Trusting the internet: An overview of anti-disinformation laws

March 2020

As new cases of the novel coronavirus disease known as COVID-19 continue to emerge, so too do reports and posts on the internet and social media platforms about it – many of which have proven to be misleading or outright false. From posts about the source of the virus and its health impact, through to the impact on basic supplies such as toilet paper, the coronavirus has brought into sharp focus the importance of being able to trust what we read online. In this article, we take an in-depth look at the state of the law in Hong Kong SAR and Mainland China, as well as developments aimed at addressing the challenges of disinformation in Hong Kong SAR and Mainland China, as well as in Singapore and the UK.

Existing anti-disinformation laws in Hong Kong SAR and Mainland China

Hong Kong

State of the law

In Hong Kong, there is no legislation which specifically combats the spread of online disinformation. Currently, authorities rely on existing laws, created largely to deal with real-world issues, to combat misconduct that occurs online. For example, in the context of the current coronavirus crisis, an individual was recently arrested for posting online messages stating that individuals near their workplace were infected by coronavirus. The police relied on the Summary Offences Ordinance, which prohibits people from sending messages which they know to be false, for the purpose of causing annoyance, inconvenience or needless anxiety to anyone else.[1] Other examples of laws that could be used to pursue action against a wrongdoer include criminal intimidation under the Crimes Ordinance, blackmail under the Theft Ordinance, libel laws and common law offences such as incitement to commit public nuisance.

All of these, of course, rely on being able to locate the perpetrator of the false information and being able to enforce the law against that person in the relevant jurisdiction (made all the more difficult by online anonymity and the global reach of the internet). Enforcement against platform operators based outside Hong Kong remains difficult, particularly in jurisdictions without applicable mutual legal assistance arrangements with Hong Kong – an issue that become pronounced in 2019 in relation to the Dubai-based instant messaging tool Telegram.[2]

(1) https://www.scmp.com/news/hong-kong/law-and-crime/article/3048986/hong-kong-man-arrested-suspected-spreading-fake-news
(2) https://www.scmp.com/news/hong-kong/law-and-crime/article/3036007/hong-kongs-ban-posting-online-material-inciting

Official requests to remove online content

In recent years, various government bodies have made requests to online platform operators to remove certain postings. These requests are typically subject to the platform operator's policies on user content and community standards. Unsurprisingly, there was a huge increase of such requests in 2019 in the midst of the Hong Kong protests on the grounds that certain postings violated the community standards of the platform because they contained fake news or hate speech. However, from statistics published by the Innovation and Technology Bureau, such requests have only been partially acceded to, as platform operators are not obliged by Hong Kong law to remove such content and content removal remains subject to the discretion of platform operators.[3]

Mainland China

By contrast, under Chinese law the spread of disinformation for the purpose of disturbing social order is prohibited, as is posting content which (among other things) contradicts constitutional principles, jeopardises national security or incites ethnic hatred.[4] Platform operators have various legal duties to curb the dissemination of disinformation.

Duty to identify and verify user information

When platform operators provide users with information publication services, they must require users to provide their real identity information at the time of entering into the relevant online service agreement.[5] Platform operators are then required to verify user identity, which suggests that technology companies are expected to play a key role in enforcing cyber norms, and not to act merely as neutral providers of online platforms.

Duty to manage published content

Article 47 of the Cyber Security Law (CSL) requires platform operators to strengthen their management of information published on their platforms and to take appropriate measures if they discover disinformation on their platforms. While the CSL does not specify what steps precisely a platform operator must take to "discover" disinformation, it is provided in other regulations that platform operators are, at minimum, required to establish a mechanism to examine and manage published content.

In that regard, the Provisions on the Governance of Network Information Content Ecology, enacted in March 2020, provide a framework for platform operators to establish a content management mechanism, including:

- formulating rules on content governance;
- improving response systems for "rumors" (谣言) and "black industry chain information" (黑色产业链信息);
- assigning personnel to be responsible for content governance; and
- setting up facilities to receive user complaints and reports, which must be promptly processed and actioned by the platform operators.

(3) https://gia.info.gov.hk/general/201912/11/P2019121100578_332416_1_1576055810720.pdf
(4) Article 15, Administrative Measures for Internet Information Services; see also Article 56, Telecommunications Regulations of the People's Republic of China.
(5) Article 24, Cyber Security Law of the People's Republic of China.

Additional requirements for content management mechanisms may be imposed by administrative authorities or industrial self-discipline organisations, depending on the specific service offered by a particular platform. For example, if a platform allows users to comment on news reports, then the platform operator is required by the Cyberspace Administration of China (CAC) to establish a pre-publication examination system to vet user comments (rather than rely on post-publication review).[6] Such pre-publication examination requirements are also imposed on platforms for short videos by the China Netcasting Services Association, in addition to duties to set up teams of examiners and to maintain blacklists of users who repeatedly or severely violate rules.[7]

Duty to report disinformation

Upon discovery of disinformation, platform operators are required to immediately stop transmission of such content, take measures to delete or otherwise prevent the disinformation from spreading, retain relevant records of their actions, and report to the relevant authorities.[8]

Liabilities of Platform Operators in Mainland China

Failure by a platform operator to fulfil its legal duties may attract administrative, civil and criminal liabilities.

For administrative liability, a platform operator that fails to perform its duty to manage and report disinformation to relevant authorities will be required to rectify its failure. For severe violations, registration authorities of platforms may suspend licenses or order an operator to shut down its website, depending on whether paid services are provided.[9]

In addition, failure to take measures to stop transmission of disinformation or to take down disinformation may trigger penalties on both the platform operator and on responsible personnel.[10]

The Chinese authorities may also adopt softer approaches to assist their supervision. For example, before imposing an administrative penalty on a platform operator, the CAC or its local branches may arrange for a meeting with the relevant platform operator to inform it of findings of illegality, the reasons and basis for proposed penalties, and the measures the platform operator is expected to implement to improve its content management mechanism.[11] This supervision method is milder and has less direct legal and regulatory implications as compared with imposing more traditional administrative measures (such as license restrictions, revocation or fines) and has been widely adopted by the CAC as an enforcement measure.

Criminal liability may be triggered when a platform operator fails its administrative duty, and fails to make corrections after the relevant authorities have conducted interviews or issued a penalty notice, resulting in the widespread dissemination of disinformation. Criminal liability may be imposed on both the platform operator and the persons in charge of the platform operation.[12]

(6) Article 2(3), Administrative Provisions on Internet Follow-up Comment Services.
(7) Article I and II, Management Standards of Network Short Video Platforms.
(8) Article 47, Cyber Security Law of the People's Republic of China.
(9) Article 23, Administrative Measures for Internet Information Services.
(10) Article 69, Cyber Security Law of the People's Republic of China.
(11) Article 35, Provisions on the Administrative Law Enforcement Procedures for Management of Internet Information Content.
(12) XXVIII, Amendment IX to the Criminal Law of the People's Republic of China.

Civil liability is usually reserved for situations when a party's rights or interests are infringed by a user of a platform and where the platform operator has been made aware of the offending conduct but fails to take necessary action (for example, to delete or block the offending content or break links to stop the spread of the offending content).[13]

A comparison with other jurisdictions

United Kingdom

In the UK, the government is pushing forward the first online safety laws of their kind in the world, designed to impose a heavier burden on technology companies to protect users from various online harms, including online disinformation.

The online safety laws were proposed in the Online Harms White Paper (White Paper), followed by a public consultation period which closed on 1 July 2019. In February 2020, the UK government published its initial consultation response (Response).

In brief terms, the White Paper proposed the following major areas of reform:

- appointing a regulator to enforce stringent new standards;
- introducing a new statutory duty of care on all companies that allow users to share or discover user-generated content or interact with each other online, regardless of the company size;
- granting the regulator with powers to issue substantial fines, block access to sites and impose liability on individual members of the senior management.

Duty of care – in the context of online disinformation

The Response indicates that the proposal that companies should be required to do what is "reasonably practicable", taking into account what is proportionate in the circumstances in light of the company's user base and the likely severity of the harms, has been met with a positive response. It is expected that a code of practice will be issued, which outlines expectations on how technology companies should fulfil their proposed duty of care.

In the context of online disinformation, technology companies will face a range of new obligations to:

- set out guidance in their terms of service as to what constitutes disinformation, the expectations they have of users, and the penalties for violating the terms of service;
- use fact-checking services;
- make content which has been disputed by reputable fact-checking services less visible to users;
- promote authoritative news sources and diverse news content;
- ensure a reporting process is put in place to enable users to easily flag content that they suspect or know to be false;

(13) Article 36, Tort Law of the People's Republic of China.

- ensure that algorithms that automate the dissemination of content are not manipulated or abused; and
- publish data that will enable the public to assess the overall effectiveness of the actions these companies are taking to address the issue.

It is expected that the chosen regulator (which the Response indicates may be the existing telecoms regulator, Ofcom) will adopt a risk-based approach, prioritizing regulatory action to tackle harms that have the greatest impact on individuals or wider society, and taking into account factors such as the type of services offered, service size and whether there are any known issues with serious harms.

Enforcement measures

In the White Paper, the issue of cross-border enforcement was specifically addressed. The White Paper suggested that these reforms should apply to all companies that provide services to users located in the UK, regardless of whether they have a legal presence in the UK. The appointed regulator is envisaged to be able to take enforcement action against foreign companies, including blocking platforms from being accessible in the UK as a last resort. It is also possible that companies not based in the UK will be required to appointed a UK or EEA-based nominated representative, similar to the concept of nominated representatives under the GDPR.

In the Response, the UK government also promised to further consider senior management liability and business disruption measures. More details will be set out in the final policy position paper, which is due to be published later this year.

Industry response

While policymakers around the world start to consider regulation of platform operators, the White Paper is the most far-reaching proposal so far. The industry, unsurprisingly, have challenged the White Paper proposals for being too broad, undermining privacy, and producing a chilling effect on freedom of speech.

In the Response, the UK government pledged to respect the freedom of speech and several safeguarding measures were proposed. For example, the new law would differentiate between “illegal content” and “content that has potential to cause harm”, making it clear that it would not be compulsory for companies to remove the latter. In addition, it is not envisaged that the regulator will consider individual complaints. The UK government emphasized in the Response that the primary aim of the new law is to ensure that platform operators have systems and processes in place to deal with online harms, and it is ultimately up to platform operators to decide what content and behavior they deem to be acceptable on their sites.

Singapore

In Singapore, the Protection from Online Falsehoods and Manipulation Act (POFMA) came into effect on 2 October 2019. POFMA seeks to regulate the electronic communication of false statements of fact or misleading information. Under POFMA, a person must not communicate a statement which that person knows, or has reason to believe, is false, if that statement is likely to (among other things) prejudice national security, public health or safety, public tranquillity, influence elections, incite hatred or diminish public confidence in the Singapore government.

Liability of platform operators

Platform operators are classified as "Internet Intermediaries" for the purposes of POFMA. Under POFMA, Internet Intermediaries can be directed to send corrective notices to specific end users, to publish corrective notices generally and to disable access to content. If a website contains three or more items that have been subjected to directions under POFMA, the website may be declared as a "Declared Online Location". The operator must then notify end-users that the website is a "Declared Online Location". Failure to comply with directions or obligations under POFMA may result in penalties and site blocking orders.

These powers were used against Facebook in November 2019, when Facebook was directed to publish a notice underneath a posting of claims about election rigging and the alleged arrest of a whistleblower to alert users that the post contained false information.[14] In February this year, Facebook was again ordered to disable access to a news page, which had put up a Facebook post claiming that Singapore had run out of face masks.[15]

Self-regulation: what measures do tech companies put in place to curb disinformation?

In recent years, tech companies themselves have been taking the lead to curb the spread of disinformation, and increasingly we see a transition from giving one-off responses to major incidents to putting in place systems which ensure effective identification of disinformation, adequate reporting and appeal mechanisms.

In response to the widespread dissemination of coronavirus-related disinformation and misinformation, different tech giants have been implementing measures to contain the spread. For example, WeChat has installed a "fact-check platform" and Tencent has limited or shut down user accounts with a history of publishing disinformation about coronavirus. Other efforts made by tech companies include measures to make disinformation harder to access in search results, providing links to credible sources of health information and engaging third parties to undertake fact-checks of online content.

(14) https://www.thestar.com.my/news/regional/2019/12/01/facebook-complies-as-singapore-govt-begins-using-anti-fake-news-law
(15) https://www.bbc.com/news/world-asia-51556620

Some tech companies are taking a further step to set up comprehensive systems to ensure user-generated content is factually accurate. For instance, Facebook is setting up an Oversight Board, an independent panel which adjudicates on disputed content on Facebook (such as political advertisements which contain inaccurate statements). Weibo, the Chinese-equivalent of Twitter, set up a "rumor refuting platform" in 2015, through which users can report alleged false content. According to an annual report on Weibo's "rumor refuting data", Weibo handled over 77,000 pieces of disinformation in 2019.

What next?

The challenge of curbing online disinformation is not a new one – from controversies about electoral fraud to misleading information about vaccinations, and now, to fake news about the coronavirus, the ability to trust what we read online is becoming increasingly important. As regulators start to consider more stringent regulation of online platforms, operators are moving quickly to self-regulation.

We expect more tech companies to design systems to prevent and promptly detect the spread of disinformation, while regulators around the world will be closely watching the introduction of laws like those proposed in the UK. Events like the coronavirus have only strengthened the need for regulators and industry alike to ensure what we read on the Internet can continue to be trusted.

For additional information on our firm, please visit our website at **simmons-simmons.com.**

5340216v1