Fake news and information in Social Media: Problems and challenges, the case in Indonesia

ASHWIN SASONGKO SASTROSUBROTO1 & SURYA PRATAMA2

1Senior Researcher at the Indonesian Institute of Sciences (LIPI)
   Email: ashw001@lipi.go.id
2Media Relation Manager at the Agency for the Assessment and Application of Technology (BPPT)
   Email: surya.pratama@bppt.go.id

ABSTRACT
The use of social media in Indonesia currently shows tremendous growth together with increasing Internet penetration. However, along with this growth, fake news in Indonesian social media is also currently showing rapid growth. Social media is being increasingly used to form and signify public opinion. This information trend has been highly used by some public organizations.

Several approaches have been taken to avoid the problem of fake news: socialization through media and group discussions; technical approach mainly by identifying and then blocking the fake news by using crawling engine Cyberdrone 9; and legal approach based on the Electronic Information and Transaction Law which prohibits fake news.

Some problems however still exist:
• The huge quantity of news in social media makes it difficult to be tracked.
• It is difficult to identify and find those who make fake news if foreign IP addresses or foreign Top Level Domains are used.
• Although the content in a particular social media has been blocked, it might have been copied and distributed through Intermessaging Services such as WhatsApp, etc.

To overcome the above problems, it is important to promote self identification of fake news by the communities.

Keywords: Fake news, social media, cyber attack, net attack, socialization
Introduction

The growth of Internet penetration in Indonesia shows high growth every year. In 2017, Internet users reached 143.26 million users, increasing from 132.7 million users in 2016. Of this, 87.13 percent are social media users. With an estimated population of 262 millions, certainly the number of social media users is significant (APJII Survey, 2017).

In Indonesia, social media is more than just information for some users. Facebook and Twitter are often quoted in the mainstream media such as Radio, TV and newspaper. Hence, it can be regarded as social mobilization and social changes tool. Many people, organizations and even the government use social media to transmit information to the public. Hashtags are widely used to stress the message sent to the public. The government’s outcomes of development are also communicated through the social media (Wiwi Syafarhadiati, 2017).

Beside positive impacts, the above situation is also used to spread fake news in the social media. This has caused numerous problems such as possible increase of polarization index in Indonesia that has the potential to cause horizontal conflict. In a country like Indonesia, which consists of thousands of islands with numerous ethnicities, cultures, languages and many other differences among the population the increase in polarization index should be taken seriously.

This paper will discuss the above with references mainly to the studies carried out recently by the author and colleagues in the field of social media problems and the polarization that follows. In addition, the response to overcome the fake news problems are described including the problems faced. It has to be noted that media relation is very important to combat fake news. Finally, several suggestions on how to overcome the problems at international level will also be discussed.

Social Media – Basic theoretical framework

Social media today is a collaborative place for value creation and consumption. It has transformed the way a person influences others. It creates value for persons who look through it. The value creation only occurs when the person who would like to influence others or builds his or her network (e.g. invites friends,
suggest his or her friends to invite his/her other friends). He or she may also increase influence using the platform service tools such as ‘update status’ or ‘like’ or ‘dislike’ signs.

In addition to being a value creator, social media may also act as an amplifier. While conventional media may only reach millions of readers, social media may reach billions of them. Hence, the keynote theme is amplified once it is in the network.

Rumata, Karman and Sastrosubroto (2017) proposed the following model of Social Media shown in Figure 1. With the model, it can be seen clearly that Social Media may act as Value Creator and Amplifier.

![Fig. 1: Social media as a value creator and amplifier in polarization context.](image)

**Polarization in Indonesia**

Indonesia is a country that consists of thousands of islands, including five big main islands. In addition, there are many ethnic groups, languages, cultures, religions and many others that diversify the country. From this qualitative information alone, it can be understood that the Ethnic Polarization Index (EPOI) might be higher compared to a country with a homogeneous population.

A survey conducted in 2010 found that the Ethnic Fractionalization Index (EFI) of Indonesia is 0.81. Interestingly, the EPOI is quite low, only 0.5. This number is below the normal threshold of 0.6. It means that Indonesia is a highly heterogeneous society, yet not polarized, so that any potential conflict is
unlikely to occur (Wiwi Syafarhadiati, 2017). It is worth to be noted that in Jakarta, the capital of Indonesia, while the EFI is 0.76, the EPOI is much higher, 0.66. Since it is higher than the threshold which is 0.6, it is easier to initiate a conflict in Jakarta than other areas with lower EPOI.

Rumata et al. (2017) also argue that the recent Jakarta governor election may also increase the polarization index in Jakarta and in Indonesia since the news about major activities in Jakarta is normally followed by people in other regions of the country. It has to be noted that with this year 2019 presidential election, fake news is also soaring. Hence, it can be argued that the EPOI may also increase.

**Vulnerable computers and users**

It is commonly known that computers are vulnerable to attack that may cause them to stop working. Since the computer can be used for many purposes, the termination of their work can be certainly devastating. A large system such as an electricity power plant, controlled by the computer, might be stopped too.

The data stored in, and/or handled by the computers can also be destroyed, changed or copied and taken away. The computer system itself may still work, but it may not handle its task properly. If the data is not changed and only copied by the attacker, the computer system is normally not affected and even after the attack, the system might not show any problem.

Currently, however, the attack also targets the people who use computers. In this case, the computer is not attacked at all, but since the users use computers to access many type of content, this content is often used to attack the users’ mind. In this type of attack, fake news is normally used.

In addition to fake news, which can be responded directly with information of the real valid news, another type of attack is also used. In this type, the news is reframed such as shortening the full news to highlight a particular message and then pass that particular message to users. In many cases, the full valid news is also given and can be accessed by clicking a link in the reframed news. Thus the valid news is reframed while the full news is also given. However, since people may not have enough time to open
and read the complete news, they might rely only on the shortened news provided.

Rumata and Sastrosubroto (2018) describe the above in a short model as shown in Figure 2. In this model, the attack on the computer is categorized as Cyber attack while the attack on the people’s mind is called Net Attack.

![Fig. 2: Various types of computer attacks](image)

**Overcoming the Net Attack**

Basically, there are three methods to overcome the Net attack that can be carried out by the government in cooperation with the public, including political parties, Non Government Organizations, etc. In addition, this can be realized through international cooperation as well. The methods can be outlined as:

- Regulatory setup
- Massive socialization
- Content blocking
- International cooperation

Each of the above has problems in implementation and this will be discussed below.

**Regulatory setup:** Realizing that the content in the Internet may be fake news/information, in 2008, Act number 11/2008 on Electronic Information and Transaction (EIT) was released. Like the older law that prohibits fake news in conventional media like newspaper, magazines, etc. fake news is also prohibited in the Internet by this EIT law. This law prohibits among others, Fake news and Misleading informations; News with content that may cause SARA problems (SARA – ethnic groups, religions, races, and inter-groups) and even Hatred speeches.
The EIT law was amended by Law number 19 in 2016, explicitly giving the government the right to block prohibited content like fake news and others in the Internet. The law however still faces several legal problems. It argues whether reframed valid news can be considered as ‘misleading information’. In addition, in what way and to what extent this reframed valid news can be considered as hatred speech. So unclear is the status that it is recommended for the government to review and/or ask the Supreme Court for the interpretation of reframed news.

Despite all the problems faced, law enforcers have successfully identified many fake news makers and brought them to court. It has to be noted, however, that tracking down a fake news maker is not easy since they can use fake names and addresses when they register as social media users. They can even register with foreign social media and/or mailing list operated by foreign operators. In addition, they can also use foreign IP addresses as well as foreign Domain Names and Top Level Domain.

**Massive socialization:** Although regulations against fake news have been set up and the problem of fake news has been identified, the public still needs to be fully informed about this. Considering the diversity of the Indonesian population spread across so many islands, this certainly is not an easy task.

To carry out the socialization, the government in cooperation with many non government organizations and communities works together for intensive socialization against fake news. In addition, the Directorate General of Public Communication and Information of the Ministry of Communication and Information Technology is also tasked with overall socialization of fake news.

Despite intensive socialization, fake news is still uploaded and spread in the social media, hence the socialization against fake news still has to go on.

**Content blocking:** Since the release of the EIT Law, the government through the Ministry of CIT has blocked many prohibited content by blocking websites hosting such content. The prohibited content includes among others pornography, gambling and many others including websites that spread fake news.
The prohibited content is normally identified by the Ministry and also from the information provided by the public. In 2017, the Ministry installed a crawling engine called Cyberdrone 9 to help identify prohibited contents. Once it is identified, the ISPs (Internet Service Providers) in Indonesia are ordered to block the sites of the contents. If the content providers/makers are located in Indonesia, they will be notified to remove the content or they can even be brought to the court depending on the investigation.

The problems faced in blocking prohibited contents are already known widely. Firstly, the amount of prohibited content is huge. While some of them can be easily identified, many may not. So identification is already one of the main problems.

Secondly, while the website featuring the content has been blocked, the content itself might have been copied and spread through group-based social media such as WhatsApp, which is difficult to be tracked and centrally deleted.

Thirdly, one of the most difficult problems is if a major part of a foreign website is used and accessed by the public while only a small part of the website has prohibited content. In this case, the foreign operator will be requested to remove the content or at least block its access to all Indonesian IP addresses. The problem of course lies in the fact that a foreign website operator does not need to follow Indonesian laws.

This last problem is the reason why Indonesia proposes international cooperation so that if a particular country hosts an operator with prohibited content, then that country should help the other country to stop the content to be accessed from the country.

**International cooperation:** It has to be noted that this type of cooperation has never been discussed in-depth internationally. Indonesia has formally proposed international cooperation in many international meetings, among others, ITU Council meetings 2012 and also 2013, high level government meetings during IGF 8 in Bali 2013, Word Conference on International Telecommunications (WCIT 12) in Dubai and many others.

International cooperation can start with Cyber ethics. Multinational discussions can then be conducted with the
intention to set up agreements. International organizations such as UN ITU and others can facilitate these discussions.

Conclusions

Currently, fake news is a problem in Indonesia and many countries. Despite strong efforts to overcome the problems, fake news is still soaring. Both technical and non-technical problems in removing fake news are still faced. Sharing of information and knowledge to overcome the problems among concerned countries is necessary. Therefore, international discussion to reduce fake news should be conducted as soon as possible with a target to achieve international agreements.

References:

Indonesian Contributions in ITU Council meeting 2012 and 2013.
Indonesian proposal for WCIT 12, Dubai, 2012.