Social Media Censorship Policy and Law: Balancing Good Governance and National Security

Non Naprathansuk, Maejo University, Thailand

The Asian Conference on Business and Public Policy 2014
Official Conference Proceedings

Abstract
Social media has grown in number and influence, there has been an increase in political participation around the world. On the other hand, Thailand, Computer Crime Act of 2007 is a piece of legislation that has had a significant and negative impact on freedom of Expression on the Internet since it came into force in July 2007. Thus, Thai government is facing a serious challenge in good governance and national security.

On the other hand, cyber-crime, cyber-terrorism, and tradition terrorism are using a new way to damage and destroy infrastructure also trade and investment. Therefore, to help Thai government balancing good governance and national security at the same time, this analysis examines four policy alternatives: (1) the status quo policy, (2) cooperation with trusted Non-Government Organization (NGOs), (3) amendment computer crime act, and (4) government participates in social media.

All of four alternatives are assessed in terms of their ability to meet the following four goals: improve good governance (primarily on government transparency); improve democracy (maximize to civil and political participation); improve national security (emphasizes on peaceful strategy); and cost-effective (minimize cost on social media and internet censorship). On the basis of this assessment, the concludes that Thai government should participates in social media by using communication platforms such as Facebook, Tweeter, YouTube, and Line which are the best solution for improve good governance especially in transparency and maintain national security as well. Also, it will help Thai government more accountability and makes people participates in political which will improve democracy. Therefore, Thai government can balance their good governance and national security in the same time.

Keywords: Social Media Censorship, Policy, Good Governance, National Security

Introduction

Social media are more than just a buzzword or an interesting phenomenon to our teenagers. They are a way of life. Researches show that active participation on sites like Facebook, communicating via texting and chat programs, and creating blogs are everyday occurrences for new era of mankind communication. Moreover, social media has grown in number and influence, there has been an increase in political participation around the world for example, Arab spring, Occupied Wall Street, and Thai people factions' conflict. However, in Thailand, the government has authority and power to control information and communication by using censorship policy and law. It claims to protect national security issues, but it creates controversial issues especially on good governance and democracy.

On the other hand, Thailand, Computer Crime Act of 2007 is a piece of legislation that has had a significant and negative impact on freedom of Expression on the Internet since it came into force in July 2007. Thus, with this law and policy, Thai government is facing a serious challenge in good governance for manages and develops country. On the other hand, cyber-crime, cyber terrorism, and tradition terrorism are using a new way to damage and destroy infrastructure also trade and investment. The terrorism has been moved downward from middle-east to Southeast Asian especially in Indonesia, Malaysia, and Southern of Thailand. Moreover, Thailand social media and internet censorship is being implemented using two methods. One, the Thai police has placed an online roadblock to about 32,500 websites which permanently prevents such sites from being viewed by Net users in the country and two, the Communications Authority of Thailand has additionally filtered an undisclosed number of websites right at the country's Internet gateway. To censor a website, the Ministry of Information and Communication Technology sends a request to each of the 50 or so non-profit and commercial ISPs in the country.

Any Internet services provider that fail to blacklist a requested website will be reprimanded by the government via cancellation of licenses or restriction on bandwidth capacity. For fear of sanctions, local ISPs strictly abide by Thailand Internet censorship. Just three years ago, the country's communications ministry requested for approximately 2,500 websites to be blocked. A year after that, the number of blocked websites increased to more than 13,000 which represents over 500% rise in blacklisted sites. Today, the number of websites censored by the ministry through local ISPs is largely unknown.

The reason for blocking websites is for national security which disclosed to the public. Many Internet users feel that the rules regarding Thailand Internet censorship are mainly based on the government's security and stability. Thai government has also spent millions of dollars for an Internet gateway system that will block any harsh comments on the country's supreme ruler. The same system can also be used to blacklist sites owned by terrorists and those that deal in pornography. It must be emphasized, though, that all the steps taken by Thai government to censor inappropriate websites are all within the bounds of the local laws. As a matter of fact, blocking certain websites is aimed at safeguarding the privacy of millions of Internet users in the country. Moreover, social media has been restricted and censored ever more severely since Thailand faced unrest resulting from political conflict between many different groups. During this political crisis, the correct role of the Thai state is

to protect rights and liberties for people to access news and information and express opinions because it is a critical time when the public needs to receive information from a variety of sources in order to be able to assess the situation both in terms of the safety of themselves, their property, and society, and political matters.

Therefore, to help Thai government balancing good governance and national security at the same time, this analysis examines four policy alternatives: (1) the status quo policy, (2) cooperation with trusted Non-Government Organization (NGOs), (3) amendment computer crime act, and (4) government participates in social media. All of four alternatives are assessed in terms of their ability to meet the following four goals: improve good governance (primarily on government transparency); improve democracy (maximize to civil and political participation); improve national security (emphasizes on peaceful strategy); and cost-effective (minimize cost on social media and internet censorship). On the basis of this assessment, the concludes that Thai government should participates in social media by using communication platforms such as Facebook, Tweeter, YouTube, and Line which are the best solution for improve good governance especially in transparency and maintain national security as well.

Also, it will help Thai government more accountability and makes people participates in political which will improve democracy. The adoption of deregulation to trusted NGOs also has the potential to improve significantly the efficiency and accountability of government. While it would probably not be as efficient and appropriate as the preferred alternative, it is probably more insecure that cybercrime, cyber terrorism, and tradition terrorism can link or hack the NGOs websites and creates miss information or frauds reports. Moreover, Thai government participates in social media would ensure efficient trust information source and reduce cost in cyber security that people can share and receive a correct information. This alternative could also be designed and implemented so that national security improved as well as good governance.

Thai Government and Censorship Policy

There is a long history of Censorship in Thailand. Harassment, manipulation, and strict control of political news was common under the Thaksin government (2001–2006), restrictions and media harassment worsened after a military junta overthrew the Thaksin government in a 2006 coup and increased until present. Thailand ranked 59th out of 167 countries in 2004 and then fell to 107th out of 167 countries in 2005 in the worldwide Press Freedom Index from Reporters Without Borders. Thailand's ranking fell to 153rd out of 178 in 2010 and rose to 137th out of 179 in 2011-2012.

Therefore, consequence of Thailand's Computer Crime Act of 2007 has been criticized for being overbroad and for granting authorities too much discretion in prosecuting Thai citizens and online service providers. However, the Computer Crime Act (CCA) suffers from many defects such as vague, overbroad, and overly punitive provisions. Moreover, it could inhibits Thai service providers from offering Web 2.0 services and harm Thailand's global economic competitiveness and downgrade of good governance in the Information Age.

Social Media

Research shows that active participation on sites like Facebook, communicating via texting and chat programs, and creating blogs are everyday occurrences for new era of mankind communication. As well as in Thailand, political unrest and conflict between "Red Shirts" and "Yellow Shirts" have been recurrent events when the Red Shirt crisis that plunged Bangkok into violence in April and May 2010 was a catalyst for the rise of social media particularly Twitter, Facebook, and YouTube. Moreover, the numbers tell a story from both sides. Facebook's growth resulting from January 2009, there were 250,000 Facebook members in Thailand by April 6, 2010 until May 21 it was 3.1 million.

This was an important phenomenon which 500,000 people added in less than six weeks by September, it was more than 5 million people subscripted (Carthew, 2010). On the other hand, according to Congressional Research Service (CRS, 2008) the report to US congress said it is clear that terrorist groups are using computers and the Internet to further goals associated with spreading terrorism. This can be seen in the way that extremists are creating and using numerous Internet websites for recruitment and fund raising activities, and for Jihad training purposes. It is possible that as criminals and terrorist groups explore more ways to work together, a new type of threat may emerge where extremists gain access to the powerful network tools now used by cybercriminals to steal personal information, or to disrupt computer systems that support services through the Internet.

Therefore, to improve democracy and national security in Thailand, government must look at this potential and promotes social media which brings people to help government monitors rather than censor or block websites.

Good Governance

A Thai academician advocated that the term good governance was used to replace modernization of the public administration because the World Bank (WB), first used the term in 1989, wanted to address the problem of public administrative corruption in developing countries but was unwilling to use the word corruption as such because it is a negative word and might offend governments of countries which the WB works with In the WB report Sub-Sahara: From Crisis to Sustainable Growth, good governance is referred to good management of government mechanisms in administering social and economic resources for development. Later UNDP elaborated the meaning of good governance by addressing what is bad governance. Bad governance was defined to include failures by government to provide good and efficient public services.

In private sector, the issue of corporate governance has also become vital in respond to the financial crisis in 1997 towards economic recovery and a more sustainable development. The Asian Development Bank reported in 1999 that the crisis in Southeast Asian countries, including South Korea, was caused by a failure in implementing corporate governance. They were (1) a high concentration of company ownership, for instance, 57 %; (2) ineffective mechanisms of Board of Directors supervision; (3) inefficiency and in-transparency of the procedures for acquiring company control; (4) external funding domination of a company's source of funds,

i.e., bank loans; and (5) external funding was not accompanied by adequate creditor supervision. Hence, good corporate governance is therefore associated with well-functioning, competitive corporate finance market, solid legal protection for outside investors, both for creditors and shareholders, and outside shareholders being able to influence director and management behavior.

National Security

The process of Thailand's national security policy making and implementing has historically been dominated by a small elite. Thai core values began to take root in the mid-19th century when the King and aristocracy established the concept of nation, religion, and kingship in the national consciousness. Under the domination of the military and the bureaucracy, Thai conceptions of security were influenced by militaristic-authoritarian ideology. Since the 1990s there has been a significant change in national security policy making. The process of security policy making has moved from military leaders to a group of authorities, which consists of the head of state, military leaders and civilian leaders in related fields. The security making group, which was formed as a committee, is known as the National Security Council.

They attempted to systematically define and narrow the concept of security by focusing on five specific dimensions: political security, economic security, social and psychological security, military security and science and technological security. Nowadays Thailand's National Security Council, which is chaired by the Prime Minister, is responsible for the security policy making process by looking at external threats and internal issues. At the present time, in the absence of immediate external aggression, they are concerned about local and regional issues such as borders, maritime claims, drug trafficking and resources.

Also the new threat is cybercrime and terrorism, Thailand's cybercrime ranking in the Asia Pacific region has risen due to an increase in the online population, while the global underground economy continues growing without any impact from the global economy, according to a new Symantec Internet Security Threat Report, which highlights key trends in cybercrime in 2009. The attackers are leveraging the abundance of personal information openly available on social networking sites to synthesis socially-engineered attacks on key individuals within targeted companies. Furthermore, web-based attacks continued to grow unabated. Attackers leverage social engineering techniques to lure unsuspecting users to malicious websites.

Thai media analysts even labeled the alleged bombings and the blacklisted on money-laundry as parts of sinister plans to drag Thailand into counterterrorism networks. To be fair, quite a few, however, realized that with more potential terrorists using Thailand as a haven, it could cause a "risky situation" for the country. Therefore, the dilemma situation is facing to Thai government which needs to changes their policy and strategy for balancing security and good governance.

Policy Goals

What policies should Thai government follow to balance good governance and national security in the same time? An answer to this question requires the specification of policy goals that provide an appropriate basis for comparing current

policy with possible alternatives. The preceding discussion of problems inherent in the status quo immediately suggests a number of important goals.

First, social media censorship policy is a potential value for national security and easy to control and manage, because of good governance it is a currently iniquity on Thai government. Thus, a primary goal, therefore, should be good governance of Thai government. The primary measure of the projected impact of each alternative in terms of this goal is transparency. One of the principal ways that the government can improve their accountability is by becoming more transparent that are, offering more information to the public and allow people critical and share their opinion.

Second, it relates to primary goal that democracy it will helps Thai government more good governance according to The National Democracy Indicators (NDI, 2007) is designed to determine how a society is doing in developing as a democracy. It is just one of many tools that can be used to judge a society. The objective of the democracy indicators is to have the participants judge their own democratic institutions to determine where they are strong and where they are weak. Moreover, according to World Democracy Audit ranking Thailand rank 89 out of 150.

Therefore, the empirical data shown that Thai democracy is low level thus, to improve Thai democracy which is a principal ways that Thai government needs to let civil and political participate in social media and internet. Thus, the primary criterion for measuring progress toward this goal is the level of people participation in social media and website block rate.

Third, nation security is one of the policy goals that help Thailand secures from cybercrime, cyber-terrorism, and tradition terrorism. According to Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana (Report on Thailand's CCA prosecutions and Internet censorship-iLaw, 2001) in Freedom Against Censorship Thailand point out the cybercrime rate has been rising since 2005 from 9 to 185 in 2010. Thus, the primary criterion for measuring progress toward this goal is the degree of cybercrime, cyber-terrorism, and tradition terrorism rate.

Fourth, Costs and benefits of the good governance and national security should be maximizing distributed to Thai people. Thus, cost-effective should be a policy goal. Maximizing requires that government spends their cyber security budget in terms of smallest amount but gain a maximize efficiency. Moreover, minimize cyber security budget will sharply effects to cyber security unit which is the Technology Crime Suppression Division (TCSD). This division is under The Ministry of Information and Communication Technology (MICT). However, as an alternatives policies have implications for government budgeting and expenditures, minimize government budget needs to be concern. According to Ministry of Information and Communication Technology (MICT) budgeting in 2012, cyber security has 32,885 Million Thai Baht (1,096.1 Million US dollars). Therefore, the primary criterion for measuring progress toward this goal is minimizes fiscal year specifically in cyber security.

It is important to note that the goals are often in conflict. For example, while reduce cost on Technology Crime Suppression Division (TCSD) might be made bureaucracy officers works inefficient and inefficiency, it would conflict with the goal of cost-

effective. Therefore, selecting the most beneficial to people or society desirable policy involves making trade-offs among the goal.

Alternative Policies

The analysis presented in the remainder of this report compares the status quo policy to the following three alternatives.

1. Cooperation with trusted Non-Government Organization (NGOs)

This alternative adapted concept from Transparency of Intergovernmental Organizations by Alexandru Grigorescu. His research analyzed the ability of NGOs that provides information and answer question to public which is accountability and transparency. Thailand is one of the countries where NGOs have been playing an important role in the country's economic, social, and political development. Thus, there are a numbers of trusted NGOs is that people can rely on. This is the most important for people can received an official information and correct data from trusted organization besides government released or distributed to public. For examples trusted NGOS in Thailand, Wongsanit Ashram, Duang Prateep Foundation, and Thailand Volunteer Service Foundation (TVS). However, recently and the government did not cooperate with NGOs to distribute information and data. Therefore, with this opportunity this alternative policy will help government improve their good governance.

2. Amendment Computer Crime Act

This alternative largely follows the social media phenomena around the world and social media concept by Antony Mayfield (2008). Social media is as a group of new kinds of online media, which share most or all of the following characteristics: participation, conversation, openness, community, and connectedness also the phenomena around the world such as Arab spring, Occupied Wall Street, and U.S. elections. This empirical evidences that social media is positive tools rather than negative tools. Thus, social media allows government to have a closer, more intimate relationship with people and being authentic in social media really means to be government itself, but with filters.

3. Government participates in social media

This alternative strongly recommend from the most famous empirical phenomena specifically in US. Governments may not be early adopters but the proliferation of social in national media has ramped up its importance for governments around the world. While this initial stance kept politicians on the defensive, enough time has passed that individual politicians and even entire governments are starting to use social media to connect with their communities in new, open ways.

In US case, Social media has a strange role in America as both kingmaker and career wrecker. For every social media success story like President Barack Obama's 2008 grassroots campaign there is another of a career-crippling gaffe, like Weinergate, when New York Rep. Anthony Weiner accidentally tweeted a picture of his crotch. Consequently, Social media can help government and government agency promote

government information and services. Moreover, government uses this tool like Facebook, Tweeter, and Youtube to bring people together around government and their agency's work and information. Also social media expand the government's outreach capabilities and improve their ability to interact with and serve the public.

Thus, government participates in social media will ease Thai government more transparency, improve democracy, and gain people allies with government to help national security in cybercrime, cyber-terrorism, and tradition terrorism. In addition, interagency and intergovernmental social media can promote cooperation across government. Internal social media can establish connections across hierarchy and geographically dispersed organizations which will help government collect information and data faster and more accurate to protect and suppress cybercrime, cyber-terrorism, and tradition terrorism. Also it will strongly effect to cost-effective because of government does not have to heavily invest for cyber security, people across the country and boarder will form community to monitor cyber security and share information among them and government. Therefore, government fiscal year will sharply decrease but maximize efficiency on cyber security.

Conclusion, Assessment, and Recommendation

The issues discussed in this section of the report are summarized in a simple matrix (table 1) that presents policy alternatives on one dimension and the goals for assessing them on the other. It should be stressed that these are predictions, based on the empirical data and succeeded sample, of how each of the alternatives would perform in terms of government goals. Of course, the preferred alternative depends on how Thai government weights the goals described above.

Table 1, summarizes the major impacts described in the previous section. It is clear that all three alternatives are superior to the status quo in terms of most all the goals. Government participates in social media is the highest-ranked alternative in terms of good governance because it would result government is more transparency and accountability which is a two ways communication. Government distributes information also communicate directly to people and people can share their opinions or participates with government agencies. Moreover, it will improve democracy which people are more participation and expression their opinions, their voice can count. But it still has a weakness point that Thai government can get fraud information from people who do not like this government and anti-government or trouble makers. It should concerns in political feasibility as well because of opposite political interest group will use this channel to discredit to recent government, thus it needs to filter information to select good information and delete misinformation. Also national security efficiency, because of government and people are sharing information, cooperation which is a nationwide networking and cost savings. Most of this entire benefit of this alternative is government can do right away and it will not create a political conflict. Also government can gain support from people and political stability.

Moreover, to implementation this alternative policy, current Yingluck administration can do right away. To do so, prime minister provides this policy to ministry of ICT to implement it by release government official information then creating two ways communication in bureaucratic official website in social media platform such as Line,

you tube, Tweeter, and Facebook. After that promote civil servants and government agencies use social media to update information or answering question from people. Meanwhile, promote on public broadcast and social media to let people join and share information to help government improve democracy, political stability, and especially national security. Finally, government agencies can collect feedback from people and evaluate people respondent to improve policy.

On the other hand, amendment the computer crime act is a second place but the weakness is it will create a huge political conflict in parliament between Pros side who would like to deregulation this law and Cons side which concerns more security especially from ministry of ICT and TSCD department who is a main player. Moreover, it will cost a lot of money to make a referendum and time consuming. However, in the long run government will improve good governance and democracy which are more transparency and accountability. Because of government disclose information and cooperate with people also national security as well.

In addition, cooperation with trusted NGOs is the third place. Thai government will gain more good governance and democracy because of trusted NGOs will supports government which become alternatives distribution information channels and bridge between government and people. Even though NGOs in Thailand has a long history and it is one of the main player in many dimensions but it will create a conflict between ministry of ICT and TSCD department. Ministry of ICT will reduce their role and especially their annual budgeting also cyber-crime and cyber terrorism committee their crime indirect to government organizations both on cyber and infrastructure via trusted NGOs social media channels.

Finally, it is a close call in choosing among these three alternatives. My recommendation is that the government should adopt government participates in social media. This is, however, a radical departure from status quo, and it would not difficult to implement and it would not be a political conflict rather than another alternative or status quo. Therefore, Thai government can balance their good governance and national security in the same time.

Table 1: A Summary of Balancing Good Governance and National Security Alternatives in Terms of Policy Goals

Goals	Criteria	Policy Alternatives			
		Current Policy: Continued censorship	**Cooperation with trusted Non-Government Organization (NGOs)**	**Amendment Computer Crime Act**	**Government participates in social media**
Good Governance	Government distributes information to the public	**Poor-** Hi negative respond from people. People cannot receive sufficient information.	**Good** Hi positive respond from people. People can receive sufficient information via trusted NGOs	**Excellent** Law and policy disclose make government transparency and promote accountability	**Excellent** Government engages in social media and it helps government more transparency
Improve Democracy	The level of people participation in social media and website block rate	**Poor** A number of website block is hi rate but limited people participate in social media	**Good** Numbers of NGOs website increasing and people participate via social media but the website block rate still high mostly on political	**Excellent** Government and people cooperate each other. Government will receive public feedback to improve their performance	**Good** It is a two ways communication but Gov. can get fraud information and website blocks rate are reducing sharply
Improve National Security	The degree of cybercrime and cyber-terrorism rate	**Poor** Cybercrime rate is hi level	**Fair** Government gains alliances to share information and reduce cybercrime rate but cyber terrorists can use NGOs social media to commit cyber crime	**Excellent** Government's improves the quality of information and cybercrime and cyber-terrorism rate will decrease sharply	**Excellent** Government collaborates with public and private to create network for greater safety cyber security and the crime rate will reduce dramatically
Cost-Effective	Minimize fiscal year specifically in cyber security and reduce poverty	**Poor** Annual cyber security fiscal is hi and but poverty rate is medium	**Good** Cyber security annual fiscal will reduce and government can spends the surplus to another program but it will create controversy between TSCD unit and NGOs	**Good** Time consuming to amendment the law and policy**.** Also government must spend a lot of money to make a referendum	**Excellent** The potential for increased efficiency and cost savings. Also reducing poverty rate sharply

References

Aelst, J. V. (2009). *Cyber-Protest and Civil Society: the Internet and Action Repertoires in Social Movements in Handbook on Internet Crime.* Devon: Willan Publishing.

Barber, B. (1984). *Strong democracy, participatory politics for a new age.* Los Angeles: University of California Press.

Beramendi, V. A. (2008). *Direct democracy* . Stockholm: The Internationa IDEA.

Charoen, D. (2012). The Analysis of the Computer Crime Act in Thailand. *International Journal of Information and Communication Technology Research Volume 2 No. 6*, 519-526. Retrieved from , "", May 2010.

Clive, C. (2012). Towards understanding eParticipation in the public sphere. *Review of Business Research (International Academy of Business and Economics)*, 140-146.

Coleman, B. J. (2001). *Realising democracy online: A civic commons in cyberspace* . London: Institute for Public Policy Research.

Coleman, S. a. (2009). *The internet and democratic citizenship: Theory, practice and policy.* Oxford: Oxford University Press.

Gilberto Corso Pereira, M. C. (2012). e-Participation: Social Media and the Public Space. *International Conference on Computational Science and Its Applications* (pp. 491-501). Heidelberg: International Conference on Computational Science and Its Applications.

Grigorescu, A. (2007). Transparency of Intergovernmental Organizations: The Roles of Member States, International Bureaucracies and Nongovernmental Organizations. *International Studies Quarterly, Volume 51, Issue 3*, 625-648.

Jonathan, F. (2010, 06 19). *Internet censorship:The iron firewall of the 21st Century*. Retrieved from eastasiaforum.org: http://www.eastasiaforum.org/2010/06/19/internet-censorship-the-iron-firewall-of-the-21st-century/

Mark Manyin, E. C. A. (2004). *Terrorism in Southeast Asia.* The Library of Congress: Congressional Research Service.

Nojeim, G. (2009). *Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace.* Center for Democracy and Technology.

Pasuk Pongpichit. (2001). Good Governance: Thailand's Experience. *Asia Pacific Finance Association (APFA)* . Bangkok: APFA.

Peter Chalk, A. R. (2009). *The Evolving Terrorist Threat to Southeast Asia: A Net Assessment.* Santa Monica, CA: RAND Corporation.

Powner, D. (2009). *NATIONAL CYBERSECURITY STRATEGY Key Improvements Are Needed to Strengthen the Nation's Posture.* United States Government Accountability Office.

Putnam, T. a. (2001). *International Responses to Cyber Crime in The Transnational Dimension of Cyber Crime and Terrorism.* Editors: The Hoover Institution Press.

Sawatree Suksri, S. K. (2011, 01 05). *Report on Thailand's CCA prosecutions and Internet censorship-iLaw, 2001.* Retrieved from Freedom Against Censorship: http://facthai.wordpress.com/2011/01/05/report-on-cca-prosecutions-and-internet-cen

Shetret, L. (2011). *Use of the Internet for Counter-Terrorist Purposes.* Center on Global Counterterrorism Cooperation.

Thailand, F. A. (2013, 11 07). *Freedom Against Censorship Thailand*. Retrieved from Freedom Against Censorship Thailand: http://facthai.wordpress.com/cybercrime-bill/

Vadhanasindhu, C. (2001). Good Corporate Governance in Thailand. *Thai Journal of Development Administration*, 37-54.

Wilson, C. (January 29, 2008). *Botnets, Cybercrime, and Cyberterrorism:Vulnerabilities and Policy Issues for Congress.* CRS Report for Congress.