Asia-Pacific
Economic Cooperation

Advancing Free Trade
for Asia-Pacific Prosperity

Public-Private Dialogue on Status, Trends, Opportunities and Threats of Social Networks

APEC Telecommunications and Information Working Group

April 2022

Asia-Pacific
Economic Cooperation

Public-Private Dialogue on Status, Trends, Opportunities and Threats of Social Networks

APEC Telecommunications and Information Working Group

April 2022

APEC Project: TEL 09 2017S

Produced by
Ministry of Digital Economy and Society
The Government Complex
Chaeng Watthana Road, Laksi,
Bangkok 10210, Thailand
Telephone: +66 2 141 6903
Fax: +66 2 143 8029
Email: tip-arpa.t@mdes.go.th, pijitra.s@chula.ac.th

For
Asia Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#222-TC-01.1

Contents

Executive Summary

This paper is part of the proposal of the self-funded project, entitled Public-Private Dialogue on Status, Trends, Opportunities, and Threats of Social Networks, Thailand put forward in APEC TEL 56, held in December 2017 in Bangkok. In partnership with the Faculty of Communication Arts, Chulalongkorn University in Thailand, the project aims to promote the sharing of information and experiences between the public and private sectors, including NGOs and the academia, with a view to examining and updating the status, trends opportunities, and threats, as well as bringing forward current practices and recommendations on social network governance for future APEC collaborations.

To provide a foundation for this paper, two workshops were organized: 1) Workshop on Public-Private Dialogue on Status, Trends, Opportunities, and Threats of Social Networks, held in Taipei in October 2018 and 2) Multi-Stakeholder Regional Workshop on Social Networks and Digital Platform Governance in February 2019 in Bangkok. The information, views and experiences shared in the Workshops are incorporated into this paper. In addition, further studies are conducted by Chulalongkorn University's Faculty of Communication Arts to examine the subject of social network governance. As such, case studies of emerging governance structures and current practices in different regions, and recommendations to cope with the challenges of information disorder are included and form major parts of the paper.

The paper is divided into 3 main sections: 1) Regional and Global Status and Trends of Social Networks; 2) Case Studies and International Current practices on Social Network Governance in APEC; and 3) Challenges and recommendations.

On Regional and Global Status and Trends of Social Networks, this section shows that despite a trend of improvement in digital divide in APEC, there are emerging challenges in content regulation on social networks, as well as increasing vulnerabilities from rapid business expansion of the platforms, and the gaps in social network regulation. While on Case Studies and International Current practices on Social Network Governance in APEC, the section examines the practices of industry's

self-regulation, government's regulation, and regulatory collaboration between multiple stakeholders, be they government agencies, social/digital platforms, international organization and civil societies. These recommendations are drawn from various case studies and the discussions in the Workshops held in Taipei and Bangkok, various actors are undertaking some of the following practices:

1. APEC should promote free and fair competition, responsibility, and accountability, as well as the diversity among platforms.
2. APEC should encourage measures to strengthen the protection of personal information and privacy of users.
3. APEC should promote social network literacy among users, in conjunction with the efforts to monitor and curb harmful contents of false and harmful information with appropriate regard to principles such as free speech and privacy.
4. APEC should promote close consultation between all relevant stakeholders, where sharing current practices and lessons learned are encouraged
5. APEC should promote capacity building to develop experiences and expertise on relevant issues such as fact-checking, professional journalism on social networks to sustain quality of journalists. APEC should promote the maintenance of diversity and sustainability of the quality independent news media, through funding, supporting, and training of journalists and fact-checkers.

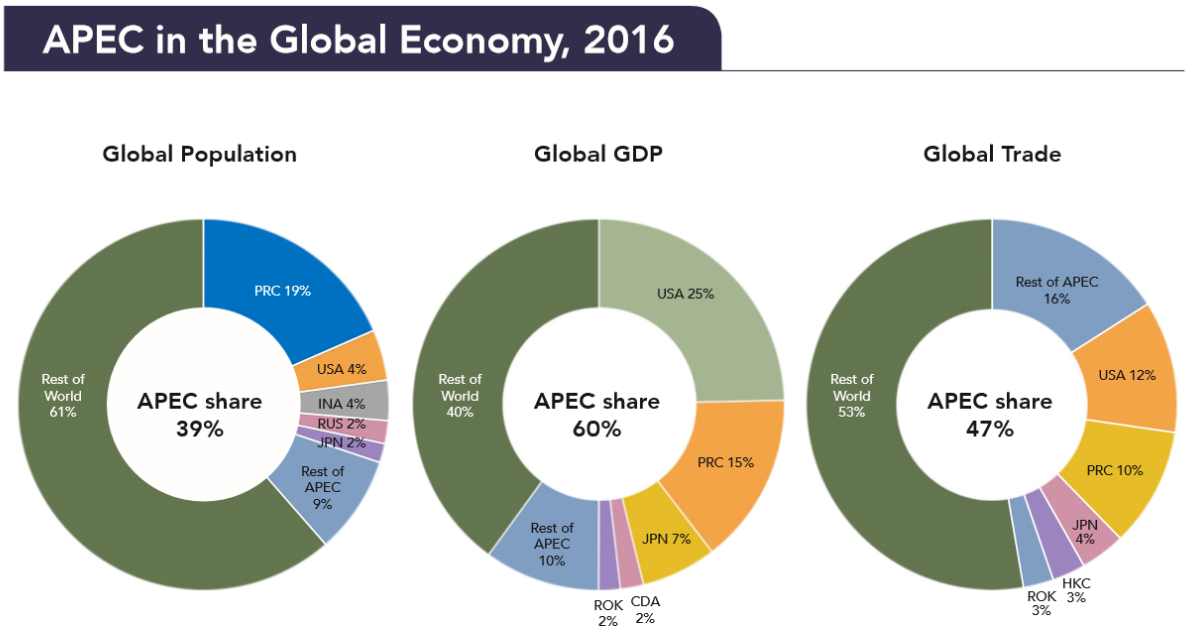
I. Regional and Global Status and Trends of Social Networks

1. Background and Rationale

APEC is considered the world's largest economic area, with its GDP and trade accounting for 60% and 47% of the global GDP and trade, respectively. More than one third of the world population lives in the APEC region. Naturally, the region is one of the world's most crucial markets for goods and services, including social network.

Throughout APEC economies, social network has become a vital part of social and commercial life. A large portion of APEC's population visits social media platforms every day. Therefore, it is clear, from the demand side, APEC stands as the world's biggest market and social network community. From the supply side, the APEC region is both the birthplace and home to the world's biggest social network platforms, which operate across economies, such as Facebook, YouTube, LINE, WeChat, KakaoTalk, etc.

Figure 1.1: APEC in the Global Economy, 2016



Source: (APEC Secretariat, 2017)

However, the growth of social networks globally and in APEC economies has raised some challenges, e.g. privacy and data protection, or the spread of false and harmful contents. Hence, it is necessary to understand the characteristics and the dynamics of the social network, including its collective responses to such challenges.

In this respect, the first part of this report outlines the status and trend of social network across APEC and describes the diversity of platforms and their usages. It outlines potentials and problems that have emerged from the uses of social network. It also shed some light on how platforms and other stakeholders evolves in their responses to such opportunities and challenges.

Upon the growth of digital economy in APEC, there lie emerging challenges that has increasingly threatened trust, confidence, and stability of the regional economic development. The challenge can be characterized by the spread of false information and the proliferation of harmful online contents. As a consequence, public trust in media and the potential of the internet as a medium to produce a closer and more informed global community is being undermined.

The second part of this report outlines the complexities of false and harmful information across social network platforms in APEC and different regulatory frameworks. In addition, it discusses case studies of social network governance. The paper concludes in the third part of recommendation for APEC to enhance social networks for all users in the region.

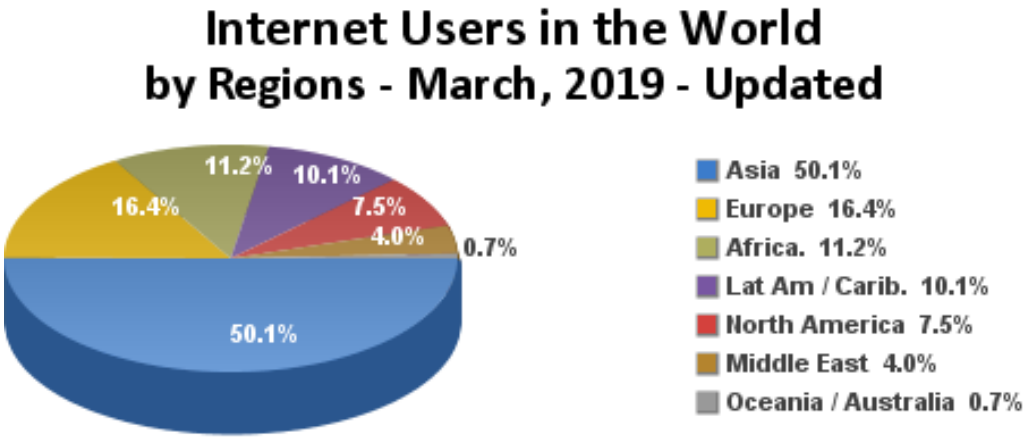
2. Global Status and Trends of Social Networks

The Internet World Report 2019 (Mini watts marketing group, 2019) shows that there are 4,388 million internet users around the world, while the number of social network users is 3,484 million. The internet and social network penetration rate increase by 9% from last year. In addition, the most popular devices remain mobile phones, whose users are numbered at 5,112 million, up 2% from 2018. In terms of the internet penetration by region, Europe and North America rank the highest, with their internet users accounting for 88% to 95% of the populations. In Southern Europe, the highest-growing region, there are 11% more internet users annually. Meanwhile, Latin America

ranks the second in the number of internet users. By contrast, Africa has the lowest number of internet users, only 12% to 51% of its populations.

In Asia, the number of internet users account for 50.1% of the global internet users, the highest rate, while the America and Europe regions constitute 17.6% and 16.4%, respectively. Africa makes up 11.2%, while the Australia and Oceania region has the lowest rate, accounting for 0.7% only.

Figure 1.2: Internet Users in the World by Regions in March 2019

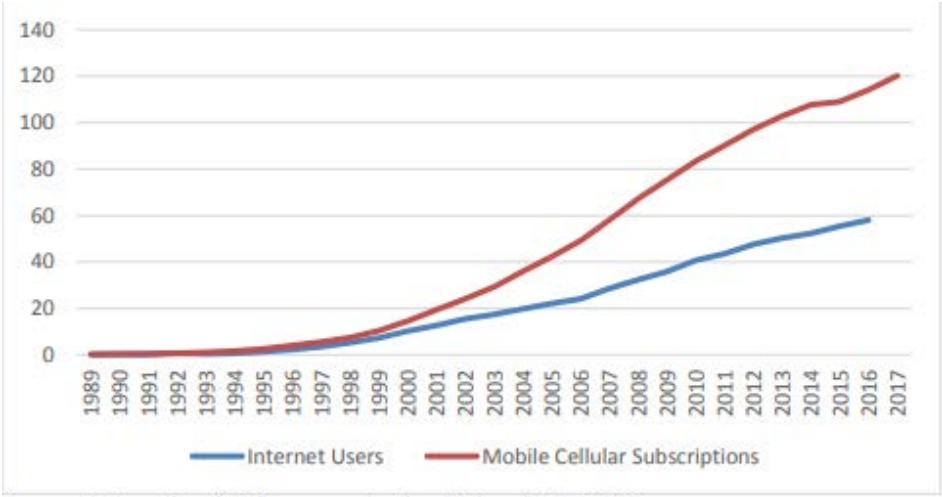


Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,383,810,342 Internet users in March 31, 2019
Copyright © 2019, Miniwatts Marketing Group

As for the global trend of social network, the mobile phones, particularly smart phones, play an important part in improving the internet and social network penetration rate. In the past, the users are now getting access to internet and social network through mobile devices, as opposed to PCs and laptops, as in the past (ITU, 2018). In this regard, social network platforms are more likely to pay more attention and respond to the demand and lifestyle of mobile and smart phone users. ITU data shows expanding of mobile phone user that increase from 1989 – 2017.

Figure 1.3 Digital technology per 100 people in APEC, 1989-2017

(Asia-Pacific Economic Cooperation Policy Support Unit, 2019)



Source: International Telecommunication Union; StatsAPEC.

In 2018 Users, on average, hold up to 8 different social network accounts, increasing by 2 times as many from the last 5 years (Globalwebindex, 2018). Latin America has the highest number of social network accounts, that is, averaging 9.1 networks. By contrast, North America has the lowest number of social network accounts, averaging only 6.6 networks. Moreover, the social network platforms, which provide messaging services, will experience more rapid growth than the traditional social network. The messaging applications, such as WeChat, WhatsApp, and Facebook Messenger, will have stronger growth than the social media platforms, like Twitter and Instagram (We are social, 2019).

In terms of content, video files will become valuable assets, with 28% of users on 4 major platforms (Facebook, YouTube, Facebook Messenger, and WhatsApp), not including China, tends to participate in live streams on social networks monthly. Facebook remains the most popular platforms for live video streaming. In other words, 59% of internet users currently consume the live content through social networks, while 27% of the figure creates and shares videos on regular basis.

In addition, instead of consuming news and information through traditional media, users are now going through social network platforms for news and a wide range of

information**.** Convenience and readiness are the deciding factors for the rise of social network as the main source of news and information**.**

The new social network platforms become more popular and help the legacy media **(**e.g., CNN and BBC**)** in disseminating their news reports through the platforms**.** Currently, CNN has 4**.**7 million followers on a Japanese messaging application, while LINE and BBC have been using WhatsApp and WeChat in India since the beginning of 2014**.**

3. The Status and Trends of Social Networks in the APEC region.

3.1 APEC Social Network Penetration

The number of social media users in 2019 as a percentage of the population varies across the region. Australia; Brunei Darussalam; Chile; Hong Kong, China; Indonesia; Malaysia; New Zealand; Philippines; Korea; Singapore; Chinese Taipei; Thailand and USA have a social media usage rate of more than 70% of the population. Canada; China; Japan; Mexico; Peru; Viet Nam; Indonesia; Russia range between 47% and 69% penetration in terms of social media use with Australia on the top end and Russia on the low end. Papua New Guinea is the outlier with just 9% penetration of social media.

In Brunei Darussalam; Chile; Indonesia; Mexico; Peru; Philippines; and Singapore social media penetration and internet penetration is identical or differs by just one percentage point. According to the statistics from We Are Social in 2019, developing economies in East Asia and Southeast Asia, which have lower internet penetration rate, use social media at a higher rate than developed economies, such as Canada and Japan, which have higher internet penetration rate.

3.2 Time Spent on the Internet around APEC

There is significant variation in the time spent on the internet by users in APEC economies (We are social, 2019). APEC's members particulary in Southeast Asia has among of the highest rates of internet usage in the world. The Philippines has the highest rate of time spent on the internet proximately 10 hours and 2 minutes per day.

Close behind the Philippines is Thailand where users report spending 9 hours and 11 minutes on the internet per day. Next is Indonesia with 8 hours and 35 minutes followed by Malaysia with 8 hours 05 minutes and Mexico with 8 hours 01 minutes on the internet per day. While most of APEC economies spend 7 – 5 hours on the internet per day such as Australian; Canada; China; Hong Kong, China; Korea; New Zealand; Singapore; Chinese Taipei; the USA and Viet Nam.

3.3 Bridging the Digital Divide in APEC

According to an APEC-endorsed study (AHSGIE, 2017), there is a reduction in digital divide, with the gaps in internet penetration being narrowed. With the Internet and Digital Economy Roadmap, APEC has promoted innovative, inclusive, and sustainable growth, as well as to bridge the digital divide in the APEC region. This emerging trend is most likely caused by the improvement in access to online technologies and the rapid growth in social media penetration in developing economies. The trend in social media acceptance from the users and the availability of the social media services in APEC's developing economies should continue to grow and help drive forward the economic development in the region for the foreseeable future.

3.4 Major Social Networks in APEC Economies

The APEC region has the most diverse and dynamic landscape of social media platforms in the world. It includes global leaders in the social media industry as well as lesser-known platforms with extensive reach in only a few economies. The global platforms, Facebook, and YouTube, are used in most of the region and play a role of mainstream media. Like Facebook, YouTube is given attention in this study due to its prevalence as a platform for accessing news. Digital platforms from USA expand their services throughout the APEC region, except in those large economies which possess 'economy of scale', and, therefore, can develop their home-grown platforms and applications for domestic users. Also significant in APEC economies are platforms that originate in Asian economies. Notable platforms are WeChat, QQ and Weibo from China, LINE from Japan, and KakaoTalk from Korea.

Figure 1.4 Top 3 APEC's most Popular Social Network Platform 2018

(We are social, 2019)

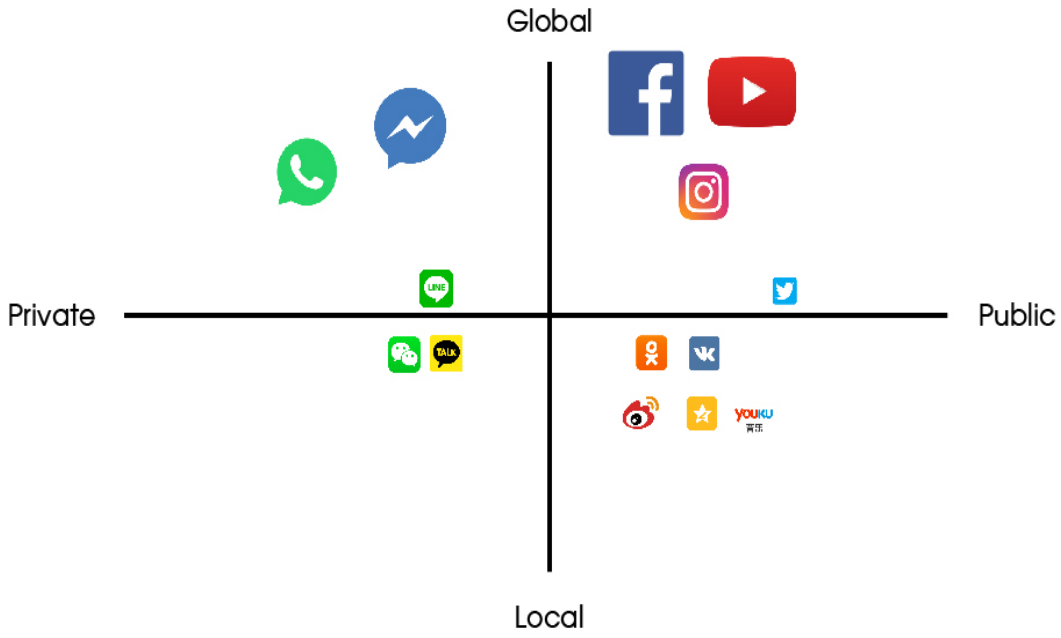
APEC Economies	*Top 3 Ranking popular platform (active use in social media)*		
	Top 1	Top 2	Top 3
Australia	Facebook (70%)	YouTube (68%)	Facebook (N.A.) Messenger (49%)
Brunei Darussalam	Facebook (N.A.)	YouTube (N.A.)	Instagram (N.A.)
Canada	YouTube (74%)	Facebook (72%)	Facebook (N.A.) Messenger (50%)
Chile	Facebook (N.A.)	YouTube (N.A.)	Pinterest (N.A.)
China	WeChat (46%)	Qzone (33%)	Youku (31%)
Hong Kong, China	Facebook (75%)	WhatsApp (74%)	YouTube (73%)
Indonesia	YouTube (43%)	Facebook (41%)	WhatsApp (40%)
Japan	YouTube (70%)	LINE (54%)	Twitter (45%)
Korea	YouTube (74%)	Facebook (62%)	Kakaotalk (58%)
Malaysia	Facebook (70%)	YouTube (69%)	WhatsApp (68%)
Mexico	Facebook (59%)	YouTube (58%)	WhatsApp (56%)
New Zealand	YouTube (74%)	Facebook (73%)	Facebook (N.A.) Messenger (56%)
Papua New Guinea	Facebook (N.A.)	YouTube (N.A.)	Instagram (N.A.)
Peru	Facebook (N.A.)	YouTube (N.A.)	Pinterest (N.A.)
The Philippines	YouTube (57%)	Facebook (56%)	Facebook (N.A.) Messenger (49%)

Russia	YouTube (63%)	VK (61%)	Odnoklassniki (42%)
Singapore	WhatsApp (73%)	YouTube (71%)	Facebook (70%)
Chinese Taipei	Facebook (77%)	YouTube (75%)	LINE (71%)
Thailand	Facebook (75%)	YouTube (71%)	LINE (68%)
USA	YouTube (73%)	Facebook (72%)	Facebook Messenger (51%)
Viet Nam	Facebook (61%)	YouTube (59%)	Facebook Messenger (41%)

Facebook and YouTube are the main public platforms used and carry different features and functionalities. On the one hand, Facebook is used to share information and interact with friends and the public through its peer-to-peer network. On the other hand, YouTube is mainly considered one-way communication to view visual information, as most users take a role as 'passive' audience. Moreover, APEC users are inclined to use the social network in parallel with the private messenger, global platforms, such as WhatsApp and Facebook Messengers.

In the APEC economies of North America, South America and Australia, Facebook Messenger and WhatsApp messaging platforms occupy the top two places as the most popular apps for smartphone messaging. However, the picture in Asia is very different. According to SimilarWeb, ten different messenger apps are making up the top two most popular apps in each economy of Northeast and Southeast Asia. They include Facebook Messenger, WhatsApp, Viber, WeChat, LINE, KakaoTalk, WeChat, QQ, BBM (Blackberry Messenger), Zalo - Gọi Video sắc nét (Bobrov, 2018). Many of these applications have expanded well beyond messaging and have become diverse social media and commercial platforms.

Figure 1.5 Categories of Popular Social Media and Digital Platform in APEC 2018



In addition, the home-grown platforms in some APEC economies, such as LINE, are being promoted as regional platforms. Some platforms, such as WeChat in China and Odnoklassniki in Russia, are created and mainly used as local ones, as the hosting economies possess economy of scale.

4. Challenges of Social Network in APEC

4.1 Social Network Platform Competition and Inter-sectoral Business Synergy

Despite the rapid growth of social media users in developing economies, there is a sign of maturing market for social media in more developed economies in the region. As a result, the competition between global social platforms is increasingly intensified. The strategies for creating and maintain the user base through network effect are implemented, including the strengthening of their role as intermediary platform for two-sided market-social media users and businesses in other sectors, including logistics, finance and banking, that require more interactive channels to online customers. Worth noticing is the trend of emerging business synergy between social media platforms and such businesses as news media, entertainment media outlets, etc., which allows the platforms to produce and provide professionally generated content

(as opposed to the prevalent user-generated contents), in the midst of heated competition for consumer's trust and demand for reliable information.

4.2 Lower Trust and concern on false information in social media

The Reuters Institute and Commonwealth bank's study (Reuters Institute, 2018) differentiates trust in various sources of news in selected APEC economies and finds that trust in news obtained through search engines and social media is particularly weak. Only 34% reported trusting the news they find in search engines most of the time. Trust drops even further when social media is considered. Only 23% of the global sample reported trusting news from social media most the time. These low levels of trust may undermine the capacity of the internet and social media to contribute to social and economic progress.

The low rate of trust in news accessed through social media reflects a growing public concern about falseinformation. The global public has developed a dangerous level of concern about news distributed through social media channels. According to the Reuters Institute Digital News Report, 54% of a global sample expressed strong concern about 'what is real or fake' regarding online news (Reuters Institute, 2018). The proportion of people has higher concern in Chile; Singapore; Australia; USA; Mexico and Korea. The Edelman Trust Barometer Global Report finds that nearly 7 in 10 people globally worry about false information being used as a weapon.

4.3 Privacy and data protection

There is also growing awareness on the issues of the violation of users' data privacy on social media platforms. The data breach in 2018 has higher occurrence, increasing 6.4% from the previous year (IBM Security, 2018). Disturbing cases of major hacking have been continually reported, including the online theft of IDs and passwords of 6.5 million user accounts of LinkedIn in 2012, as well as that of 'access tokens' of Facebook users in 2018. These incidents caused damages to businesses, and undermined users' trust in a serious way. As a countermeasure, governments around the world have intensified efforts to protect users' private data.

II. Case Studies and Current Practices on Social Network Governance in APEC

With the growth of social network penetration, there emerges more exposure of users to cyber threats. The users' ease of access to social network accounts through multiple devices, the lack of requirement for real identification registration, as well as the encryption of messages and conversations with the existing ability to share them to the large group of users, have made social network an effective channel for harmful messages, including those of terrorists and ill-willed political propagandists. Social network services range from networking services (e.g. Facebook, Twitter, and Instagram), content hosting services (e.g. YouTube), crowdfunding services (e.g. GoFundme.com, Youcaring.com, Kickstarter.com) and internet communication services (e.g. LINE, WhatsApp). In some cases, these services, providing different levels of connection and interaction, can be abused by criminals, and those with harmful intent, including terrorists. Through the use of false and harmful information, these ill-willed actors pollute the social network. At the same time, these services are also used to help protect the anonymity of targeted groups, such as political dissidents, activists, and minorities.

In the Asia Pacific region, cases of false information in social network have led to more active efforts and stronger commitments by stakeholders to stem the problem, particularly how governments can collaborate with industry to address malign propaganda, violent extremism, and criminal acts. The case studies of counter-terrorism and false information represent an effort of multi-stakeholders to ensure trust in social network platform. Based on the discussion and recommendations from the APEC Multi-stakeholder Regional Workshop on social media and Digital Platforms in Bangkok in 2019, this section presents some approaches to counter false information while protecting privacy and freedom of expression. Case studies are also included to give more detailed context on each presented practice.

1. The Case of Social Network Governance to Counter-terrorism

Terrorists use social networks to communicate violent extremist messages to a far wider circle of potential adherents than they could have reached with traditional media.

Today, big public social network platforms like Twitter, Instagram, Facebook, and YouTube, together with private messaging platforms, such as LINE, WhatsApp, etc., offer the ability to instantaneously convey one's message to users around the world. With crowdfunding emerging as a popular form of social network used for fund raising, problematic or harmful content and activities, including propaganda, extremist recruitment, and terrorist financing become more effective and widespread on social platforms and beyond. For example, the ISIS terrorists' official propagandists could create and disseminate up to 1,146 separate units of propaganda in 30 days (Winter, 2015).

The following analyses of the counter-terrorism measures, based on the official information available online, mainly focus on the regulatory efforts by relevant stakeholders. In addition, the case studies are drawn from the information and experiences, shared in the Multi-Stakeholder Regional Workshop on Social Media and Digital Platform Governance, in February 2019 in Bangkok.

1.1 Case Studies: Industry's self-regulation on counter terrorism in social networks

- **Facebook**

In 2017 Facebook investigated terrorist activities across the Facebook's family apps included Instagram and WhatsApp. With the Community Standard, Facebook relied on algorithms and the following technological techniques to track terrorist groups and activities:

1) Image matching: Facebook flag terrorist propaganda's images and videos are tracked and recognized to prevent the online upload.

2) Language understanding: Facebook use AI to recognize terrorist content through 'text-based-signals'.

3) Algorithms to find clusters: Facebook use AI to screen content from known terrorism-associated pages, posts, or accounts, and investigate related materials supportive of terrorism.

4) Other initiatives: Facebook use logo detection, audio matching and a 300+ subject matter expert team to reviews content and ensure new propaganda is also added to Facebook's photo and video matching system.

- **YouTube**

YouTube does not permit terrorist organizations to use the platform for any purpose, including recruitment. It also strictly prohibits content that promotes terrorism, such as content that glorifies terrorist acts or incites violence (Youtube, 2019). YouTube has developed tools and processes to find and monitor contents relating to terrorism as follows:

1) YouTube Trusted Flagger Program (Canegallo, 2019): This program helps provide robust tools for individuals, government agencies, and non-governmental organizations (NGOs) that are particularly effective at notifying YouTube of content that violates its Community Guidelines. YouTube recently increased independent experts to identify contents that are likely to be used to support radicalization.

2) Technology to detect violative content: YouTube has developed automated systems that aid in the detection of content that may violate policies. Potentially problematic content is flagged for human review. Machine Learning helps YouTube take down content before it is widely viewed. 98% of the videos YouTube removes for violent extremism are flagged by machine-learning algorithms, machine learning is helping YouTube's human reviewers remove nearly five times as many violent extremist videos than previously. In addition, over 90% of the videos uploaded in September 2018 and removed for violent extremism had fewer than 10 views (Youtube, 2019).

3) Human Content Reviewers: YouTube proactively increased its content reviews by human and take a tougher stance in scanning for videos that do not clearly violate its original content policy.

4) Redirect method: YouTube is also working with partners to support the expansion of the Redirect Method (redirect method, 2018) to divert those target audiences deemed most susceptible to violent extremist messages towards alternative videos, which debunk the harmful messages and recruitment narratives.

- **Twitter** (Twitter, 2019)

Proprietary spam-fighting tools: Twitter develops machine learning tools that identify and take action against networks of spammy or automated accounts automatically rather than waiting until they receive a report (Harvey, 2019). Twitter has taken a collaborative approach to develop and implement these changes,

including working in close coordination with experts on its Trust and Safety Council. The Global Internet Forum on Counter-Terrorism (GIFCT) reported that between July 2017 and December 2017, a total of 274,460 Twitter accounts were permanently suspended for violations related to the promotion of terrorism. Of those suspensions, 93% consisted of accounts flagged by internal, proprietary spam-fighting tools, while 74% of those accounts were suspended before their first tweet.

1.2 Case Studies: International Fora and Organizations on counter terrorism in social networks

- **GIFCT**

The Global Internet Forum on Counter-Terrorism (GIFCT) is an industry-led initiative to substantially disrupt terrorists' ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence using social network platforms. GIFCT works in close partnership with the UN Counter-Terrorism Executive Directorate (UN CTED), and the Tech Against Terrorism initiative to share knowledge and expertise. GIFCT's efforts can be categorized as follows:

1) Technological Solutions: GIFCT members have created a shared industry database of "hashes". A hash is a unique digital fingerprint that can be used to track digital activity across platforms. When pro-terrorist content is removed by one GIFCT member, its hash is shared with the other participating companies to enable them to block the content on their own platforms (Macdonald, 2018).

2) Research: GIFCT is supporting a Global Research Network on Terrorism and Technology **(** GRNTT**)** aimed at developing research and providing policy recommendations around the prevention of terrorist exploitation of technology by RUSI in the United Kingdom (Macdonald, 2018)**.**

3) Knowledge sharing: GIFCT provides a formal structure to share current practices around counter-terrorism. The Forum supports workshops and meetings with smaller companies to help them better tackle terrorist content on their platforms.

4) Global multi-stakeholder engagement: The GIFCT carries out global workshops to share knowledge between tech industry, government and civil society. In partnership with Tech against Terrorism. As of today, there have been 11 workshops on 4 continents. The GIFCT has engaged with over 120 tech companies.

- **European Commission and the Code of Conduct**

Measures are taken by the European Commission to counter hate speeches online through the endorsement of the EU Code of Conduct on Countering Illegal Hate Speech Online in 2016 (European union, 2017). The Code of Conduct not only aims at curtailing hate speeches online, but also targets the use of violent extremist messages and terrorism propaganda, through the close collaboration between global social network and digital players, such as Facebook, Google, Twitter, and Microsoft. Within this collaboration, the EU's Code of Conduct encourages the private sectors, especially social network platforms to engage in 'privatized enforcement', including the suspension and removal of active accounts participating in terrorism propaganda.

- **OECD Voluntary Transparency Reporting Protocols**

Following the Christchurch attacks and the Osaka G20 Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism, Australia partnered with the OECD, and co-financers New Zealand and Korea to develop a Voluntary Transparency Reporting Protocol (VTRP). This project is bringing together industry, governments, academia, and civil society to establish a common protocol for online platforms to publicly report what steps they are taking to prevent, detect and remove terrorist and violent extremist content.

The VTRP will strengthen online platforms' public reporting on preventing terrorist and violent extremist content online, and support industries and government's ability to analyse, compare and react to emerging trends. The VTRP also supports the operationalisation of the Christchurch Call commitment made by industry to implement regular and transparent public reporting in a way that is measurable and supported by clear methodology.

1.3 Case Studies: Role in Countering Terrorism in social media

- **#NotAnotherBrother by The Quilliam Foundation**

Civil society organizations, such as the Quilliam Foundation, have an important role in fighting against terrorism, through promoting awareness and literacy programs with a

view to enhancing understandings in terrorists' tactics in social network. The programs make use of valuable insight data in data analytics and promote counter narratives against the terrorism and extremism ones. The Foundation has made an impactful counter-terrorism effort by releasing the full version of a new counter-extremism video as part of our #NotAnotherBrother campaign.

- **Tech Against Terrorism**

Tech Against Terrorism is a project, run by Quantspark in pursuit of the UN Security Council resolution 2354 (2017) and the UN Counter-Terrorism Committee Comprehensive International Framework to Counter Terrorist Narratives. It works with multiple stakeholders, including the global technology industry, to tackle terrorists' use of the internet, whilst respecting human rights. It encourages the development of an online knowledge sharing platform, advocating the strengths of an industry-led, self-regulatory approach. It also partners with the Global Internet Forum to Counter Terrorism (GIFCT) to share current practices and tools between major tech and social network companies and smaller tech companies. A closed webinar is organized to convene cross-sector experts to initiate discussion and find ways to use machine learning, data analytics, and AI to understand and stem the use of the internet for terrorist purposes.

2. Case Studies of Social Network Governance to Counter False information

The problem of information disorder in social network are likely to exacerbate in the election period. Social networks and online platforms play a role in elections, democratizing access to the political process for both the candidates, political parties, and electorate as channels of information exchange. However, we have also seen these channels misused to spread false information. The widespread uses of political propaganda and discourses based on false or fabricated information leads to the strengthened efforts at social network governance to stem the problem of false information, which will be elaborated in the case studies as follows:

2.1 Case Study: Centralized and Top-Down Regulation

This approach of government- led regulation ensures that the public interest is prioritized, and the rights to privacy and personal information are upheld and respected by social network companies. In addition, the governmental agencies are legitimate,

leading actor in promoting cybersecurity and ensuring public safety from false and harmful information on social networks. Interesting cases of centralized, top-down regulations on social network are presented as follows:

- **Australia**

The Australian Government has issued a draft online safety charter (Australian Government, 2018), which outlines what the Australian Government expects of technology companies operating in Australia. It includes expectations regarding the identification, moderation, and removal of harmful and illegal contents, aiming to protect children from cyber bullying and violence. There are requirements for products and services such as "built-in" child safety mechanisms as well as accountability and transparency measures.

In 2015, Australia enacted the Enhancing Online Safety Act to establish what is called the eSafety Commissioner. The Commissioner has the power to identify and remove illegal online content - via a legislated take-down scheme for online illegal and child sexual abuse materials. The Commissioner also provides a complaint service for young Australians who experience cyberbullying. Platform companies are required to comply with notices issued by the commissioner to remove cyberbullying material or face penalties. The Commissioner has powers to issue notices to individuals who post cyberbullying material and request that they take the material down, refrain from posting further cyberbullying material or apologies to the child who is the target.

In 2018, the Commissioner was given additional powers to facilitate the rapid removal of intimate images to combat the non-consensual sharing of intimate images.

In 2019, the Australian Government passed new legislation aimed at reducing the incidence of online platforms from being misused by perpatrators of violence. The legislation created two new offfences that require industry to take action to report to police, and to expeditiously remove access to, abhorrent violent material.

- **Malaysia**

In March 2018, former Malaysian Prime Minister Najib Razak proposed a draft of the Anti-Fake News Bill 2018 to the Parliament, in the midst of the intense election

campaign. Later in April that year, the Malaysian Parliament passed the draft Bill, introducing an anti-fake news law specifically tailored to countering the information disorder.

The Bill defined fake news as the information, news, or report, the content of which was false, misleading in part or in whole. It applied to the content, appearing in the press and media in forms of text, visuals, and sound, including those on digital and social media platforms. The Bill carried the penalty of fine (up to 500,000 Ringgit) and imprisonment (up to 6 years) for the offenders, Malaysian or foreigners, residing in Malaysia or abroad, who intentionally spread the false information that affected the economy or its people (Anti Fake News Bill, 2018). However, later after the election, the government coalition successfully pushed the House of Representatives to repeal the Bill, but the Senate later blocked the repeal effort by the House. So far, the Bill is still in effect (Business Insider, 2019).

- **Singapore**

In May 2019, the Singaporean Parliament passed the Protection from Online Falsehoods and Manipulation Bill (POFMA), which provides a suite of measures to address the impact of specific individual falsehood and source of falsehoods. The measures fall into the following categories: (1) providing access to and increasing the visibility of corrections, (2) disrupting fake accounts that amplify falsehoods, (3) discrediting online sources of falsehoods, and (4) levers cutting off financial incentives of online sources of falsehoods. According to the Bill, the government is empowered to order platforms and individual publishers to not only remove any false information, but also make a correction statement, if considered necessary and in the public interest (Government, Singapore, 2019). In addition, criminal offences apply to malicious actors who deliberately undermine society using falsehoods, which carries the harsh penalty of fine of up to 1,000,000 Singapore Dollars for non-individuals, or fine of up to 100,000 Singapore Dollars and/ or imprisonment of up to 10 years for individuals, depending on the severity of the offence. It is worth noticing that the Bill is also applied to the personal messaging services, including the closed, encrypted social network platforms, such as Whatsapp. However, the POFMA does not give the government any powers to view or modify the contents of personal messages. When the government becomes aware of falsehoods that are spreading through personal

messages on a sufficient scale to impact the public interest, and the government becomes aware of it, the government may require other open platforms to carry corrections to counter the falsehoods on these closed platforms.

2.2 Case Studies: Self-Regulation of Tech Industry

To tackle certain challenges, self-regulation of industry has proven to be an effective approach. In the context of the Internet industry, self-regulation enables online platforms and digital service providers to respond to challenges based on their technical know-how, while also preserving opportunities for innovation and economic growth. However, a key consideration in self-regulatory efforts is the need for multi-stakeholder discussions on the social, economic, and political implications of the online challenges the platforms seek to address. In addition, transparency is also a core issue to ensuring self-regulatory approaches are effective.

- **Facebook**

Facebook has played a leading role in the fight against the false or/and harmful information, through the following tools:

1) **The Community Standard Policy:** As part of its platform's content regulation,

its Community Standards aim to create healthy and non-harmful content on the platform. The Community Standards are maintained through the support of users who are encouraged to notify Facebook if they identify content that violates the standards. In addition, Facebook gives its users the option to report, block, unfollow, or hide people and posts, so that they can control their own experience on Facebook. Community Standards are regularly refined. Every two weeks there is an internal debate on the standards, which leads to regular updates. The Community Standards are supported by a team of reviewers who assess flagged content. The reviewers assess content in 50 languages and operate 24 hours a day, seven days a week. They are subject to rigorous training and regularly audited. To ensure the quality of the process, the auditors are also audited.

2) **Facebook Journalism Project**: By promoting the availability and quality professional produced content on platform, the Journalism Project reflects the Facebook's commitments to compete with mis-information and false information for

public awareness. This represents the collaboration with news organizations to develop products together and provide tools and services for journalists.

3) News Integrity Initiative: A global consortium, representing close collaboration between Facebook and professional media and tech companies, focuses on helping people make informed judgments about the news they read and share online.

4) Investigative Tool: Facebook launched a new "investigative tool" to prevent the dissemination of false news and propaganda during Election.

5) Third Party Fact Checking Initiative: This program is created to counter false information on the platform. Facebook works with the third-party fact-checkers who are certified through the non-partisan International Fact-Checking Network (Poynter, 2015) to help identify and review false news. The program develops the process of analysis and response with regards to false news as follows: 1) identifying false news 2) reviewing content by Factchecker to check its facts and rate its accuracy 3) showing false content lower in News Feed 4) taking action against repeat offenders.

- **YouTube**

Google implements various product strategies to counter false information that are relevant to YouTube (SPSG, 2019)[1].

1) Make Quality Count: YouTube deploys effective product and ranking systems that demote low-quality false information and elevate more authoritative content. For example, two cornerstone products - the Top News shelf and the Breaking News shelf - prominently display authoritative political news information.

2) Counteract Malicious Actors: YouTube rigorously develops and enforces content policies. The platform protects the integrity of information tied to elections through effective ranking algorithms, and tough policies against users that misrepresent themselves or who engage in other deceptive practices. YouTube removes monetary incentives through heightened standards for accounts that seek to utilize any of YouTube's monetization products.

3) Give Users Context: In certain instances, YouTube provides users with additional information through information panels with publisher or topical context to help them better understand the sources of news content they watch.

[1] White Paper: How Google Fights False information

4) The Community Guidelines (Youtube, 2018): There are several policies in YouTube's Community Guidelines that are directly applicable in some form to false information. These include policies against spam, deceptive practices, scams, impersonation, hate, and harassment. The platform will issue warnings and strikes to the accounts, whose contents have violated the community guideline. Unless there is an adequate action taken by the account owners to remove the problematic contents within 90 days, the accounts will be indefinitely shut down (Youtube Help Center, 2019). General users can report to the platform admin any inappropriate content, through flagging notification.

5) The Google News Initiative: Youtube also supports journalism with technology that allows news to thrive. One example of this is collaboration on the Google News Initiative, a program that provides funding for journalism and houses products, partnerships, and programs dedicated to supporting news organizations in their efforts to create quality, independent reporting that displaces false information.

- **LINE**

LINE represents a private platform, whose contents are encrypted private conversation between users. According to its content policy, LINE prioritizes the protection of privacy and private information. That said, LINE also takes steps towards countering false and harmful information, through the following tools:

1) LINE Today: As the main channel for reliable, professional news on the platform, LINE Today focuses the attention onto sourcing news from authoritative partners and developing specialized content partners to mitigate the possibility of dissemination of falsehoods through LINE News.

2) Digital Literacy Program: LINE has been conducting digital literacy programs in Japan and Thailand[2]. In Japan, they run LINE Youth Digital School camps. They develop digital literacy teaching materials together with an education expert.

2.3 Case Study of Co-regulation

[2] In Thailand, LINE has partnered with ETDA (Electronic Transaction Development Office Public Organization) to conduct Digital Literacy programs.

- **The Case of European Union**

European Union formed a high-level group of experts (The HLEG) to advise on policy and current practices to counter fake news and the spread of false information online. The report's recommended multi-dimensional approach rests on five pillars:

1.1. enhance transparency of online news.
1.2. promote media and information literacy to counter false information and help users navigate the digital media environment.
1.3. develop tools for empowering users and journalists to tackle false information and foster a positive engagement with fast-evolving information technologies.
1.4. safeguard the diversity and sustainability of the European news media ecosystem.
1.5. promote continued research on the impact of false information in Europe.

The HLEG recommended the countering of False information in steps, as follows:

1) First step: In short to medium term, self-regulation should be promoted, based on a binding implementation roadmap, inclusive of participation from stakeholders, with a set of specific actions. A code of practices should be established and committed by all relevant stakeholders, be they online platforms, news media, journalists, fact-checkers, independent content creators or the advertising industry. Objectives and principles, particularly freedom of expression, as well as roles and responsibilities of each stakeholder should be clearly defined in the code of practices. A coalition of multi-stakeholders should be formed to ensure the first step is implemented, with monitoring and reviewing processes.

2) Second step: In this step, co-regulation should be promoted. The European Commission should be invited to examine and assess the progress of the first-step implementation, including the implementation of the code of practices. The public authorities at national and EU levels should play a facilitating role to ensure continuous monitoring and evaluation of the code's implementation, and to support research on information disorder. The code of practices must be backed by a structured cross-border and cross-sector cooperation, network, or body, involving all relevant stakeholders, in order to foster transparency, algorithm accountability and public trust in media to an appreciable extent.

The Code of Practice has been well received by the global platforms[3], which lead its implementation. Concrete steps taken can be summarized as follows:

1) **Google** improved the scrutiny of ad placements in the EU and provided an update on its election ads policy.
2) **Facebook** provided further information on its political ads policy, which would apply also to Instagram. The company launched a new, publicly available Ad Library globally
3) **Twitter** updated its political campaigning ads policy and provided further details on the public disclosure of political ads in Twitter's Ad Transparency Centre.

3. Current practices on Social Network Governance

Based on Twitter's self-regulation of the content on its platform, in the second half of 2016, of the 376,890 accounts suspended for posting terrorism-related content, just two percentages were the result of the governments' requests to remove data. This figure is an example of the commitments made by the global platforms in the fight against information disorder. In addition, the self-regulation efforts at both the company and industry levels are developed on the foundation of collaboration and agreement on common standards of practice on countering the information disorder.

That said, improving trust on social networks requires multi-stakeholder partnership and close consultation between industries, governments, civil society, and international organizations to ensure that social network is developed and used in a secure and balanced fashion.

3.1 Multi-Dimensional Approach

The current practices for social network governance can be drawn, based on a multi-dimensional approach to governance. Within this approach, the nature of responses and countermeasures in various areas, which are deemed effective and delivered by relevant stakeholders, to tackle information disorder are taken into account, such as:

[3] http://europa.eu/rapid/press-release_STATEMENT-19-2174_en.htm

3.1.1 Transparency: Social network platforms disclose or are more transparent about the following information:

1) Sponsored contents and their sources of fund; sponsors of online media, legacy media, and online influencers, particularly the sponsors of those contents relating to political campaign
2) Process of fact probe, performed by fact-checker, and regulatory bodies, to inform the public in case of account suspension or content censorship.
3) Algorithmic content feeding on the platform to help the users to be aware of the 'echo chamber' issue, which is responsible for the lack of content diversity.

3.1.2 Media and information literacy: the reassessment and adjustment of educational policies and the media and information literacy programs for citizens of all ages should be considered.

3.1.3 Empowerment of users and journalists: Development of online tools for user empowerment for fact-checking or exercise their rights to reply and report, as well as to correct false information or harmful information. In addition, consider ways to empower journalists by sponsoring journalists for training programs to promote quality, independent content**.**

3.1.4 Diversity and sustainability of the news media ecosystem: Promoting diversity can be done through supporting independent quality news media, training journalists, and empowering fact-checkers in both regional and domestic level.

3.1.5 Process and evaluation: Attention should be given to building and enhancing the processes, in which frameworks and guidelines for action are established and implemented by relevant stakeholders, under self-regulation and co-regulation regimes. Evaluation of the implementation should be promoted with clear measurement.

3.2 Multi-Regulatory Approach

The current practices for social network governance can also be extracted from the nature of the interaction and synergy between relevant stakeholders in their efforts to regulate the use, quality, and content of the platforms. The current practices can be categorized as follows:

3.2.1 Self-regulation: There are two levels of self-regulation, company and industry levels, where the current practices are drawn. Under this regulatory regime, despite being independent of the intervention from public authorities, the platform companies and the whole industry are required to develop transparency and accountability towards content policy, through the following steps: 1) Formulation and implementation of Codes of Conduct and common guidelines for the content regulation; 2) publication of transparency reports; 3) development of mechanisms for evaluating the implementation of the codes of conduct and guidelines; 4) building accessible, real-time communication channels for receiving reports and complaints on the content policy violation.

3.2.2 Centralized regulation: This government-led regulation, to a large extent, relies on the uses of legislation and public authorities' enforcement mechanisms in stemming the information disorder. It is interesting to observe the development of effective legal instruments, e.g. 1) cybercrime laws, 2) cybersecurity laws, and 3) laws on privacy and personal data protection. In addition, the public authorities are expected to be more effective actors, when it comes to the issues of large-scale emergency or in times of crisis. As such, the authorities should consider establishing a rapid response unit to counter false, fabricated, or harmful contents, particularly when the contents threaten homeland security.

3.2.3 Co-regulation: The collaboration between public authorities, industries, civil societies, and academia to jointly formulate common rules and agreements, including codes of conduct, with binding effect to all stakeholders. The public authorities are expected to play a multi-faceted role in leading, enforcing, facilitating, and mediating the issues and agenda under this regulatory framework. The independent mechanisms, such as a center of excellence, can be established and funded by relevant stakeholders, to perform the evaluation of the implementation of the rules, guidelines, and codes of conduct by stakeholders.

4. Challenges on Social Network Governance in APEC

4.1 Security Paradox of Self-regulation

Given the successful implementation of the industrial code of conduct, the social network industry has taken an important role and responsibility in monitoring disinformation and misinformation, as well as terrorist propaganda, under the self-regulation scheme. In effect, this has reduced the availability of such mal-information on social network platforms to the extent that the governments may neither be able to early on identify nor correctly understand the scope and extent of such emerging threats as extremism (Social Media in Operation: a Counter-Terrorism Perspective, 2017).

4.2 Inter-platform flow of information

With the emergence of new social network platforms, which offer different functional features and content policies, there are more options available for users, whose choice of usage is based on personal and practical preferences. The users can choose to simultaneously use multiple platforms, both public and private. As a result, information from one platform can easily flow to other platforms, thus making it difficult to regulate problematic contents, such as false information and mal- information, without cooperation between platforms, both local and global. In addition, users can always migrate from strictly regulated platforms to other platforms where content is encrypted or not monitored as strictly. For example, ISIS supporters have also moved their community-building activities to other platforms, particularly Telegram.

4.3 Gaps in Social Network Governance

Self-regulation efforts at social network governance have successfully been made by the tech industry under the leadership of global platform companies. That said, in many cases, the implementation of the Code of Practice on Disinformation, for example, is on voluntary basis and varied from companies to companies, depending on capacity and will to act. In addition, the implementation is varied from economies to economies, depending on regulations by local public authorities. Gaps still exists between companies as well as between authorities in different economies and regions. It takes time for lessons from one economy to be learned by other economies, as it takes strong political will to take necessary regulatory actions-both self-regulation,

centralized regulation, and co-regulation. At the regional and international levels, consensus is required, but hard to achieve, as long as this trans-border issue of cyberspace is considered an issue of ‘homeland’ security.

III. Recommendations on Social Network Governance in APEC

On Regional and Global Status and Trends of Social Networks, there are emerging challenges of false information on social networks, as well as increasing vulnerabilities from rapid business expansion of the platforms, and the gaps in social network regulation. Recommendations are put forward to address the challenges, including:

1) APEC should promote free and fair competition, responsibility, and accountability, as well as the diversity among platforms.
2) APEC should encourage measures to strengthen the protection of personal information and privacy of users.
3) APEC should promote social network literacy among users, in conjunction with the efforts to monitor and curb harmful contents of false and harmful information with appropriate regard to principles such as free speech and privacy.

On Case Studies and International Current practices on Social Network Governance in APEC, drawning from various case studies and the discussions in the Workshops held in Taipei and Bangkok, participants are undertaking some of the following practices:

1) APEC should empower users and professional journalists by promoting their roles in fact checking and correction of falsehoods and harmful information.
2) APEC should maintain diversity and sustainability of quality independent news media, through funding, supporting, and training of journalists and fact-checkers.
3) APEC should promote close consultation between all relevant stakeholders, where sharing current practices and lessons learned are encouraged.

4) APEC should promote capacity building to develop experiences and expertise on relevant issues such as fact-checking, professional journalism on social networks to sustain quality of journalist in the region.

IV. Report Summary: Public-Private Dialogue on Status, Trends, Opportunities and Threats of Social Networks

1. Background and Rationale

This paper is part of the proposal of the self-funded project, entitled Public-Private Dialogue on Status, Trends, Opportunities, and Threats of Social Networks, Thailand put forward in APEC TEL 56, held in December 2017 in Bangkok. In partnership with the Faculty of Communication Arts, Chulalongkorn University in Thailand, the project aims to promote the sharing of information and experiences between the public and private sectors, including NGOs and the academia, with a view to examining and updating the status, trends opportunities, and threats, as well as bringing forward current practices and recommendations on social network governance for future APEC collaborations.

To provide a foundation for this paper, two workshops were organized: 1) Workshop on Public-Private Dialogue on Status, Trends, Opportunities, and Threats of Social Networks, held in Taipei in October 2018 and 2) Multi-Stakeholder Regional Workshop on Social Network and Digital Platform Governance in February 2019 in Bangkok. The information, views and experiences shared in the Workshops are incorporated into this paper. In addition, further studies are conducted by CU' s Faculty of Communication Arts to examine the subject of social network governance. As such, case studies of emerging governance structures and current practices in different regions, and recommendations to cope with the challenges of cybersecurity and information disorder are included and form major parts of the paper.

2. Project Overview

This project aims to provide the current status, trends, opportunities and threats of social networks and provides recommendations to best deal with this digital technology from public and private sectors. All member economies can use the recommendations to establish their own social network governance. There are outputs as reports and activities which are.

1. Report of Regional and Global Status and Trends of Social Networks
2. Report of Case Studies and International Current practices on Social Network Governance in APEC
3. Report of Cybersecurity, Cybercrime and Cyber Norms on Global Social Networks in APEC.
4. 1-day Regional Workshop on status, trends, opportunities and Threats of Social Networks, the project is expected to open discussion and brainstorm by sharing information, experience, related policies, and regulations and or current practice on trends and impacts of social network, specifically in APEC. Then the participants can get the benefits from exchanging views and discussions
5. 1-day Regional Workshop on International Current practice and Case studies on social media and Digital Platform Governance. This workshop aims to global and regional current practice to recommendations to best deal with this digital technology from public and private sectors. All member economies can use the recommendations to establish their own social network governance include Cybersecurity, Cybercrime and Cyber Norms.

3. The Workshop

The project of Public-Private Dialogue on Status, Trends, Opportunities and Threats of Social Networks arranged 2 Regional Workshops which are;

3.1 Regional Workshop on status, trends, opportunities, and Threats of Social Networks in APEC TEL 58

The Project of Public-Private Dialogue on Status, Opportunities and Threats of Social Networks hosted by Thailand is a Self-Funded project under SPSG Steering Group. In APEC TEL58 Thailand's HOD form Ministry of Digital Economy responsible for the workshop, aim to achieve APEC TEL Strategic Action Plan 2016-2020. The key objective of the action plan is to Promote a Secure, Resilient and Trusted ICT Environment. This workshop hosted 45 delegates from APEC members on October 1st, 2017, in Taipei.

1) The Workshop's Programme

Workshop on Public-Private Dialogue on Status, Trends, Opportunities and Threats of Social Networks

Room 2F 201BC @ APEC TEL 58 Meeting

1st October 2018, 2.00 – 5.30 pm.

Time	Activity
Introduction	
14:00	Opening Remarks by SPSG Convenor

14:10	Introduction by Thailand HOD
Session 1: Social Network: Opportunities and Challenges The Adoption and Regulation of Digital and Social Media Platforms: In Pursuit of Social Innovation, Economic Growth and Sovereignty. This session will generate public – private dialogue concerning the trends, opportunities and challenges of social network and digital platforms pertaining to social innovation, economic growth and the Sovereignty of APEC Member Economies. It aims to share experiences and establish a common ground between public and private sectors in regard to the tensions between different goals and how they can be resolved.	
14:30	James Chio, LINE
14:45	Michale Bak, Facebook
15:00	Pellaeon Lin, Open Culture Foundation
15:15	Noelle de Guzman, ISOC
15:30	Coffee Break
Session 2: Cybersecurity in Social Network: Lesson learn The challenge of social freedom, unity, and the security of APEC Member Economies. This session will discuss case studies from APEC Member Economies on current practices of balancing free speech, social unity and security through social media and the digital economy laws and regulations. It aims to promote an understanding of the social and regulatory norms as they relate to social freedoms, social and political cohesion and the security of member economies.	
15.45	Adli Wahid, APNIC
16:05	Thongchai Sangsiri, ETDA, Ministry of Digital Economy and Society of Thailand
16:20	Nathaniel K Jones, Homeland security, USA.
16:35	Associate Prof. Ching-Heng Pan, National Chung Hsing University , Chinese Taipei
16:50	Q & A

Closing Session	
17:20	Closing Remarks by Thailand HOD
17:30	End

2) The Workshop's summary

In the workshop of Public-Private Dialogue on Status, Opportunities and Treats of Social Network hosted by Thailand, the participants found several opportunities and challenges of social network in APEC.

Opportunities of Social Network	Challenges of Social Network
1. Social media had become an important medium of socialisation, commerce and also governance.	1. Risk on privacy of social media user's personal data.
2. Social media platforms are a vital means powerful means for Women and disadvantaged communities.	2. Challenge of machine learning and AI in social media.
3. APEC can take a leading role in addressing the issues of global social network governance.	3. Risk on social media content related to issues of 1) Disinformation 2) Misinformation and 3) Malinformation
4. Idea of 'Mega Platform' would decentralize concentration of social media by introducing inter-platform portability of data, education of users, and net neutrality.	4. Challenge of social media's inclusive and universal access of social media in APEC.
5. Opportunity of overcoming threats by strengthening the economy's cyber security ecosystem, building up the cyber security workforce, securing critical infrastructure from cyber threats.	5. Challenge of battle with cybercrime which increasing the reach and volume of potential security threats.
	6. Challenge of social media concentration of ownership.

3.2 The Multi-stakeholder Regional Workshop on social media and Digital Platform Governance

This workshop aims to promote open, constructive consultation and dialogues concerning current practices of social media governance among APEC economies. The workshop brings together a cross-section of stakeholders, including government officials involved in policy formation, academic researchers, social media platform policy executives and NGO leaders to discuss how to secure social media to enable prosperous digital communities by addressing, misinformation and disinformation, i.e. information disorder across social media platforms. The self-regulation policies of each platform will be introduced and discussed to create a foundation for planning further collaboration among key industry, government, and civil society stakeholders. The result of this workshop will be submitted to APEC TEL as a key study to promote healthy and secure social media platforms that support emerging digital societies in APEC member economies. Thailand has hosted 70 delegates on Monday Febuary, 18th 2018.

1) The Workshop's programme

8.30 - 9.00	Registers
9.00 - 9.15	Opening Remarks
9.15 - 10.30	Keynote Address Information Disorder: Policy Challenges and Opportunities by Carol Soon, Lee Kuan Yew School of Public Policy
10.30 - 10.45	Break
10.45 - 12.00	Current practices for Digital Platform Self-Regulation: Views from the Private Sector Speakers • Sheen Handoo, public policy manager, APAC, Facebook • Jake Lucchi, Head of Content and AI, Public Policy, Google Asia Pacific • Taimu Negishi, Public Policy Strategist, LINE Corporation
12.00 - 13.00	Lunch break
13.00 - 14.00	Self-regulation Lab Showcase
14.00 - 14.15	Break
14.15 - 15.30	Dialogue between multi-stakeholders: Possible Best Practices on Governance beyond Self-Regulations: Domestic and Regional Perspectives
15.30-16.00	Closing remark

2) The Workshop's summary

Practices of Social and Digital Platform's Self-regulation

1. Facebook

Facebook shares its content policy or so-called community standards, and how to implement the policy on its platform. The policy or community standards are established with a view to prohibiting certain kinds of behaviors, such as self-harm,

child exploitation, sexual abuses, graphic violence and hate speech, to ensure its users safety, diversity, and freedom of expression. The community standards are reviewed constantly in consultation with outside experts, considering cultural diversity and contexts. With the use of AI, the internal reviewers work 24 hours to monitor the violating contents in languages with and without reports from users. Fake accounts, spams, violent content, terrorist propaganda, bullying and harassment are taken down in a significant number.

2. Youtube

Youtube shares its core values of its platform, such as freedom of expression and freedom to belong, upon which its platform and content policy are developed. Misinformation and disinformation are the issues Youtube is trying to regulate through its content policy implementation and the use of AI. It also changes the search algorithm to demote low quality content, while promoting authoritative content. It provides authoritative references and promote professional high-quality journalism on the platform. Community guidelines are in place to prohibit contents of violence, and nudity. AI is used to flag the problematic contents to its human resources for their reviews, taking into account contexts. Partnership with other platforms, NGOs, governments, international organizations are highlighted on the area of counter-terrorism.

3. LINE

LINE shares its security and privacy policy. According to Japan's Secrecy of Communication Law, Chat, LINE's messaging feature is so strictly encripted that its staff cannot read the messages. To prevent misinformation and disinformation on its news feed, cooperation with 300 outside content partners is strengthened to ensure the accuracy and quality of the news. Media and information literacy programs are promoted to ensure the awareness of misinformation and disinformation among youths and internet users in economies.

References

AHSGIE. (2017). *APEC Internet and Digital Economy Roadmap.* Viet Nam: APEC Secretaria.

Anti Fake News Bill. (2018). Retrieved from https://www.cljlaw.com/files/bills/pdf/2018/MY_FS_BIL_2018_06.pdf

APEC Secretariat. (2005). *APEC Privacy Framework.* Singapore: TI Sub-Fora & Industry Dialogues Groups, Electronic Commerce Steering Group(ECSG).

APEC Secretariat, A. P. (2017). *APEC in Charts 2017.* Singapore: APEC Secretariat, APEC Policy Support Unit. Retrieved November 2017

APG/MENAFATF. (2019). *SOCIAL MEDIA AND TERRORISM FINANCING.* New South Wales: APG Secretariat.

Asia-Pacific Economic Cooperation Policy Support Unit. (2019). *APEC REGIONAL TRENDS ANALYSIS.* Singapore: APEC Policy Support Unit.

Australian Government. (2018, December 16). Retrieved from Online safety Charter: https://www.communications.gov.au/documents/fact-sheet-online-safety-charter

Bickert, M. (2017, November 28). *Facebook News Room*. Retrieved from https://newsroom.fb.com: https://newsroom.fb.com/news/2017/11/hard-questions-are-we-winning-the-war-on-terrorism-online/

Business Insider. (2019, April 3). *Anti fake news laws around the world*. Retrieved from Business Insider: https://www.businessinsider.in/indiainsider/anti-fake-news-laws-in-singapore-russia-germany-malaysia-france/slidelist/68704974.cms

Cabanes, J. C. (2018). *he architecture of networked disinformation.* Leeds: University of Leeds. Retrieved from https://newtontechfordev.com/wp-content/uploads/2018/02/ARCHITECTS-OF-NETWORKED-DISINFORMATION-FULL-REPORT.pdf

Canegallo, K. (2019). *Fighting disinformation across our products*. Retrieved from https://www.blog.google/around-the-globe/google-europe/fighting-disinformation-across-our-products/

Derakhshan, C. W. (2017). *INFORMATION DISORDER:Toward an interdisciplinary framework.* Strasbourg: Council of Europe. Retrieved from https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Doan, E. Z. (2019, March 20). *Active social media user penetration in selected Asia-Pacific countries as of January 2019.* Retrieved from Statista: https://www.statista.com/statistics/255235/active-social-media-penetration-in-asian-countries/

esafety commissioner. (n.d.). Retrieved from eSafety Commissioner: https://www.esafety.gov.au/

European union. (2017). *CODE OF CONDUCT ON COUNTERING ILLEGAL HATE SPEECH ONLINE.* Brussel: European Union.

European union. (2017). *CODE OF CONDUCT ON COUNTERING ILLEGAL HATE SPEECH ONLINE.* Brussel: European Union. Retrieved from file:///C:/Users/JRCom_Pijitra/Downloads/CoCEN.pdf

Gemalto. (2018). Retrieved from Thales: https://safenet.gemalto.com/resources/data-protection/breach-level-index-2018-h1/

Globalwebindex. (2018). *GlobalWebIndex's flagship report.* London: Global Web Index. Retrieved from Global Web Index: https://www.globalwebindex.com/hubfs/Downloads/Social-H2-2018-report.pdf

Government, Singapore. (2019, April 1). *Protection Online Falsehood and Munipulation Bill.* Retrieved from https://www.parliament.gov.sg/docs/default-source/default-document-library/protection-from-online-falsehoods-and-manipulation-bill10-2019.pdf

Harvey, Y. R. (2019). *How Twitter is fighting spam and malicious automation.* Los Angeles: Twitter. Retrieved from https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html

IBM Security. (2018). *2018 Cost of a Data Breach Report.* New York: IBM Security. Retrieved from https://www.ibm.com/security/data-breach

ITU. (2018). *Guide to developing a nation cybersecurity strategy.* Geneva: ITU. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

ITU. (2018, July). *World Telecommunication/ ICT Indicators Database*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx

Macdonald, S. (2018). How Tech companies are successfully disrupting terrorist social media activity. *The Conversation*.

Mardisalu, R. (2019, April 3). *14 Most Alarming Cyber Security Statistics in 2019*. Retrieved from The best vpn: https://thebestvpn.com/cyber-security-statistics-2019/

Milkovich, D. (2018, December 3). *13 Alarming Cyber Security Facts and Stats*. Retrieved from Cybint solution: https://www.cybintsolutions.com/cyber-security-facts-stats/

Miller, D. (2016). *How the World Changed Social Media.* London: UCL Press. Retrieved from https://ucldigitalpress.co.uk/Book/Article/10/35/362/

Mini watts marketing group. (2019, June 30). *Internet World Stats.* Retrieved from https://www.internetworldstats.com/stats.htm#links: https://www.internetworldstats.com/stats.htm

Morrow, S. (2019). *The Future of Cybercrime & Security.* Hampshire: Juniper. Retrieved from https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

NEWMAN, L. H. (2018, September 7). *The Worst Cybersecurity Breaches of 2018 So Far*. Retrieved from Wired: https://www.wired.com/story/2018-worst-hacks-so-far/

NEWMAN, L. H. (2018, September 7). *Wired*. Retrieved from https://www.wired.com/story/2018-worst-hacks-so-far/

Norton Rose Fulbright. (2019). *Norton Rose Fulbright*. Retrieved from https://www.nortonrosefulbright.com/en/services/172fd60c/data-protection-privacy-and-cybersecurity

Poynter. (2015). *International Fact Checking Network.* Retrieved from Poynter: https://www.poynter.org/ifcn/

redirect method. (2018). Retrieved from redirect method: https://redirectmethod.org/

Reuter. (2018, April 2). *Malaysia outlaws 'fake news'; sets jail of up to six years*. Retrieved from Reuter: Malaysia outlaws 'fake news'; sets jail of up to six years

Reuters Institute. (2018). *Digital News Report 2018.* London: Reuters Institute Studies of Journalism. Retrieved from http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf

ROBINSON, M. (2019, Fabuary 4). *UK Column*. Retrieved from MIKE ROBINSON

Singapore Government Agency Website. (2018, Febuary 5). *CSR Singapore*. Retrieved from https://www.csa.gov.sg/legislation/cybersecurity-act#sthash.5ujm5q0r.dpuf

Sobers, R. (2019, April 17). *60 Must-Know Cybersecurity Statistics for 2019*. Retrieved from https://www.varonis.com/blog/cybersecurity-statistics/: https://www.varonis.com

(2017). *Social Media in Operation: a Counter-Terrorism Perspective.* Turkey: Nato Stratcom. Retrieved from https://www.stratcomcoe.org/social-media-operations-counter-terrorism-perspective

Soon, C. (2018, Febuary 2). Information Disorder: Policy Challenges and Opportunities. (P. Tsukamoto, Interviewer)

Stats APEC. (2018). *Statistic APEC*. Retrieved from http://statistics.apec.org/index.php/key_indicator/economy_list

Symantec. (2019). *Internet Cybersecurity Threat Report.* Symantec.

Tech Accord. (2018). *Cybersecurity Tech Accord*. Retrieved from https://cybertechaccord.org/accord/

Twitter. (2019). Retrieved from Twitter help center: https://help.twitter.com/en/rules-and-policies/violent-groups

We are social. (2018). *2018 Global Digital Report.* New York: We are social. Retrieved from https://wearesocial.com/blog/2018/01/global-digital-report-2018#

Winter, C. (2015, August 1). *Fishing and ultraviolence*. Retrieved from BBC: https://www.bbc.co.uk/news/resources/idt-88492697-b674-4c69-8426-3edd17b7daed

Young, Z. (2018, April 4). *French Parliament Pass Law Against Fake News*. Retrieved from Politico: https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/

Youtube. (2018). *Policy and Safety*. Retrieved from Youtube: https://www.youtube.com/yt/about/policies/?#community-guidelines

Youtube. (2019). Retrieved from Transparacy report: https://transparencyreport.google.com/youtube-policy/featured-policies/violent-extremism?hl=en

Youtube Help Center. (2019). Retrieved from Community Guidelines strike basics: https://support.google.com/youtube/answer/2802032?hl=en

Appendix 1: Summary of the Workshop on Public-Private Dialogue on Status, Trends, Opportunities and Threats of Social Networks.

Location**:** Room 2F 201BC @ APEC TEL 58 Meeting
Time**:** 1st October 2018, 2**.**00 **–** 5**.**30 pm**.**
No**.** of Delegates**:** 45

Opening Remarks by SPSG Convenor

Opportunities:

- Social media is an important medium of socialisation, commerce and governance, and brings great convenience.

Challenges:

- There are growing financial and privacy-related risks that must be addressed

Mr Kajit Sukhum, the Assistant Permanent Secretary, Ministry of the Digital Economy and Society, Head of Thailand Delegation

Opportunities:

- APEC, based on its leadership of the supply and demand side of the social media economy, and its strength in public-private dialogue, it can take a leading role in addressing the issues of global social network governance.

Challenges:

- There is a need to pay attention to capacity building in social media security and governance.
- There are large gaps between those developed and developing member economies, which need to be bridged in order to collectively cope with the threats and opportunities of social network platforms.

Session 1: Social Network: Opportunities and Challenges

I. James Chio, LINE, Corporate Affairs, Chinese Taipei.

Opportunities:

- Platforms like LINE are bringing people and information together in a single portal
- Social media platforms are the basis for expanding fintech services, which are growing rapidly.
- Social media platforms generate enormous amounts of data that be useful to law enforcement agencies.

Challenges:

- Excessive interest from govt. agencies in accessing and using social media user data is a threat to user privacy and potentially can undermine public trust in the platforms.
- There is a need to pay attention to the boundaries between government, the private sector, and privacy issues.

II. Michale Bak, Facebook Head of Public Policy in Thailand

Opportunities:

- Through connecting people, it is possible to create better lives for people and empower people to build communities.
- Evidence from Thailand indicates that social media platforms are a vital means and powerful means for small businesses to grow their business.
- Women and disadvantaged communities are using Facebook at a high rate to grow their businesses.
- Data on social media usage can be leveraged to improve the distribution of aid and other services.

Challenges:

- When you create things with a good purpose, there will always be people who use it for a negative purpose.
- The spread of misinformation, disinformation and malinformation through social is a major threat that must be addressed through partnerships, consultation, and feedback.
- Creating greater transparency is an important challenge that can decrease misinformation and increase trust in the platforms.

- AI can help identify fraudulent content, but humans are also needed to assess content, especially in diverse cultural contexts.

III. Pellaeon Lin, Open Culture Foundation

Opportunities:

- Social media can be a medium for creating more open access to data and transparent government.
- Decentralized social media could lead to a more democratic social media ecosystem.

Inter-platform portability of data, education of users, and net neutrality could support the development of alternatives to the current mega platforms.

Challenges:

- The private sector is engaging in data collection without consent and using it with machine learning.
- Platform companies have a tendency to comply with local governments and therefore can be used as mediums of mass surveillance.
- Algorithms used in the curation of content are not transparent and they have the potential to be exploited by automated systems.
- Efforts to mitigate misinformation can undermine freedom of speech. It is important to find a balance.
- It is possible that minority groups will be impacted disproportionately if free speech on social media is suppressed.
- Ad and content targeting on social media can lead to discrimination,
- Network effects make it difficult for alternatives social media platforms to emerge.
- Over-regulation could restrict the emergence of new platforms since only established platforms would have the resources to manage the regulations.

IV. Noelle de Guzman, Internet Society

Opportunities:

- Social media is often the first experience people have with the internet and can be seen as driving people to experience the internet.

- Social media is a medium for the grassroots to organise and apply pressure on governments and big business to pay attention to their rights.
- Social media is a powerful medium for marginalized businesses to grow their business.
- Social media reduces barriers to online services and can potentially contribute to greater financial inclusion.
- In Asia, which is disaster-prone, social media can support how people respond to emergencies and disasters.

Challenges:

- There are large disparities of social media used across Asia from Korea to Papua New Guinea, especially in terms of access.
- Application islands are emerging, whereby people use only a few applications and never leave them to explore other options and information sources.
- Zero-rated access schemes enable the poor to access the internet and social media but also limit their experience of their internet to designated social media platforms.

Session 2: Cybersecurity in Social Network: Lesson learned

V. Adli Wahid, APNIC

Opportunities:

- To address cybersecurity and defend against criminal attacks he said there should be network controls, greater user awareness, and greater information sharing among stakeholders.

Challenges:

- Social media platform are similar in their structure and malware works in similar ways across different platforms.
- Criminals are developing tools for other criminals. Before attackers set-up tools and infrastructure from scratch, but now they can buy tools and

infrastructure, which is increasing the reach and volume of potential security threats.

- Attackers are using fake profiles and engaging in trust building with targets on social media before they send malicious files to them or engaging in other criminal activities such as extortion.

VI. Thongchai Sangsiri, ETDA, Ministry of Digital Economy and Society of Thailand

Opportunities:

- By creating security and trust among users, they will be more willing to engage with government digital services.
- There are large opportunities in e-commerce, but trust is crucial if they are to be realized.

Challenge:

- To improve capacity and build trust, there needs to be collaboration among all stakeholders.

VII. Nathaniel K Jones, Homeland security, USA.

Opportunities:

- Social media companies have a vested interest in securing social media. Facebook, for instance, is being transparent and active in self-regulation.

Challenges:

- Overcoming threats by strengthening the economy's cybersecurity ecosystem, building up the cybersecurity workforce, securing critical infrastructure from cyber threats.

VIII. Associate Prof. Ching-Heng Pan, National Chung Hsing University, Chinese Taipei

Opportunities:

- Governments can be active users of social media rather than regulators of it.
- Users perceive more opportunity than risks in using social media indicating their openness.
- Governments can use social data science to engage in evidence-based decision making.
- Governments can engage in policy marketing using precise/ targeted marketing, and customized marketing.

Challenges:

- In economies like Chinese Taipei, there is a duopoly between Facebook and LINE.
- Governments are risk adverse in their use of social media and only use it to engage in one-way communication like traditional media.
- There is a need for greater analysis of G2C interactions.

Q and A

Opportunity:

- Economies such as China have already established relevant regulations on social media's commercial transactions.
- Economies can implement appropriate regulatory measures to promote online transactions, and taxation, to enhance economic opportunities.
- Platforms such as Facebook are demonstrating an effort to increase capacities to tackle content related issued through human resource strengthening and improving their AI tools.
- Coordinated multi- economy efforts to respond to social media attacks can address threats to social media and users in respective economies.

Challenge:

- Social media-based cross-border commercial transactions and platform operations potentially deprive the governments of tax revenue.

Given the multi-economy character of social media platforms, it is difficult to impose content controls on them.

Appendix 2: Summary of the Workshop on The Multi-stakeholder Regional Workshopon Social Media and Digital Platform Governance

18 February 2019, Bangkok

Practices of Social and Digital Platform's Self-regulation

- Facebook shares its content policy or so-called community standards, and how to implement the policy on its platform. The policy or community standards are established with a view to prohibiting certain kinds of behaviors, such as self-harm, child exploitation, sexual abuses, graphic violence and hate speech, to ensure its users safety, diversity, and freedom of expression. The community standards are reviewed constantly in consultation with outside experts, taking into account cultural diversity and contexts. With the use of AI, the internal reviewers work 24 hours to monitor the violating contents in languages with and without reports from users. Fake accounts, spams, violent content, terrorist propaganda, bullying and harassment are taken down in a significant number.
- Youtube shares its core values of its platform, such as freedom of expression and freedom to belong, upon which its platform and content policy are developed. Misinformation and disinformation are the issues Youtube is trying to regulate through its content policy implementation and the use of AI. It also changes the search algorithm to demote low quality content, while promoting authoritative content. It provides authoritative references and promote professional high-quality journalism on the platform. Community guidelines are in place to prohibit contents of violence, and nudity. AI is used to flag the problematic contents to its human resources for their reviews, taking into account contexts. Partnership with other platforms, NGOs, governments, international organizations are highlighted on the area of counter-terrorism.
- LINE shares its security and privacy policy. According to Japan's Secrecy of Communication Law, Chat, LINE's messaging feature is so strictly encripted that its staff cannot read the messages. To prevent misinformation and disinformation on its news feed, cooperation with 300 outside content partners is strengthened to ensure the accuracy and quality of the news. Media and information literacy programs are promoted to ensure the awareness of

misinformation and disinformation among youths and internet users in economies

Panel Discussion on Possible Current practices on Governance beyond Self-Regulations

Governance structure:

- Co-Regulation is a promising alternative to the current governance of self-regulation by the platforms and top-down regulation by governments. The objectives is to strengthen transparency, accountability and consistency of the platforms.
- At the initial stage, trust and confidence building, as well as close consultation are required among platforms. Then the process should expand to include public sectors and academia, NGOs, and so on. In this regard, the efforts to organize multi-stakeholder regional workshop should continue.
- The areas of co-regulation can encompass content policy, privacy protection, fact-checking and media and information literacy. Some examples of co-regulation initiatives are highlighted, including the global internet counter-terrorism program, the platforms' collaboration with the external oversight content boards with binding, transparent decisions on content policy reviews.
- An NGO and academics encourage the establishment of a multi-stakeholder body, such as UN-supported efforts in establishing a Social Media Council, to provide channels for appeals and counter review, especially focusing on the areas of human rights. In addition, standards for social media and digital platform governance should be established.
- What needs to be done regarding handling misinformation: 1. Understand challenges by sharing challenges with government, 2. Understand process to make it a healthy one, 3. Make incentives aligned among stakeholders, keeping in mind the ultimate goal of having a safe online environment and making technology available to people.

Government's regulation:

- Platforms stress the importance for governments to have a full understanding of the scale and true natures of challenges the platforms are now facing, as

well as the implications of the regulation efforts for the platform businesses and users. Therefore, it is necessary for the platforms and the governments to have close consultations and shared objectives, with some degree of flexibility for the platforms to work on those objectives.

- Australian government just legislated Online Safety Charter, which sets expectation on social media and digital platforms regarding content moderation, child safety protection and transparency. There is also an ongoing assessment of impacts to Media and Advertising market on such issues as market power, regulatory oversight and copyright. Other measures include removal of non-consensual contents from social media and protection of individual privacy.
- Cybersecurity officials asked how government should work with global digital platforms on cybersecurity threats. Platform providers responded that a number of measures already in place such as
  - Need of real name identification for user registration
  - Efforts to remove fake ids, misinformation and harmful contents
  - Fact checking support such as mechanism to flag false contents
  - Problems categorization and implement corresponding countermeasures

<u>NGOs' efforts and proposals</u>

- ISOC: Highlighted the goal of getting people not yet connected to connect and the importance of freedom of expression, privacy and security issues. ISOC engages in the areas of public policy, public education and technical solutions.
- Netizen: Questioned about the transparency of the flow of information inside a local economy, as opposed to cross-bordered flow which has been already reported. He also proposed that a forum is needed to support smaller local companies who need to comply with transparency reporting practices.
- The questions are raised including discrimination by political identities and how to hold government officials accountable for perpetrating misinformation.
- Ways to support fact checking are discussed. Efforts by platforms to provide investment fund to fact checking startups and incentives to make fact checking sustainable businesses are highlighted. (A startup in Belgium doing crowdsourcing for fact finding services)

Academics' proposals

The necessity of digital literacy especially for senior citizens or matured adults is discussed. Digital literacy and critical thinking skill is needed.