with potentially dangerous consequences.

Figure 1: The rise in internet adoption, driven by mobile broadband networks and access to smartphones, has led to the rapid expansion of online communities around the world



Data as of December 2020
Source: GSMA Intelligence, DataReportal, Statista

In recent years, there has been a surge in false information online globally, resulting in rising concern among internet users. A poll by the Lloyds Register Foundation, with respondents from 142 countries, found that 57% of internet users, across all geographies, age groups and socioeconomic backgrounds, perceived false information on the internet as a major concern.[3]

There are a number of reasons why online channels make the spread of false information more rapid. These include:

- the scale of online communities, given that most of the world's population is now online
- the convenience and instantaneity of online channels relative to their offline counterparts
- the use of technological tools and techniques that drive virality, such as bots, videos and 'deepfakes'[i]
- the proliferation of user-generated content online, often unmoderated and unverified, through blogs, apps and social media platforms.

Bringing people online has a net positive impact on society

Since 2014, nearly 2 billion people around the world have connected to the mobile internet for the first time. By 2025, around 5 billion people will be using mobile internet services. The Covid-19 pandemic has highlighted the importance of connectivity and the contribution of the mobile industry in efforts to realise the UN's Sustainable Development Goals (SDGs), as digital technologies help to improve people's livelihoods. Those who have had access to the internet during the pandemic have depended on it to work, learn, shop, seek employment, get medical help and stay connected with loved ones. This means that unconnected populations have been excluded from many life-enhancing and life-saving online content and services.

1.2 Impact of false information online on society

The global nature of the internet means that false information can spread across borders in real time. The Covid-19 outbreak – the first pandemic in the internet age – is a case in point. Evidence from internet search data shows an explosion in user-generated content on the pandemic and people responding to reports of the outbreak by immediately seeking information about the virus (from predominantly internet-based sources). Consequently, Covid-19 has been referred to as an infodemic[ii] in public health.[4] Other related types of inaccurate information being spread via the internet include claims of risk from 5G networks to public health and the myth linking 5G to the spread of Covid-19.[5]

Public interest on various topics may vary from country to country. As a result, the impact and consequences of the spread of false information are mostly felt in local communities. This does not make it less damaging. National health authorities around the world have noted how online misinformation on prevention and treatment therapies for Covid-19 undermine efforts to control the spread of the pandemic within local communities. The 5G/Covid-19 myth has resulted in

[i] Deepfakes are synthetic images and videos created by artificial intelligence (AI) technologies using aggregated existing media. They can be satirical or benign but have also been created for more harmful purposes, such as manipulative video clips of politicians and celebrities. According to start-up Sentinel, the number of deepfake videos online jumped from 14,678 in 2019 to 145,277 by June of the following year. For more information, see https://www.dataguidance.com/opinion/international-deepfakes-and-their-risks-society

[ii] An infodemic is a situation in which a lot of false information is being spread in a way that is harmful.

harassment of engineers and the vandalisation of telecoms infrastructure in several countries. It has also led to protests and even pressured local governments to delay 5G rollout plans.[6]

The wide range of themes targeted by false information online, including particularly sensitive areas such as politics, climate change, religion and health, makes the impact even greater. Outcomes for affected individuals and communities include increased stigmatisation and victimisation, human rights violations, and even violence in some cases. At a global level, a report published by the Royal Swedish Academy of Science warned that false information could jeopardise efforts to tackle environmental challenges such as climate change – an area in which the mobile industry has become increasingly engaged.[7]

Arguably the most significant and widespread impact of false information online, irrespective of the theme or target audience, is the growing mistrust of institutions and the disruption of democratic processes around the world. This could have dire consequences for social cohesion and inclusive progress in affected communities and wider society in the long term.

Covid-19 and 5G conspiracy theories

Researchers identified five phases in the evolution of false information linking 5G to Covid-19 on Facebook between January and mid-April 2020:[8]

- **Phase 1 –** Posts were mainly about pre-existing conspiracy theories (including claims of 'toxic' 5G emissions). On 20 January, a French-language blog linked the virus outbreak with a claim[iii] that there was substantial 5G deployment in Wuhan, China.
- **Phase 2 –** The Wuhan-5G connection claims crossed into English and began to spread widely among Facebook communities across the world (including in non-English speaking countries).
- **Phase 3 –** From late February, claims around 5G-activated vaccines coincided with the implementation of national lockdown measures.
- **Phase 4 –** In the second half of March, false claims emerged that Africa had seen few Covid-19 cases because it was not a priority for 5G rollout. This phase was also marked by claims that lockdowns were a way to facilitate 5G installations.
- **Phase 5 –** Late March to mid-April saw arson attacks[iv] in several countries, including the UK, the Netherlands, Belgium, France, Italy, Cyprus, Sweden and New Zealand.

Following these attacks, the World Health Organization (WHO)[9] added 5G to its Covid-19 Mythbusters list on 8 April 2020. Other authorities and mainstream media outlets have also expanded fact checks on 5G conspiracies, while social media companies have used warnings and labels, and have even blocked content that links Covid-19 with 5G. Attacks on masts subsided in the second half of 2020 but there were new incidents in France and South Africa in January 2021. In India, myths linking Covid-19 to 5G resurfaced in May 2021 following the announcement of plans for 5G trials and network deployment.[10]

[iii] The UK fact-checking organisation Full Fact addressed the claim on 29 January 2020 (see https://fullfact.org/online/wuhan-5g-coronavirus/).

[iv] The GSMA identified 332 arson attacks across 21 countries between March 2020 and March 2021 based on data from media reports and MNO trade associations. In the Asia Pacific region, there were 17 attacks in New Zealand and six in Australia.

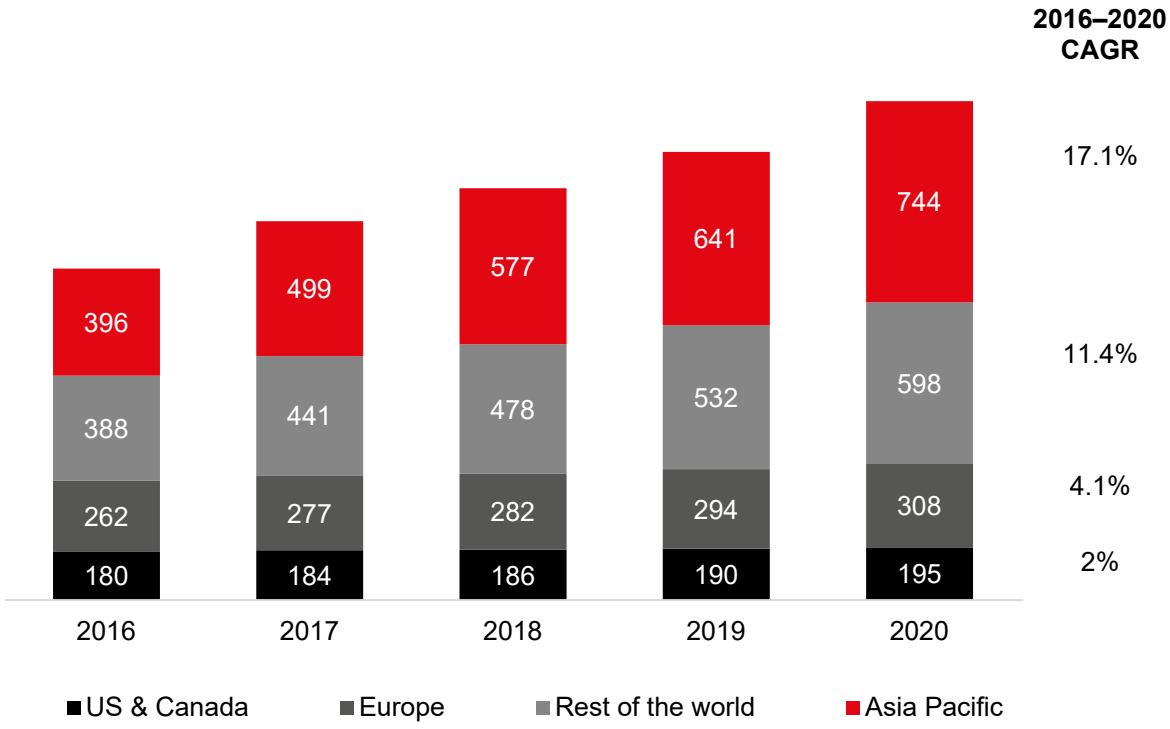
1.3 Asia Pacific: trends in false information online

Asia Pacific is home to some of the largest and fastest-growing online communities in the world. Excluding China, the region has more than 1.2 billion mobile internet users, equivalent to a third of the total number globally. Asia Pacific is a diverse landscape, featuring some advanced mobile markets and others at an earlier stage of digital development. It is this latter group of emerging markets where new subscriber growth has been most profound in recent years, driven by mobile operator investment in extending network coverage and efforts to address barriers to mobile internet adoption and usage.

Social media adoption is also growing rapidly in Asia Pacific, which is home to the majority of social media users. By number of active users, seven of the 20 largest Facebook markets, seven of the largest 20 Twitter markets and six of the 20 largest Instagram markets are in Asia Pacific. Of the social media platforms, Facebook is the largest in the region, accounting for 79% of all social media accounts in Asia Pacific. As of April 2021, there were over 330 million Facebook users in India alone, making it the largest Facebook market by number of users. The other Asia Pacific countries in the global top 20 markets for Facebook are Indonesia (140 million), the Philippines (85 million), Vietnam (70 million), Thailand (52 million), Bangladesh (43 million) and Pakistan (43million).[11]

Figure 2: Facebook has more users and is growing faster in Asia Pacific than in any other region

Number of daily active users (million)



Source: Facebook

Like in every other region, there has been much false information online around Covid-19 in Asia Pacific since the start of the pandemic:

- In Bangladesh, 85 major misinformation posts at the start of the pandemic garnered around 1.87 million interactions on social media.[12]
- Analysis of claims debunked by five Indian fact-checking websites between January and June 2020 shows that Covid-19 accounted for 58% of 1,447 false information posts circulating online.[13] Fact-checking organisation BOOM observed that 35% of the false or misleading claims about Covid-19 were circulated with videos.[14]
- In Indonesia, the Indonesian Ministry of Communications and Informatics/Kementerian Komunikasi dan Informatika (MCI/Kementerian Kominfo) discovered 1,513 'Covid-19 hoax' posts circulating on social media between 23 January 2020 and 6 April 2021.[15] The Indonesia Anti-Slander Society (Mafindo) also considers that disinformation has played a role in limiting vaccine take-up: the non-profit organisation recorded 712 hoaxes about vaccines between January and November 2020.[16]
- Pakistan has been severely impacted by false Covid-19 information, leading the government to launch a website (www.covid.gov.pk) to restrict the spread of fake news further online.
- Thailand's Anti-Fake News Centre, under the Ministry of Digital Economy and Society, recorded nearly 500 'fake news' posts about Covid-19 between January and June 2020, with the number of incidents peaking at 151 in March.[17]
- In Vietnam, the government identified 654 cases of Covid-19 misinformation online between January and May 2020.[18]

Aside from Covid-19, there has been an increase in the spread of inaccurate and potentially harmful online content on issues around politics, religion, health and climate change. In many cases, deliberate disinformation efforts have been directly linked with violence against vulnerable individuals and communities. One of the most notable cases is the 2018 mob killings in India that occurred after rumours about child abduction went viral on WhatsApp.[19]

2. Countermeasures to the spread of false information online in Asia Pacific

Tackling false information online has become a priority for governments and other stakeholders across Asia Pacific. This has resulted in a number of countermeasures in recent years, some with significant implications for content creators, platforms, internet users and mobile operators. This section examines the roles and considerations for four groups of stakeholders in efforts to address false information online: mobile operators; other industry players (notably social media platforms); governments; and citizens and citizen organisations.

2.1 Mobile network operator countermeasures

Mobile operators (and other telecoms service providers) sit in a unique position on this issue: they provide the connectivity that powers online communities, acting as the transport layer for content, but are subject to laws on the confidentiality of communications and typically do not host content. With this in mind – in addition to the fact that many browsers, servers and communications services are encrypted from end to end – much of the responsibility to mitigate the spread of false information falls outside of the purview of operators.

There are often misconceptions that operators may be to blame for the spread of 'negative content'. Operators can, however, contribute positively to efforts to address false information online. Specifically, mobile operators can take the following actions.

Promote trustworthy sources

With large subscriber bases and established customer relationships, operators can play a supportive role by pointing customers towards useful information on relevant issues from credible sources. As has been demonstrated in Pakistan, operators can utilise their own channels to steer customers towards verifiable, accurate information, such as links to government awareness campaigns on an operator's website or communication directly to subscribers (within the boundaries of data protection laws).[20] Some operators have also warned customers of potential cyber fraud and offered advice on how to stay safe while connected.[21] In Australia[22] and New Zealand,[23] operators have used humour to tackle false claims about 5G on social media and in specific communities. In Indonesia, all operators have come together to disseminate trustworthy information by broadcasting SMS messages on a daily basis with Covid-19 related information and reliable sources of information.

Enhance digital literacy

Beyond responding to false information, operators can take proactive steps to promote connectivity as a platform for collaboration, entrepreneurship and freedom of expression, as well as civic participation in issues such as fighting climate change. Efforts to promote digital literacy, capacity building and ICT skills could equip citizens, especially children, to use technology to fully participate in the digital world in a safe way. In November 2018, Telenor began its free Digital School programme to train 100,000 students across Myanmar, building on its earlier Digital Summer School initiative.[24] Operators could also consider partnering with local experts such as children's non-governmental organisations (NGOs), charities and parenting groups to help shape their messaging and reach the intended audience.[25]

Comply with legal obligations

Mobile networks are used by some to spread false information and illegal content. Laws and licence conditions typically require operators to retain data about their customers' mobile service use and disclose it, including personal data, to law enforcement and national security agencies on lawful demand. They may also require operators to have the ability to intercept customer communications following lawful demand.[26] Mobile network operators act as a mere conduit to the transmission of content on their networks; they do not view the content itself, and their consequent protection from being liable for such material is fundamental to the balancing of rights and legal processes.

That said, operators have robust processes in place that enable the swift removal or disabling of confirmed instances of illegal content hosted on their services while balancing the need to protect customer privacy – for example, by having procedures in place for the timely compliance with 'notice and take-down' orders upon receipt of a judicial order.[27] In Asia Pacific, many operators also adhere to the GSMA's Mobile Privacy Principles to provide openness, transparency and notice to their customers.[28]

2.2 Other industry-led countermeasures

Whether it be misinformation surrounding 4G and 5G networks, Covid-19 vaccines or sensitive themes such as politics or religion, social media platforms have been widely used to disseminate false information. Social network providers have a crucial role to play in addressing false information. Specifically, social media platforms can do this by taking the below steps.

Stem the spread of dangerous content

False information is a growing problem, affecting both traditional media and social networks. Some social media firms conduct internal monitoring of their own platforms and channels, as well as external tracking across the online landscape, to identify the tell-tale signs of fake news that might harm users or the company's reputation, including false information about vaccines and climate change. Likely sources include malicious domains and fake websites, in addition to made-up rumours proliferated by bad actors and shared instantaneously by bot accounts, which influence social media algorithms and drive 'relevance', engagement and viewership.

Monitoring this kind of activity could be critical to preventing the spread of false information, propaganda and mistruths, thereby protecting users. WhatsApp has imposed additional restrictions on how frequently a message can be shared on its platform in an effort to curtail the spread of false information. Any message that has been forwarded five or more times faces a limit that will prevent a user from forwarding it to more than one contact at a time.[29] Facebook removes false information "that may contribute to physical harm", while other types of misinformation have their distribution reduced.

Foster fairness and transparency

For social media platforms, the challenge of identifying and controlling false information is exacerbated by the need to avoid constricting legitimate free speech – particularly since there is often no clearly defined boundary between the two. Consequently, social network providers aim to be mindful of the sensitivities around censorship (i.e. removing or blocking content in an arbitrary way) and encroachment of citizens' rights to express themselves or access information. In Indonesia, Facebook has worked with the government and media partners to identify and remove

posts and user-generated content containing misleading information.[30] It has also created the Facebook Oversight Board to review and issue recommendations on Facebook content policy actions.[31] Twitter produces country-specific transparency reports that provide data on information and removal requests.[32]

Work with government and relevant authorities

Social network providers may need to act in some cases to prevent their platform being used to foment division and incite violence. The Australian Code of Practice on Disinformation and Misinformation could offer some lessons on how to prevent users succumbing to harm from false, misleading or deceptive content online.[33] Social media firms can engage with relevant authorities on issues pertaining to false information and help them understand how their technology and services work in practice, in order to support accountability and duty without onerous over-regulation. What's more, social media platforms can contribute positively to efforts to disseminate reliable and genuine information to citizens.

In India, WhatsApp has collaborated with the government and Haptik Technologies on the MyGov Corona Helpdesk bot solution, which people can text to obtain instant accurate and verified information about Covid-19.[34] In the event that they are subject to 'notice and action' orders, platforms should cooperate swiftly with law enforcement agencies. In Indonesia, the Global News Initiative has partnered with Mafindo and MCI/Kementerian Kominfo to run a media literacy programme to train the public to spot false information and hoaxes on the internet.[35] Mafindo has also created the TurnBackHoax website,[36] an archive of global fake news, and jointly developed fact-checking platform CekFakta[37] with Indonesia's Alliance of Independent Journalists (AJI) and the Association of Indonesian Cyber Media (AMSI), collaborating with firms from the tech, news and media industries.

Inform and educate users

Although they are not currently responsible for the posts of users, social media platforms simultaneously face criticism for silencing voices and acting as enablers of false information. Social media firms can implement reporting mechanisms for their users to flag content and could also consider informing users when certain accounts share illegal or deceptive posts. Facebook has announced that it will begin letting users know when groups violate the firm's community standards and reducing distribution of the content of these groups.[38] Some social networks have established community-based fact-checking services, such as Twitter's Birdwatch,[39] which can help individuals navigate and verify information, especially for user-generated content. Google extended the Google News Initiative, which aims to support quality journalism, to Asia Pacific in 2018.[40] Recently, Google provided $2.3 million in funding to news organisations across the region[41] and also provided a tool to help newsrooms detect fake images.[42]

Collaborate across sectors

Social media platforms are also working with other organisations from across the digital economy, with the potential to become a part of joint projects focused on preventing illegal and socially toxic activity online. Examples include the formation of the Coalition for Content Provenance and Authenticity (C2PA) in February 2021 and the safe.press consortium, which utilises blockchain (built using IBM's open-source Hyperledger Fabric) to track and verify information and to foster trust. The latter initiative is open to all newsmakers, from individuals to corporates, with members receiving a green safe.press stamp on the press releases or articles they publish, which acts like a "digital seal of approval".[43] In Vietnam, Viettel has worked with Facebook to resolve issues around fake accounts.[44] A further option to combat false information and build trust could be to adopt voluntary, industry-led codes of practice and standards, with specific provisions pertaining to the protection of vulnerable groups in the society.

2.3 Government-led countermeasures

The internet can be a tool for creating democratic and inclusive economies, where there is support for different voices and free exchanges of ideas and views. However, false information online can derail this by eroding public confidence in the state and institutions. There is a need for verifiable facts rather than opinions to shape minds and consensus; otherwise this could lead to a trust deficit, which has serious consequences for democracy and society. In this context, governments in Asia Pacific have undertaken a number of efforts to tackle false information online. In most cases, the rationale is to maintain social cohesion and protect the integrity of institutions, as well as to protect vulnerable individuals and communities. Below, we highlight countermeasures implemented by governments, principally those of Bangladesh, India, Indonesia and Pakistan.

Identifying false information

As a first step, it is important to distinguish between misinformation and disinformation (see chapter 1 of this report). While opposing views should not immediately be classed as misinformation or 'wrongthink', disinformation threatens public confidence and distorts perceptions of independently verifiable facts, which can disrupt democratic processes and undermine trust in institutions. In Indonesia, the government has given communications ministry MCI/Kementerian Kominfo primary responsibility for dealing with false information, although it may request assistance from other departments such as the National Cyber and Encryption Agency (BSSN), which has been mandated to handle cybersecurity-related matters.

Establishing a dedicated unit

To combat clear and obvious cases of false information, some governments have established a dedicated unit to understand and tackle misconceptions around certain issues. Such units could open a dialogue with stakeholders, listen to concerns, monitor the spread of content online and ensure the rest of the government is well informed. MCI/Kementerian Kominfo has established a unit to monitor the spread of mis/disinformation on social media and other online platforms. In January 2018, the unit began using a 'web crawler', an internet bot, to actively seek out 'negative content' and flag websites for removal.[45] Similarly, the UK government's Rapid Response Unit was established in 2018 to identify and counter dangerous false information, utilising a find, assess, create and target (FACT) model in its operations.[46]

Nurturing digital literacy

Governments, through relevant agencies, have created digital literacy awareness campaigns to engage with, inform and reassure the public. These multi-channel communication efforts (i.e. websites, TV, radio and social media) enable governments to provide a bridge between politics and fact-based information, and help them to dispel myths and educate citizens about how to distinguish between what is fake news and what is genuine. Such campaigns may involve community and religious leaders to ensure that no group is disproportionately harmed by false information and that across society people have access to reliable and trustworthy information. In Bangladesh, the government has launched a campaign, 'Asol Chini', to counter false information on social media.[47]

Spotlight on Indonesia's GNLD initiative

In 2017, Indonesia – together with partner organisations – launched the Gerakan Nasional Literasi Digital (GNLD) Siberkreasi Kementerian Kominfo, or National Digital Literacy Movement of Indonesian Ministry of Communications and Informatics, to improve digital literacy and tackle the threat of 'negative content' online.[48] The multi-stakeholder forum has over 100 institutional partners drawn from the private sector, government agencies, civil society organisations, local communities, digital platform providers, media, academia, digital literacy activists and telecoms service providers. Since launching, the initiative has conducted digital literacy activities in 500 locations and engaged with over 420,000 active participants. It has also produced a variety of digital literacy materials, which have been downloaded more than 180,000 times and reached over 83 million Indonesians through social media, websites and other online platforms.[49]

Minimising internet shutdowns

With the outbreak of Covid-19, billions of people have become even more reliant on the internet for many social and economic activities. Government-issued service restriction orders (SROs) require operators to shut down or restrict access to their mobile network, a network service or an over-the-top (OTT) service. Orders can include blocking particular apps or content, restricting data bandwidth and degrading the quality of SMS or voice services. In some cases, operators may risk criminal sanctions or the loss of their licence if they were to disclose that they had been issued with an SRO. Between January 2012 and March 2021, there were more than 500 government-imposed internet shutdowns[v] across India, the highest number of internet blockages in the world.[50] Along with India, Bangladesh, Myanmar, Pakistan and Vietnam also reported to have imposed internet shutdowns in 2020.

Given the economic and human rights implications of internet shutdowns, governments should avoid this or only use them in exceptional and pre-defined circumstances.

Using laws and regulations to manage false information

Governments have been producing rules aimed at preventing the spread of false information online. As the adoption of new laws can be slow, countries have also used existing laws to address online misinformation. Below are examples of both new and existing rules to tackle misinformation:

- The Indonesian government has utilised the Information and Electronic Transactions Law (ITE Law) to address false information online. In response to criticism of the use of the ITE law, an inter-ministerial council was formed to review the law for potential reform. This review was completed in May 2021, and an implementing guideline has been passed to the public. MCI/Kementerian Kominfo has also issued Regulation No. 5 of 2020, which contains provisions that regulate access in certain circumstances.
- In Pakistan, the government introduced the Removal and Blocking of Unlawful Online Content Rules 2020 (the Rules) to guide the implementation of Section 37 (unlawful online content) of the Prevention of Electronic Crimes Act (PECA) 2016.[51] Its aim is to curb misinformation, such as fake news, as part of its wider strategy to address online content.[52]
- Bangladesh's parliament passed the Digital Security Act (DSA) in October 2018, following sectarian violence sparked by posts on Facebook.[53] The law criminalises a broad range of cybercrimes, including "negative propaganda" against the 1971 Bangladeshi war of independence and spreading of "defamatory data".[54] By October 2020, nearly 2,000 cases

[v] The intentional disruption of internet-based communications, rendering them inaccessible or effectively unavailable, for a specific population, location, or mode of access, often to exert control over the flow of information (Internet Society).

had been filed under the DSA, according to data from the Bangladesh Cyber Crime Tribunal,[55] with an upsurge in cases during the Covid-19 pandemic.[56] Meanwhile, in April 2020, Bangladeshi law enforcement agencies asked the Bangladesh Telecommunication Regulatory Commission (BTRC) to block 50 websites and 82 Facebook pages for spreading rumours regarding the Covid-19 pandemic.[57]

- In February 2021, India announced changes to its guidelines for social media platforms, on-demand video streaming services and digital news outlets. The new measures will require big social media companies to establish a grievance redressal mechanism and appoint executives to coordinate with local law enforcement. The guidelines also mandate social media companies with over 5 million users to enable traceability of end-to-end encrypted messages.[58] Moreover, the police have used current regulations to counter false information, arresting specific individuals for allegedly encouraging violence at protests by Indian farmers at the government's agricultural reforms.[59]

The approach of directly sanctioning individuals or groups for posting false information online is becoming more prevalent across Asia Pacific. In June 2021, Vietnam's Ministry of Information and Communications (MIC) issued a code of conduct on social networks to promote a healthy and civilised social network environment and stem the spread of false information and offensive content online.[60] Several countries have recently announced new laws and regulations against fake news or stronger penalties in the wake of the Covid-19 outbreak. This includes Cambodia,[61] Malaysia,[62] Philippines,[63] Singapore,[64] South Korea,[65] Thailand[66] and Vietnam.[67]

Adopting co-regulatory mechanisms

Online content-sharing service providers currently work on a notice and take-down basis: once they are notified of content that is illegal or breaches their terms of service, they act expeditiously to remove it. Much of this content moderation is done through automated tools designed by service providers themselves and scaled to their services, supervised by moderators employed by the service providers. However, such processes are governed by rules that are often not easily understood and subject to change. To tackle this challenge, self-regulation can be complemented by co-regulation. Existing co-regulatory initiatives, such as the EU Code of Practice on Disinformation, show promise, creating an accountability mechanism and opportunities for online content service providers to share information and best practices on measures to fight disinformation.

Moving from a self-regulatory model to a more structured co-regulatory system also requires regulators to:

- define the role and responsibility of each actor in the co-regulatory model
- encourage broad membership, including a wide range of players
- outline fair and transparent processes for content moderation, which would be audited by the regulator
- introduce clear reporting requirements, more harmonised procedures and appropriate deadlines to respond to users or organisations that flag content
- improve transparency and user choice for the information that is exposed and consumed, as well as encouraging transparency in the recommendation and prioritisation of algorithms applied by online service providers without revealing trade secrets.

This co-regulatory approach would make the fight against online disinformation more effective and help to ensure balanced protection of users' rights.[68]

Participating in joint initiatives

Governments can take a collaborative approach to tackling false information online and, by extension, increase trust across the internet. Association of Southeast Asian Nations (ASEAN) countries have been cooperating to combat fake news for more than five years.[69] Meanwhile, since 2018 the EU Code of Practice on Disinformation has provided for an accountability mechanism and opportunities for online content service providers to share information and best practices on measures to combat disinformation.[70] Further, reliable notifiers could be helpful to identify the presence of such content and have it removed. Governments could also consider partnering with personalities, experts and influencers,[71] and engaging with accredited and independent 'trusted flaggers', encouraging their collaboration with hosting providers.

2.4 Citizens and citizen organisation countermeasures

Citizens are susceptible to the effects of false information and disproportionate countermeasures. However, citizen actions may also contribute to the problem with their interactions and activities online. This highlights the role of responsible digital citizenship in efforts to tackle false information online, which includes the following actions.

Develop public awareness of false information

Digital and media literacy is a critical factor in people's susceptibility to false information online. The Lloyds Register Foundation World Risk Poll reveals that a significant minority of people around the world are not aware of the risk of misinformation and disinformation.[72] This implies that citizens in this category can consume and transmit false information unknowingly, with potentially unintended consequences.

Citizen organisations have a role to play in supporting other stakeholders to increase awareness of the risks of false information online among citizens, and to teach them how to use online platforms responsibly. The number of fact-checking organisations has grown alongside the rise in online information. Fact-checking can encounter similar issues (e.g. fake fact-checking), but the International Fact-Checking Network is one organisation that promotes fact-checking best practices and a code of principles.[73] As of October 2020, Bangladesh, India, Indonesia and Pakistan all have active fact-checking sites.[74]

Remain vigilant

The growing adoption of the internet and smartphones has broadened access to information in all corners of the globe, offering people the ability to research almost any subject of interest and access worldwide media. However, not all information available online is factually correct, so there is an onus on citizens themselves not to facilitate the spread of false information, innocently or otherwise. This may mean reading beyond the headline on news articles and verifying information before attempting to share within their online communities. Social networks and internet-based messaging services, in particular, can serve as echo chambers, in which users can be manipulated or nudged into circulating fake news. Consumers should be aware of this risk and consider reporting content they feel is misleading to the platform administrator.

Support stakeholders

Citizen organisations can support people in several ways, not least by encouraging them to first and foremost rely on trusted sources of information. These organisations could consider establishing helplines and issuing guidance (in multiple languages) on how members can easily spot false information on social networks and in the media, and the importance of checking the source, the story and the intention in order to recognise fake news. Citizen bodies could also consider utilising their convening power to bring together representatives from business, academia, government, the media and members of the public, and provide spaces for them to converse and express concerns, empowering them to explore appropriate countermeasures to false information online.

Leverage prominent positions

Timely, trustworthy and actionable information is important, particularly in a pandemic. Without locally relevant information, false information can spread in a vacuum. To tackle this, trust is key to effectively address rumours and prevent the spread of inaccurate or false information. As trusted organisations, citizen advocacy groups can leverage their positions and platforms to alert the public and relevant authorities to misleading and potentially harmful content online. They could consider using various channels, social media being one, to run campaigns designed to counter false information and explore how they can lend support to government initiatives. Citizen organisations could also consider working with grassroots groups to strengthen their policy and advocacy work and messaging (e.g. around rights to free expression and access to information) and partner with relevant groups to protect vulnerable individuals and communities.

3. Limiting the negative impacts of countermeasures

The potential impact of the spread of false information online on society and the digital ecosystem is widely recognised. However, some countermeasures may have consequences that should not be underestimated. First, the approach of sanctioning individuals and groups for posting false information comes with the risk of violating international standards on human rights and freedom of expression. It also has the potential to limit the creation of valuable digital content and services as a result of self-censorship.

Second, there are valid concerns around provisions on traceability in some countermeasures and how weakening encryption could undermine the digital security and privacy of individuals. Critics of these types of rules, in some countries, claim that access requirements to people's online conversations and metadata means that the data can be used to target individuals for online content deemed harmful or misleading, with limited right to appeal.[75] These rules may also apply to internet service providers, including telecoms operators, in addition to social media companies,[76] raising questions about the implications for service providers that do not have visibility of the content transmitted across their network and are therefore unable to specifically address the flow of false information.

As such, guidelines should be targeted specifically to slow or stop the dissemination of viral content at issuance. For example, guidelines should target hosting services that play an 'active' role in the dissemination of content online, share such content with a broad audience or have the technical means to swiftly identify and remove users' specific content on a piece-by-piece basis.[77] Moreover, focusing the responsibility on where the vast majority of harm actually occurs avoids putting undue or disproportionate burdens on other service providers (such as telecoms providers) that do not facilitate false information, but rather serve as conduits for connectivity.

Of particular note is the blunt use of internet shutdowns to limit the flow of information. Internet shutdowns can undermine users' trust in the internet, with knock-on effects for the advancement of the digital economy and the reliability of critical online government services. They also come with a number of challenges:

- **Economic impact**: Society increasingly relies on internet connectivity for a broad range of economic activities and various business operations. These can be severely disrupted, thereby reducing productivity and generating economic losses in time-sensitive transactions, during internet shutdowns. Digital security and rights group Top10VPN estimates that there were over 27,000 hours of intentional internet shutdown in 2020, which cost the global economy $4 billion in lost productivity.[78] India's total internet downtime added up to 8,927 hours, resulting in economic losses of $2.8 billion.[79]
- **Human rights impact**: In 2016, the United Nations (UN) declared internet access a basic human right.[80] The importance of digital rights has been brought into sharp focus by the Covid-19 outbreak. Those who have had access to the internet during the pandemic have depended on it to live in the 'new normal', while those excluded may have had to work past new obstacles created by movement restrictions and other public health measures.

Mobile operators are directly impacted by internet shutdowns, as well as other measures designed to counter false information online. In addition to the loss of revenue caused by a shutdown,[81]

mobile operators also face reputational damage, pressure from authorities and possibly even retaliation from the public as a result of these countermeasures.

Service restriction orders (SROs)[82] are appropriate in exceptional and pre-defined circumstances, and only if absolutely necessary and proportionate to achieve a specified and legitimate aim that is consistent with internationally recognised human rights and relevant laws. SROs issued to operators should be made in writing, citing the legal basis and with a clear audit trail to the person authorising the order to promote due process, oversight and transparency. Allowing operators the ability to investigate the impacts on their networks and customers and to communicate freely with their customers about the order also promotes fairness and transparency. If it would undermine national security to do so at the time when the service is restricted, citizens should be informed as soon as possible after the event.

The challenges brought by SROs can be avoided or mitigated if the SROs are narrowly targeted by minimising the number of demands, the geographic scope, the number of potentially affected individuals and businesses, the functional scope and the duration of the restriction. Ultimately, all SRO decisions should first and foremost be made with the safety and security of the operators' customers, networks and staff in mind, and with the aim of being able to restore services as quickly as possible.

Looking ahead

The challenges of online misinformation and disinformation can be wide-ranging and felt at the individual, community and national levels. Governments across the region have initiated or ramped up measures to counter false information online. Social media companies and civil society organisations have also implemented measures to help tackle this challenge and raise digital literacy levels among citizens. Looking ahead, continued collaboration among these and other stakeholders through a 'whole-of-society' approach will be crucial to finding the appropriate balance of countermeasures to enable a safe and inclusive online environment for individuals and communities.

As this is an ongoing stakeholder dialogue, with approaches to misinformation and disinformation continually evolving, the GSMA welcomes comments on this report. This feedback will drive the conversation forward in future efforts. To submit feedback, please contact the GSMA at apac_enquiries@gsma.com.

References and further reading

[1] Journalism, 'Fake News' & Disinformation, UNESCO, 2018

[2] "Study: On Twitter, false news travels faster than true stories", MIT News, March 2018

[3] Fake news is the number one worry for internet users worldwide, The Lloyd's Register Foundation World Risk Poll, 2020

[4] D. Banerjee, K.S. Meena, COVID-19 as an "Infodemic" in Public Health: Critical Role of the Social Media, 2021

[5] "Authorities should lead in addressing 5G EMF misinformation", GSMA, November 2020

[6] "5G: Masts at centre of row in Bath", BBC, December 2020

[7] "Climate fight 'is undermined by social media's toxic reports'", The Observer, March 2021

[8] A. Bruns, S. Harrington, E. Hurcombe, Corona? 5G? Or both?': The dynamics of COVID-19/5G conspiracy theories on Facebook, 2020

[9] "Coronavirus disease (COVID-19) advice for the public: Mythbusters", World Health Organization, May 2021

[10] "No link between 5G technology and COVID-19 spread", Government of India Ministry of Communications, May 2021

[11] Statista

[12] "Youth volunteers bust COVID-19 myths and combat misinformation", Unicef, August 2020

[13] "Coronavirus: The human cost of fake news in India", BBC, July 2020

[14] "Fake News In The Time Of Coronavirus: A BOOM Study", BOOM, May 2020

[15] MCI/Kementerian Kominfo

[16] "'There's no virus here': An epic vaccine race against all odds in Indonesia", Washington Post, March 2021

[17] See COVID-19 Infodemic Management: Thailand Experience

[18] Nguyen TTP, Nguyen DC, Nguyen ATT, Nguyen LH, Vu GT, Nguyen CT, Nguyen TH and Le HT, Fake News Affecting the Adherence of National Response Measures During the COVID-19 Lockdown Period: The Experience of Vietnam, 2020

[19] "India 'WhatsApp child abduction rumours': Five more lynched", BBC, July 2018

[20] "Zong 4G and UNICEF Pakistan Partner to Create Awareness around COVID-19", UNICEF, April 2020

[21] "Telcos issue advisory against fake messages promising free recharges", ET Telecom, April 2021

[22] "Get the facts on 5G from our 5G Chief Investigator", Telstra Exchange, October 2020

[23] "Vodafone NZ and Ngahere Communities myth-bust global 5G conspiracy theories", Vodafone, December 2020

[24] "Telenor commences free Digital School program to train 100,000 students across the country", Telenor Myanmar, November 2018

[25] Guidelines for Industry on Child Online Protection: Mobile Operators' Version, ITU, UNICEF, GSMA, 2014

[26] GSMA Mobile Policy Handbook, GSMA, 2019

[27] Ibid.

[28] Mobile Privacy Principles: Promoting consumer privacy in the mobile ecosystem, GSMA, 2016

[29] "Facebook's WhatsApp limits users to five text forwards to curb rumors", Reuters, January 2019

[30] "Inside Indonesia's 'fake news' war room, fighting political hoaxes in election season", CNA, April 2019

[31] https://oversightboard.com/

[32] https://transparency.twitter.com/

[33] "Battling to reduce the spread of dis- and misinformation online", Addisons, March 2021

[34] "India launches WhatsApp chatbot to create awareness about coronavirus, asks social media services to curb spread of misinformation", TechCrunch, March 2020

[35] "Stop Hoax Indonesia program to educate internet users in 17 cities", The Jakarta Post, August 2019

[36] https://turnbackhoax.id/

[37] https://cekfakta.com

[38] "Facebook is cracking down on violence and misinformation in Groups", Business Insider, March 2021

[39] "Introducing Birdwatch, a community-based approach to misinformation", Twitter, January 2021

[40] "Google's News Initiative heads to APAC with grants of up to $300K for media orgs", TechCrunch, November 2018

[41] "Google gives $2.3M to 18 news organizations in Asia Pacific", TechCrunch, April 2020

[42] "The new tool helping Asian newsrooms detect fake images", Google, 2020

[43] "Can blockchain block fake news and deep fakes?", IBM, November 2020

[44] "Viettel to work with Facebook on fake account accusations", VnExpress International, February 2020

[45] "Gov't Launches 'Web Crawler' to Seek Out Negative Internet Content", Jakarta Globe, January 2018

[46] "How the Rapid Response Unit actually works (and why it's important)", PRWeek, October 2018

[47] "Govt launches campaign to make people aware of fake info", Prothom Alo, September 2020

[48] "Indonesia's National Digital Literacy Movement gains wider reach", OpenGov Asia, January 2019

[49] MCI/Kementerian Kominfo

[50] Statista

[51] See https://moitt.gov.pk/SiteImage/Misc/files/Social%20Media%20Rules.pdf

[52] See https://www.techagainstterrorism.org/2020/10/06/online-regulation-month-pakistan/

[53] "How is Bangladesh's Digital Security Act muzzling free speech?", DW, March 2021

[54] "President signs Digital Security Bill into law", Dhaka Tribune, October 2018

[55] "Bangladesh: Escalating attacks on the media must stop", Amnesty International, October 2020

[56] "Upsurge in Digital Security Act cases during the Covid-19 pandemic", Dhaka Tribune, June 2020

[57] "Govt to block 50 websites, 82 Facebook pages for spreading rumours", Business Standard, April 2020

[58] "Govt announces new social media rules to curb its misuse", The Hindu, February 2021

[59] "India's new social media rules seen echoing globally", The Economic Times, March 2021

[60] "Vietnam Tightens Grip on Social Media under the New Code of Conduct", Lexology, June 2021

[61] "Activists: Cambodia's Draft Cybercrime Law Imperils Free Expression, Privacy", Voice of America, October 2020

[62] "Malaysia imposes emergency law to clamp down on Covid-19 fake news", The Straits Times, March 2021

[63] "Jail time, up to ₱1-M fine await peddlers of fake COVID-19 news", CNN Philippines, March 2020

[64] "Singapore Fake News Laws: Guide to POFMA (Protection from Online Falsehoods and Manipulation Act)", SingaporeLegalAdvice, February 2020

[65] "Korean govt pushes for heavy fines for fake news", Dunya News, June 2021

[66] "Thailand: Proposed initiatives to combat 'fake news' undermine freedom of expression", Article 19, June 2021

[67] "Vietnam introduces 'fake news' fines for coronavirus misinformation", Reuters, April 2020

[68] Accelerating mobile internet adoption: policy considerations to bridge the digital divide in low- and middle-income countries, GSMA, 2021

[69] "ASEAN Ministers jointly declare framework to combat fake news", OpenGov Asia, May 2018

[70] GSMA's Views on the European Commission's Public Consultation on the European Democracy Action Plan, GSMA, September 2020

[71] Countering online misinformation resource pack, UNICEF, 2020

[72] Fake news is the number one worry for internet users worldwide, The Lloyd's Register Foundation World Risk Poll, 2020

[73] https://www.poynter.org/ifcn/

[74] https://reporterslab.org/fact-checking/

[75] "Pakistan: Social media curbs shrink free speech space", DW, December 2020

[76] "Draconian internet rules", Dawn, November 2020

[77] A Telecoms Industry View on the Digital Services Act, GSMA, ETNO, 2020

[78] "The Global Cost of Internet Shutdowns", Top10VPN, January 2021

[79] "How India lost $2.8 billion to internet shutdowns in 2020", The Times of India, January 2021

[80] See https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

[81] "India's internet shutdowns costing mobile carriers millions of rupees in lost revenue", Reuters, December 2019

[82] See https://www.gsma.com/publicpolicy/mobilepolicyhandbook/consumer-protection#service-restriction-orders

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com