Situational Report on Control and Censorship of Online Media, through the Use of Laws and the Imposition of Thai State Policies

by the Research Team on "The Effect of the Computer Crime Act 2007 and State Policy on the Right to Freedom of Expression"

Situational Report on Control and Censorship of Online Media, through the Use of Laws and the Imposition of Thai State Policies

This forms part of a research project on the effects of the Computer Crime Act 2007 and state policies on the right to freedom of expression

Research Team:
Sawatree Suksri, Director
Siriphon Kusonsinwut
Orapin Yingyongpathana

Research Assistants:
Danuch Wallikul
Yingcheep Atchanont
Thanakrit Piammongkol
Tewson Seeoun

Editor (English version):
Alec Bamford

Translator:
Pokpong Lawansiri

Cover Design:
Bundit Uawattananukul

Graphic Design:
Wipaporn Masrinoul

Production Editor:
iLaw Project

Financial Support:
Heinrich Böll Stiftung

Table of Contents

Situational Report on Control
and Censorship of Online Media, through the Use of Laws and the Imposition of Thai State Policies

8 December 2010

Section 45[1] of the 2007 Thai Constitution guarantees to the people the right to freedom of expression in all forms and the right to access to information. This section includes granting clear protection to media practitioners and the right to disseminate news. Media in this sense includes both traditional (mainstream) media and new alternative media. Nevertheless, under the system of the rule of law, a person's rights and liberties are limited under the law. Therefore, we can see that even the constitution includes certain provisions empowering the state to enact legal measures to limit or control the exercise of these rights and liberties. There are four justifications for this: national security; public order and good morals; to protect the rights of an individual or reputation of others; and to prevent or halt the psychological or physical deterioration of the public. However, although in its status as administrative authority, the state can pass laws or other measures to manage, screen or limit these rights and liberties, such laws and measures should be proportional to the need, cannot infringe upon the

[1] Section 45 of the Thai Constitution states that "[a] person shall enjoy the liberty to express his opinion, make speech, write, print, publicise, and make expression by other means.

The restriction on liberty under paragraph one shall not be imposed except by virtue of the law specifically enacted for the purpose of maintaining the security of State, protecting rights, liberties, dignity, reputation, family or privacy rights of other person, maintaining public order or good morals or preventing or halting the deteriorating of the mind or health of the public.

The closure of a newspaper or other mass media business in deprivation of the liberty under this Section shall not be made.

The prevention of a newspaper or other mass media from printing news or expressing their opinions, wholly or partly, or interference in any manner whatsoever in deprivation of the liberty under this Section shall not be made except by the provisions of the law enacted in accordance with the provisions of paragraph two.

The censorship by a competent official of news or articles before their publication in a newspaper or other mass media shall not be made except during the time when the country is in a state of war; provided that it must be made by virtue of the law enacted under the provisions of paragraph two.

The owner of a newspaper or other mass media business shall be a Thai national.

No grant of money or other properties shall be made by State as subsidies to private newspapers or other mass media."

essence of these rights and liberties, and must be enforced in a non-discriminatory manner.[2] However, for many years, the Thai government, through relevant agencies, has enacted laws and taken measures to control and interfere with media reporting in an unbridled and discriminatory manner. A great number of websites have been blocked with no clear reason given as to which part of the content in unlawful. In cases where reasons are given, it is debatable whether the blocked content reaches the point of illegality as threatening national security or contravening public morals. The problem arises from the vagueness of the legal language and the broad personal interpretation by state officials. In addition, in many cases where websites are blocked, the Thai government did not use legal channels such as requesting in advance a court warrant as specified under the Computer Crime Act B.E. 2550 (2007)[3] (CCA), but simply requested cooperation from internet service providers to block access to websites which the Thai state sees as "inappropriate", but which may not qualify as unlawful.

Online media has been restricted and censored ever more severely since Thailand faced an 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 and their property, the society, and political matters. However, the state has relied on powers under the Emergency Decree on Public Administration in Emergency Situations B.E. 2548 (2005) (hereafter called the "Emergency Decree")[4] to interfere with and block news without reason, even though specifying the content that is illegal is a "condition for using this power" as stated in the Decree itself. Apart from this, there are reasons to believe that the state is enforcing the law in a discriminatory manner because when content and pictures are presented with the same level of violence, the state chooses to persecute

---

[2] Section 29 of the Constitution states that "[t]he restriction of such rights and liberties as recognised by the Constitution shall not be imposed on a person except by virtue of the law specifically enacted for the purpose determined by this Constitution and only to the extent of necessity and provided that it shall not affect the essential substances of such rights and liberties.

The law under paragraph one shall be of general application and shall not be intended to apply to any particular case or person; provided that the provision of the Constitution authorising its enactment shall also be mentioned therein.

The provisions of paragraph one and paragraph two shall apply mutatis mutandis to rules or regulations issued by virtue of the law."

[3] Section 20 of the Computer Crime states that "[i]f an offence under this Act is to disseminate computer data that might have an impact on the Kingdom's security as stipulated in Division 2 type 1 or type 1/1 of the Criminal Code, or that it might be contradictory to the peace and concord or good morals of the people, the competent official appointed by the Minister may file a petition together with the evidence to a court with jurisdiction to restrain the dissemination of such computer data."

only media which presents information that the state sees as being unfriendly or in opposition to the state, but allows other media to operate freely. Even though there have in the past been efforts by many sectors to make appeals to the public, including cases filed in the courts, there has been no satisfactory response. There have been cases where the courts refuse to investigate the use of authority by the executive. (An example is an adjudged case No. 1812/2553 where Prachatai sued the Prime Minister and the Centre for the Resolution of the Emergency Situation [CRES] over the order to close their website.) Moreover, there are cases where a considerable number of members of the public and internet service providers have been accused of disseminating content that is inappropriate or illegal under a number of laws.

Based upon these disturbing facts which are not in line with democratic principles and governance, a research project was carried out on "The Effect of the Computer Crime Act 2007 and State Policy on the Right to Freedom of Expression" by a research team in cooperation with the iLaw project supported by the Heinrich Böll Stiftung. The purpose of the project is to research and gather legal information, compare policies of the Thai state with those of other countries, and document the number of websites that have been blocked, and the number of legal cases related to the right to freedom of expression in online media at all levels of the legal system since the promulgation of the CCA. This is to show the effect of law enforcement and state policy on freedom of expression in Thai society. This report also gives recommendations to remedy the situation by comparing the experience in law enforcement and policies of other states.

However, the figures presented in this report represent information obtained from only a few relevant departments. Although reference can be made to this information, any such reference must indicate its limitations in terms of diversity of information and source of information.[5] Moreover, this report is aimed to be published in the first seminar. The plan is to publicise the information gathered and push the issue out into the public sphere. The comparative study of legal matters and state policies and aspects touching on civil society groups are preliminary presentations as this is only the first part of the research. All information, including recommendations by the researchers, will be presented in the form of a more complete report in the future.

---

[4] Section 9 of the Emergency Decree states that "[i]n the case of necessity in order to remedy and promply resolve an emergency situation or to prevent the worsening of such situation, the Prime Minister shall have the power to issue the following Regulations [...]:

(3) to prohibit the press release, distribution or dissemination of letters, publications or any means of communication containing texts which may instigate fear amongst the people or is intended to distort information which misleads understanding of the emergency situation to the extent of affecting the security of state or public order or good morals of the people both in the area or locality where an emergency situation has been declared or the entire Kingdom"

Part 1

Statistics of Cases and Blocked Websites under the Computer Crime Act 2007

Source of information and relevant agencies in computer-related cases

The CCA was the first bill to be considered by the National Legislative Assembly (NLA) and was scrutinised in a very short time. It became the first law promulgated by the cabinet of General Surayud Chulanont on 18 July 2007. The Ministry of Information and Communication Technology (MICT) is the ministry in charge of enforcing the law and coordinating with other relevant agencies such as the Department of Special Investigation (DSI) and the Office of the Royal Thai Police (RTP). Nevertheless, it appears to be the case that until today, the number of officials with sufficient knowledge and ability in dealing with this kind of case is not very large in comparison with the number of cases that have been filed.[6] This is even more evident when state officials in the provinces are considered. Therefore most cases that have been filed at different police stations around the country have to be transferred to agencies in the capital that are thought to be familiar with the field, such as the Economic and Technology Crime Suppression Division (ETCS). The agency was restructured in September 2009 and divided into two agencies, namely the Economic Crime Division (ECD) and the Technology Crime Suppression Division (TCSD) so that the two agencies can deal with issues in the area of their expertise. Currently the TCSD is the agency that is

[5] This research is limited by the inability to gain full access to complete statistics on cases and websites that have been blocked. At the time of this research (when the researchers filed a request for information), no government agency had been tasked with documenting or creating a database on cases and making this information available to the public. The information was accessed through official requests or research at the relevant agencies. Some agencies were unable to provide information to the public for various reasons. These include: structural changes in the organisation; new officials tasked to monitor the information not yet familiar with the system; case data not available in digital form; relevant official transferred taking the information with them; no documentation of computer-related cases. However, while some agencies have documentation, this is in summary form and does not provide extensive details of the cases.

To make the information as reliable as possible, information was requested from the relevant agencies and officials as far as possible, and later combined. The figures in this research therefore represent a minimum number of cases that could be compiled for the period July 2007 – July 2010 only. The information that could not be accessed is mostly information from investigative officials or provincial police.

[6] The CCA stipulates that enforcement of the act must be by government officials that have been appointed by the Minister of Information and Communication Technology. These officials must have expertise in the field of work related to the cases. The Act specifies that exceptions can be made at the Minister's discretion. Currently, only 96 officials that have been authorised to work under the CCA. This number comes from the 1st to 9th Declarations by the MICT on the Appointment of Officials under the CCA. These officials are scattered around different government agencies such as the Department of Special Investigation, the Ministry of Information and Communication Technology, the Signals Department of the Royal Thai Army, and the National Intelligence Agency. Almost all of these agencies are based in Bangkok.

tasked to look directly at technology-related issues. However, since crime on the internet is interconnected with many kinds of offence, cyber crime cases are relevant to many agencies. For example, if the offence is related to the dissemination of pornography, the case would be with the Children, Juveniles and Women Division (CWD). There are also cases that link with the work of the Anti-Human Trafficking Division (AHTD). If the case is related to national security, it would be under the jurisdiction of agencies such as the Crime Suppression Division (CSD) or DSI. Most of the cases related to CCA in 2010 are being investigated by the two latter agencies.

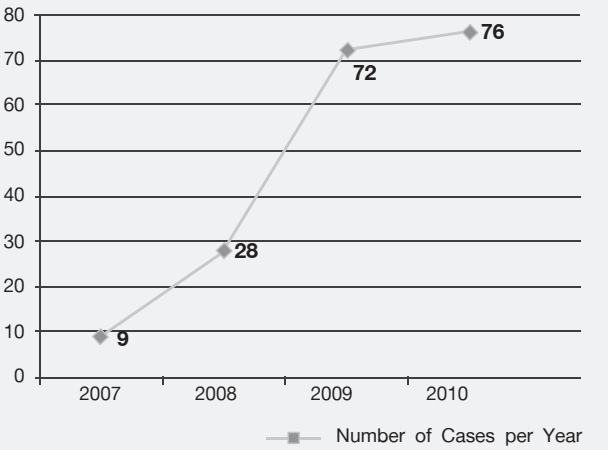
In addition, since this research project seeks to understand the effects of the enforcement of CCA through the use of two sets of data, namely statistics on prosecutions and statistics on blocked websites, the information was compiled from the following government agencies:

- Ministry of Information and Communication Technology (MICT)
- Economic Crime Suppression Division (ECD)
- Technology Crime Suppression Division (TCSD)
- Department of Special Investigation, Ministry of Justice (DSI)
- Crime Suppression Division, Royal Thai Police (CSD)
- Criminal Court

Research Finding : Statistics on prosecutions under the CCA

Based on data from July 2007 to July 2010, it was found that there are altogether 185 cases under the CCA: nine cases in 2007, 28 in 2008, 72 cases in 2009, and 76 in 2010.

Number of Cases Under Computer Crime Act from July 2007 to July 2010



These 185 cases can be analysed in terms of their progress through the judicial process and case outcomes. 1) 74 cases are with the investigators or the police; 2) 43 cases have charges brought by the public prosecutor; 3) one case was dismissed by the public prosecutor; 4) 10 cases ended with mediation, settlement, or with the charge being withdrawn; 5) two cases had the charges dismissed by the court; 6) 37 cases received verdicts of guilty; 7) 14 cases have been adjudicated by the court but the researchers could not get the access

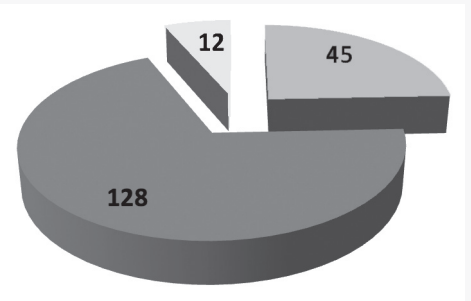
to the trial verdict; and 8) in four cases with charges under the CCA, the public prosecutor has not brought charges or the court has ruled that the offence does not fall under the CCA.

Category of Offence		Procedure of the Case							Total
	Investigating	Public Prosecutor		Court					
		Charged	Not Charged	Not Charged with CCA	Mediated/ Withdrawn	Dismissed	Guilty	Verdict made but no result	
Offences under section 5-13	26	8	0	1	2	1	6	1	45
Offences under section 14-16	48	30	1	3	8	1	31	6	128
Cannot be defined	0	5	0	0	0	0	0	7	12
Total	74	43	1	4	10	2	37	14	185

Cases under Computer Crime Act from July 2007 to July 2010

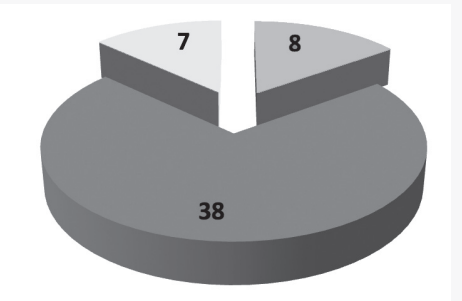
Offences under the CCA can be divided into two main categories: 1) traditional computer crimes comprising offences concerning computer data or computer systems according to sections 5-13 of the Act, including hacking into a third party's computer data, illegally accessing computer data, or sabotaging computer systems by disseminating destructive software; and 2) offences under sections 14 to 16 which deal with importing content into computer systems which the public can access. The offences here include importing information with pornographic content, information that affects national security, or defamation of third parties by edited pictures. Statistics covering three years since the CCA came into force show that 45 cases fall into the first category (24.32%) and 128 cases into the second category, (69.19%). 12 cases (6.49%) cannot be clearly categorised.

All Cases Related to Computer Crime Act



Offences related to the system (24.32%)
Offences related to the content (69.19%)
Not mentioned (6.49%)

Cases Under Computer Crime Act that the Courts Made Judgement



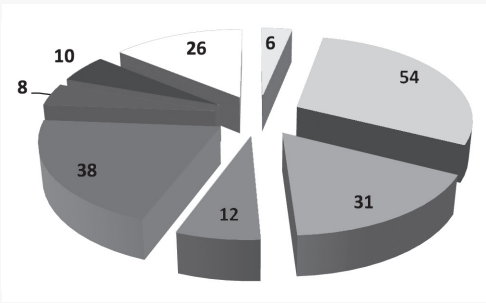
Offences related to the system (15.09%)
Offences related to the content (71.70%)
Not mentioned (13.21%)

Proportion of computer crime cases in each category

These cases can be divided into eight categories of offence:

- 54 cases involving defamation of third parties
- 38 cases involving content of a fraudulent nature (use of the internet as a tool for fraud)
- 31 cases involving lèse majesté content
- 26 cases involving other issues that cannot be categorised
- 12 cases involving pornographic content
- 10 cases involving merchandising illegal computer programmes
- eight cases involving traditional computer crime
- six cases related to national security

Numbers of Cases under Computer Crime Act Segregated by Contents



National Security (3.24%)
Defamation of third parties (29.19%)
Lèse majesté content (16.76%)
Indecent acts (6.49%)
Fraud (20.54%)
Traditional computer crimes (4.32%)
Selling illegal programmes (5.41%)
Others (14.05%)

Computer Crime Cases	National Security	Defamation	Lèse Majesté content	Pornography	Fraud	Traditional Computer Crimes	Selling Computer Programmes	Others	Total
With the investigator or with the police officials	2	12	24	1	16	5	10	4	74
Charged by public prosecutor	2	16	3	1	10	1	0	10	43
Dismissed by public prosecutor	1	0	0	0	0	0	0	0	1
Public prosecutors do not charge the case or the courts rule that the penalty is not under the CCA	0	3	0	0	1	0	0	0	4
Ended with mediation, settlement, or with the charge being witdrawn	0	6	0	0	3	0	0	1	10
Court dismissed the charge	0	1	0	0	0	1	0	0	2
The verdict rules that the defendant are guilty	1	14	4	8	7	1	0	2	37
The court has delivered the verdict but the researchers could not get the access to the result of the trial**	0	2	0	2	1	0	0	9	14
Total	6	54	31	12	38	8	10	26	185

The Progress of the Case under Computer Crime Act; Categorised According to Contents or Actions that Led to Being Charged

** Cases which CCA was charged at the investigation level, but the public prosecutor filed the charge or the judge made the verdict not under CCA*

*** These are information received from cases in the provinces. There are specific numbers and cases, but there is no information about the action of the accused and the result of the verdict.*

In addition to categorising cases according to the offence, cases can also be categorised according to the person making the accusation. In order from the highest to lowest number, 40 cases were filed by females; 30 cases had no clear origin; 27 cases were filed by juristic persons; 26 cases by males; 16 cases by the Ministry of Information and Communication Technology[7] ; 14 cases by the Technology Crime Suppression Division; nine cases by the Crime Suppression Division; eight cases by other governmental agencies; five cases by the Department of Special Investigation[8]; four cases by the Children, Juveniles and Women Division; and three cases each by the Economic Crime Division and local police.

Analysis and observations on the number of cases related to online media offences and the effect on the right to freedom of expression and opinion

Examination of all cases for which data is available shows that three years after the implementation of the CCA, the number of offences related to content is extremely high when compared with offences in other categories. Offences related to content are prosecuted under the CCA alone or in combination with other laws. The following observations can be made.

1) Offences related to defamation:

Senders and receivers of information on the internet can conceal their identities. Although they can be tracked down, it is not as easy as in normal society. Therefore, internet users can criticise, accuse, or disseminate photos and private information concerning a third party and destroy their reputation and honour without much fear of being arrested. For this reason, the number of defamation charges being brought to court has been rising, even though the plaintiff may not know who the culprit is. Also, in the past few years, there is evidence that a large number of defamation cases have been used as political weapons by politicians filing against one another or against the media. These cases take the form of criminal or civil charges demanding enormous sums in compensation. It is also to be noted that there are legal interpretations that argue that Section 423 of the Thai Civil Code and Section 328 of the Criminal Code are already sufficient protection against defamation, with no need for the section related to defamation in the CCA. In practice, a large number of defamation cases on the internet are prosecuted by combining charges under the Civil Code or Criminal Code with Section 14 (1) of the CCA (since they are not cases of defamation through the editing of photos under Section 16 of the CCA). In reality,

[7] Although the information obtained shows that altogether only 16 cases have been filed by the MICT, one case was filed by with the Crime Suppression Division together with a list of websites deemed violating Section 112 of the Criminal Code which prohibits lèse majesté. This case is still under investigation by the police. Examination of the case and the attached list of 1,037 URLs shows a possibility that there could be 997 more cases following along.

[8] The Department of Special Investigation is one of the agencies which told the researchers that there are a number of "Monarchy-Overthrowing" cases which are still being investigated but cannot be made public. A number of websites that could be related are still under investigation.

whether by an interpretation of the intent of the drafters of the CCA or the wording of Section 14 (1) of the CCA regarding the import of false or incorrect information into computer systems in a way which may harm others, the CCA is not meant to be used in a manner similar to defamation in the Civil or Criminal Code. This reveals that law enforcement officials and agencies within the Thai justice system clearly lack a sound understanding of the CCA and have used it on an incorrect basis in a confused manner, resulting in figures for CCA cases even though there may be no need to use the CCA in these cases.

2) Offences related to the dissemination of pornography:

The ability to conceal one's identity, the capacity of high speed internet communication technology and easy access are the factors that make the internet an important source for the dissemination of indecent images that may be interpreted as violating the laws prohibiting pornography. Similar to the situation with defamation offences, Thailand already has laws on obscenity under Section 287 of the Criminal Code on offences related to the public distribution of obscene images. However, the drafters of the CCA believed that this issue should be clearly defined to prevent the problem of Section 287 being interpreted as inapplicable. Nevertheless, the relationship between Section 287 of the Criminal Code and Section 14 (4) of the CCA should be that between a general law and a specific law. If a case involves an offence on the same issue or with similar characteristics relevant to both general and specific laws, the specific law should be applied first so that the accused will not be charged under different laws for the same offence. However in practice, it happens that once the CCA was promulgated, the police and public prosecutor filed charges using both the CCA and Criminal Code. The Courts themselves have ruled that the accused is guilty on both charges, which is questionable.

3) Lèse majesté charges:

In three years since the promulgation of the CCA, 31 cases have involved lèse majesté charges. The MICT has initiated or filed 16 cases. Other agencies that have filed charges include the Crime Suppression Division (six cases), the Department of Special Investigation (four cases), the Technology Crime Suppression Division (two cases), the Secretary to the Prime Minister (one case), and individual citizens (two cases). Of these 31 cases, the courts have delivered judgments in four, the public prosecutor has filed charges in three, and 21 cases are under investigation. An official from the Department of Special Investigation provided supplementary information that a large number of cases have been lumped together as "cases involving the overthrow of the monarchy", but could not disclose figures or information on these cases. These cases are typically dealt with under Section 14 (2), which concerns the importing of false data into a computer system that could damage national security or create public panic, and Section 14 (3), which involves importing into a computer system data related to offences against the security of the Kingdom or terrorism offences according to the Criminal Code. In addition,

Section 14 (5) is applied to cases of forwarding such information. 25 cases in all involve lèse majesté charges under Section 112 of the Criminal Code together with charges under the CCA. Therefore, we can see how the Criminal Code has been used together with the CCA. If charges are filed against an intermediary or internet service provider, officials will also use Section 15 of the CCA.[9]

Those who have been following the issue closely may have seen that in the past few years many agencies, whether the government, the military, the police, the MICT, the Ministry of Justice or the Ministry of Culture, all have policies to keep close watch on the behaviour and opinions of Thai citizens on the internet. State policy is heavily focused on controlling internet content. This policy has been quite strong within the MICT under Mr. Sitthichai Pookaiyaudom (Minister of Information and Communication Technology from 9 October 2006 to 30 September 2007), Mr. Kosit Panpiemras (Acting Minister from 1 October 2007 to 6 February 2008), Mr. Mun Phathanothai (Minister from 6 February 2008 to 2 December 2008), Sub-Lieutenant Ranongrak Suwanchawee (Minister from 20 December 2009 to 6 June 2010) and Mr. Juti Krairiksh (Minister from 6 June 2010 to the present). The main focus of the MICT is on inappropriate content, including comments or criticisms about institutions such as the monarchy, religion and the courts. During some administrations, the policy has gone as far as controlling content that criticised the work of the government or the Prime Minister. In the past, apart from policies to accelerate the blocking of websites, press charges against internet users and internet service providers and announce the number of websites that are blocked under each minister, there has also been the establishment of the Network of Navy Quartermaster to Promote and Protect the Monarchy on the Internet, the Internet Security Operation Centre (ISOC), and the Cyber Scouts. A Memorandum of Understanding (MOU) between 3 ministries, namely the MICT, Ministry of Justice, and Ministry of Culture, was signed to monitor internet use and create a state counter media with two operational approaches: 1) to uphold the Monarchy through the creation of websites disseminating clips, articles and videos through the internet; and 2) to prevent and suppress lèse majesté on the internet, to identify websites with comments that qualify as lèse majesté offences, to alert and report to superiors and to file criminal charges. State policy and various existing laws, which have been seriously questioned

[9] Out of all the cases, 11 individuals have been charged under Section 15 of the CCA. Interesting cases include that of the owner of the 212cafe website which hosts a free web board. The person was informed, not by a state official, of an image with pornographic content on his web board. He then removed the photo, but a few days later the web owner was arrested by the police. Another case concerns charges pressed against the Executive Director of Prachatai based upon a comment made on the Prachatai web board which an individual reported as falling under Section 112 of the Criminal Code. The comment was made in response to an article in Prachatai. The article itself did not violate Section 112. In addition to these two cases, the Pantip website was charged with defamation as an intermediary which provided a forum for discussion which resulted in defamation on the web board.

regarding their vagueness and how they have been legally interpreted, contribute to the increasing number of cases. The large number of cases may be cited to show that the CCA has been used as a political tool to attack the opposition, especially the use of the CCA together with Section 112 on lèse majesté.

There are additional observations to be noted. 1) A number of cases in the past year are directly linked to the Social Sanction (SS) group using social networks such as Facebook and Twitter. The SS, a network of internet users on different social networks, operate by looking for individuals who disseminate content that could be viewed as lèse majesté. They then condemn and vilify these individuals in public and search for private information on those individuals which they further disseminate to the public. It is a fact that the Department of Special Investigation has taken up cases publicised by the SS.[10] 2) The law enforcement agencies work in a very discreet manner when it comes to cases under this category. Information related to the cases remains confidential and off limits to non-officials, with excuse that publicising the cases is inappropriate and the cases are related to national security. Therefore, there might be a large discrepancy between the published figures and the actual number of cases. As the researchers have mentioned, statistics on CCA cases in this report do not include one case received by the Crime Suppression Division from the MICT to investigate 1,037 URLs. The CSD has separated these URLs into 997 cases which are currently being looked at further by police investigators.

4) Content affecting national security and public morals:

The CCA gives high importance to preservation of national security through Section 14 (2) and (3). This is suspicious because Section 14 (3) is already sufficient and clear in linking offences under the CCA to offences under the Criminal Code related to national security, and there is no reason for Section 14 (2) on national security. The upshot is that this section could be used as political weapon due to its obscure meaning that allows state officials to create their own interpretation. The way in which the six cases related to national security have been prosecuted gives rise to speculation that with the problems of interpretation and the current political situation, the number of national security-related cases may greatly increase since prosecutions are likely to be brought on security-related charges alone, and in conjunction with lèse majesté and terrorism charges.

[10] The technique of vilification has emerged and spread to many web boards. In late April 2010, a comment by one Facebook user on their own Facebook page was publicised and vilified for insulting the monarchy. A group of web board users searched for the individual's personal information and publicised this information. A day later, officials from the Department of Special Investigation arrested this individual. Following this case, another Facebook user was arrested after making comments on a remark that were claimed to be lèse majesté and being vilified on a web board. Both of them are currently being investigated by the Department of Special Investigation.

Research Finding : Use of judicial orders to stop dissemination of information

Since the CCA came into force, the Thai state, through the Minister of Information and Communication Technology, has been able to use measures to block or halt the dissemination of computer data which "might have an impact on the Kingdom's security or that might be contradictory to the peace or good morals of the people" through the power given under Section 20 of the Act. This particular section states that an official appointed by the Minister may file a petition with evidence to a court with jurisdiction to halt the dissemination of computer data. The researchers found evidence of 117 court orders to block access to websites since the promulgation of the CCA. In 2007, there were court orders to block access to two URLs; in 2008, 2,071 URLs; in 2009, 28,705 URLs; and from January to November 2010, 43,908 URLs. Altogether 74,686 URLs have been blocked.

Information from the Criminal Court, apart from the number of URLs that have been blocked, also gives the reasons for blocking these websites. In order of magnitude, these are: 1) lèse majesté content (62 orders; 57,330 URLs); 2) pornographic content (43 orders; 16,740 URLs); 3) content related to medicine and guidelines for self-induced abortion (four orders; 357 URLs); 4) content related to gambling (two orders; 246 URLs); 5) content insulting religion (three orders; five URLs). Other reasons range from phishing/pharming (three URLs) and websites masquerading as bank websites to lure victims to reveal their account and password information for internet banking (two URLs), but the figures are relatively low. One order blocking three URLs claims that these URLs contain information that could make the government misunderstood among the Thai public on the issue of demonstration control and create chaos and division among the Thai public. The names of the websites that have been blocked, especially those that have lèse majesté content, are kept secret and are inaccessible to the public.

Apart from court orders to stop the

Content	2007		2008		2009		2010*		Total	
	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL
Lèse majesté content	0	0	7	1,937	30	16,525	25	38,868	**62**	**57,330**
Obscene or pornographic	0	0	4	96	27	11,609	12	5,035	**43**	**16,740**
Abortion pills	0	0	1	37	3	320	0	0	**4**	**357**
Gambling	0	0	0	0	2	246	0	0	**2**	**246**
Depreciation of religion	1	2	1	1	1	2	0	0	**3**	**5**
Others	0	0	0	0	1	3	2	5	**3**	**8**
Total	**1**	2	13	2,071	64	28,705	39	43,908	**117**	**74,686**

*Statistics in 2010 collected from January to November.

The statistics of suppression on the dissemination of computer data by court orders from 2007-2010

Timing	Lèse Maiesté content		Obscene or pornographic		Abortion pills		Gambling		Depreciation of religion		Others		**Total**	
	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL	**Court order**	**URL**
Oct 07									1	2			1	2
Jan 08									1	1			1	1
Feb 08			1	7									1	7
May 08			1	1									1	1
June 08	1	9	1	2									2	11
July 08													0	0
Aug 08	2	407											2	407
Sep 08	1	630	1	86									2	716
Oct 08	1	491											1	491
Nov 08													0	0
Dec 08	2	400			1	37							3	437
Jan 09	3	808											3	808
Feb 09	4	1,400	1	305	1	14							6	1,719
Mar 09	4	765	3	825					1	2			8	1,592
Apr 09	2	887	4	936									6	1,823
May 09	3	713	4	2,213			1	72					8	2,998
June 09	3	770	3	1,948									6	2,718
July 09	2	469	3	875									5	1,344
Aug 09	1	843	1	132							1	3	3	978
Sep 09	2	1,985	2	879	1	61	1	174					6	3,099
Oct 09	3	3,737	3	1,430									6	5,167
Nov 09	2	3,007	1	741									3	3,748
Dec 09	1	1,141	2	1,325	1	245							4	2,711
Jan 10	2	4,119											2	4,119
Feb 10	4	6,731	2	1,127							1	3	7	7,861
Mar 10	6	9,672	1	373									7	10,045
Apr 10	2	2,277	1	21									3	2,298
May 10													0	0
June 10	3	4,513											3	4,513
July 10													0	0
Aug 10	5	9,289	3	1,322							1	2	9	10,613
Sep 10	3	2,267	2	944									5	3,211
Oct 10			2	998									2	998
Nov 10			1	250									1	250
Total	62	57,330	40	16,740	4	357	2	246	3	5	3	8	114	74,686

Number of court orders and URLs that were blocked each month

dissemination of information under the CCA, the researchers also found that state officials also block websites using other methods, such as sending official letters requesting cooperation to internet service providers at different levels. Importantly, the Emergency Decree which has been imposed in many provinces from April 2010 until today, is also used to block websites. A reliable source from among internet service providers notes that the number of websites that have been blocked by order of the Centre for the Resolution of the Emergency Situation (CRES) has run into tens of thousands. The process of blocking websites by the CRES is also different from the procedures used by the MICT. The CCA limits the power of the MICT to block websites only when they are problematic and subject to a court order. However, the CRES can order an immediate blocking of websites under the Emergency Decree without any order from the courts. Preliminary information accessed by the researchers (but not presented in this report) reveals that although the government led by Abhisit Vejjajiva has used the power of the Emergency Decree for only eight months, the CRES has ordered the blocking of a huge number of websites (both reported and unreported). There are reasons to believe that the blocking is being done like casting a net, because from at least three orders of the CRES citing Section 9 (3) of the Emergency Decree to block websites/URLs/IPs/phone numbers, there is a list of at least 600 items that are blocked. The blocking is not only done by specifying a website by name or a URL but there are numerous cases where the CRES has ordered blocking by citing a range of numbers of IP addresses (e.g. XXX.XXX.XXX.0 to XXX.XXX.XXX.255). This is merely because within that set of numbers there are websites that the CRES sees as falling within the Emergency Decree. The fact is that blocking in this way will affect a large number of websites that could be general websites that have done nothing wrong or are no danger under the Emergency Decree, but which merely happen to be within the range of IP numbers that the CRES wants to block. Ultimately, no one can really determine what kind of content is in websites that the CRES has ordered to be blocked (since the CRES has never specifically explained or given reasons for how its power is used). But from considering the sketchy data and the number blocked by the MICT, no one can deny that the Thai people's right to freedom of expression and opinion in the online world is in crisis.

Additional observations on blocking access to information

1) From the statistics of websites being blocked by court orders, a fact emerges that the courts take an extremely short period of time (within a day) to look at the URLs before granting an order to block access to this information. From 117 orders that the researchers could access, 104 received authorisation from the court on the very same day that the MICT made the request. 71,765 URLs have been blocked by the MICT, which means that on average 690 URLs are blocked each day. In a number

of cases the court took two days. There are very few cases where the court took more than one week to review the URLs before granting the order. In terms of the URL blocking procedure, after the court issues an order, a copy is sent to internet service providers to block access to those URLs.

2) The number of blocked websites, especially those with content under Section 112, has increased many times. In March and August 2010, more than 9,600 URLs were blocked. Those months coincided with Red Shirt protests for their political rights. Apart from the increase in the number of websites blocked, we also see an increasing number of lèse majesté cases filed. For example, an internet user under the name of "K Thong Bomb Bangkok" was arrested in February 2010 and charged under Section 14 of the CCA and Sections 116 and 392 of the Criminal Code.[11] In April 2010, the webmaster of NorPorChor USA was arrested and charged under Sections 14 and 15 of the CCA and Section 112 of the Criminal Code. This case is similar to the case of Mr. Chupong Teetuan, who was charged under Section 14 of the CCA and Section 112 of the Criminal Code.

Part 2

Laws and state policies that affect the right to freedom of expression and opinion in online media: Thailand in comparison with the United States, Germany, China, and Malaysia

This part focuses on the law, case studies, and state policies related to the rights and freedoms of citizens in online media. It is, however, only a preliminary report. All information, including the analysis comparing the situation in Thailand with that of other countries will be presented by the researchers in a more complete report in the future. The researchers have looked at the laws and state policies in the following four countries to compare with the Thai case:

1. United States of America

The expression of a wide range of opinion, especially political opinion, is protected within the U.S. Constitution. The main principle is that the free market of ideas and information is a very important matter which ensures that the political sector, which has to duty to serve the public and benefit society, is transparent and conforms to democratic principles of governance. However, such freedom also

[11] In this case, the suspect stated through Camfrog "as I said, the signal for the bomb will sound. You do not have to ask who is behind it because you do not have the right to know who is behind it. Let's just say from tomorrow onward we will hear the bombs at your gate. Let's just say it. Civil war will be declared from tomorrow onward".

have limitations. There are two kinds of laws and state policies that affect access to and expression of opinion online: the first kind protects children and youth from media with pornographic content; the second concerns national security and counter-terrorism. There are several methods used in the U.S. ranging from internet filtering, blocking of websites, and internet surveillance.

Protecting children and youth from media with pornographic content: The U.S. has two principles regarding this issue which are the prohibition of the dissemination of child pornography and prohibiting children and youth under 18 years old from accessing pornographic materials. These measures are specified in the Communication Decency Act of 1996 (CDA) which has clear regulations that service providers will have no liability under civil law when they block content that are seen as indecent, inappropriate, or offensive. Service providers, however, are responsible to operate according to government orders to block child or youth pornography. The Child Online Protection Act also states that schools and libraries must install computer programmes to filter inappropriate internet content.

Cases concerning national security and surveillance by security agencies: For security reasons the U.S. government has electronic surveillance laws that greatly violate the rights and liberties of internet users. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercepted and Obstruct Terrorism Act of 2001, commonly known as the Patriot Act, grants state agencies the power to use technology to monitor email systems and access online information on potential terrorist suspects. The U.S. National Security Agency also uses "Carnivore", an internet spy mechanism to enable the Federal Bureau of Investigation (FBI) to investigate information on various websites suspected of involvement in terrorism offences. This mechanism also allows FBI officials to analyse prodigious numbers of email systems belonging to suspects and ordinary people in the same manner. Using this special power, FBI agents have arrested an unprecedented large number of suspects. The FBI has also been able to block web pages of major internet providers such as Google, Yahoo, AOL, and Microsoft through the use of geolocation filtering systems.

The role of internet service providers in the U.S.: Presently, the Stored Communications Act gives state officials the power to summon information relating to online use of a computer. Therefore, the account name and details on internet users, internet channels, and internet addresses are documented. This information must be presented to officials when requested. The Communications Assistance for Law Enforcement Act of 1994 developed interception technologies by requiring internet providers to create surveillance systems to monitor information on internet users to enable officials to investigate and gather evidence quickly and efficiently.

2. Federal Republic of Germany:

Germany is known to be one of the countries in Europe that respect the right

to freedom of expression and give great importance to the privacy of their citizens. There have been few cases of censorship of information and news in the country, but there are certain issues on which the state prohibits its citizens from expressing their opinions freely. Section 5 of the German Constitution (Grunsgesetz) protects the rights to speak, write, draw, and otherwise express and to disseminate opinions in all forms of media, free from state obstruction, monitoring or interference. The same section also regulates the protection of the freedom to receive information as a freedom which is as important as the freedom of opinion (Meinungsfreiheit) and the freedom of the press (Pressefreiheit). Freedom of information is regarded as an important structure in creating public opinion in a democratic system. So in principle, the state cannot impede or halt the dissemination of content in any form of media. Information cannot be blocked before it is disseminated (Vorzensur) or after (Nachzensur). However, paragraph two of this section stipulates that this freedom can be limited under the law of the state.

Content of which dissemination is prohibited by law: In Germany, the state can use measures to block access to content that violates the law by using the power that is given in specific laws. These laws have the important justification of "protecting children and youth" from content containing sex and violence that would be detrimental to their mental development. There are also laws to protect the reputation and honour of individuals and to uphold public peace. Prohibited content can be segregated by offence according to different laws.

Indecent and obscene images: German Criminal Law (Strafgesetzbuch - StGB), the State Treaty on the Protection of Minors from the Mass Media (Jugendmedienschutz-Staatsvertrag - JMStV), and the Protection of Young Persons Act (Jugendschutzgesetz - JuSchG) all prohibit anyone from disseminating or allowing channels for children and youth[12] to access all forms of media with pornographic content. Violators will be prosecuted according to the law. Disseminating or providing the general public with access to indecent images containing violence, bestiality or the sexual abuse of children and youth, known as "Harte Pornografie" (hard pornography), whether online or through other media, is an offence under criminal law. It can be seen that the priority is to prohibit the dissemination of such images to protect children and youth, so that: 1) they do not have to confront such content before an appropriate age; and 2) they are protected from becoming victims of adult producers of child pornography. For these reasons and because of the problem of extraterritorial enforcement of German law and international cooperation in finding witnesses and bringing suspects to trial, the German authorities in the past two or three years have attempted to press internet access providers to take responsibility for surveillance and blocking access to child and youth pornography, in addition to prosecuting wrongdoers.

Violent left/right wing groups: JMStV and the Commission for the Protection of Minors in the Media (Kommission für Jugendmedienschutz – KJM) try to protect children and youth from political thoughts

coming from violent right-wing or left-wing groups (Rechts[13]-und Linksextremismus) and German national socialism (Nationalsozialismus). The dissemination of such ideologies in various media, including the internet, may be an offence under criminal laws, such as creating propaganda (Propaganda - § 86 StGB), using the symbols of unconstitutional organisations (§ 86a StGB), creating divisions among the public (Volksverhetzung - § 130 StGB) and also incitement to violence, destruction of human dignity, and the use of offensive content and language based upon belief, race, and religion to slander a specific group of individuals. Germany also prohibits the spread of information that urges the public to break the law (§ 111 StGB) and all kind of threatening behaviour (such as publicising threats in public) to disrupt public peace.

Glorification of violence or violations of human dignity: Expressing violence and cruelty against fellow human beings or destroying human dignity (Gewaltdarstellungen) is an offence under German law (§ 131 StGB). If a youth under 18 years old is able to access this information, the punishment is increased. Concrete examples include tasteless websites such as www.rotten.com hich publicises photographs of the victims of crimes, those injured in accidents, patients in the final stages of illness, and photographs of prisoners being tortured in Abu Ghraib prison. Although rotten.com has expressed the view that it presents pictures that are "inappropriate but lawful", but the content still violates the State Treaty on the Protection of Minors from the Mass Media (JMStV) and can be interpreted as a violation of human dignity (Menschenwürdeverstoße).

Apart from the main issues already discussed, the dissemination of defamatory material, organised gambling without state authorisation, and illegal gambling (§ 284 ff. StGB) are forbidden. Violators are punished according to the law. However, although much information is prohibited under German law, the researchers need to take note that most is legally defined in a clear and unambiguous manner. The purpose of these laws is to protect children and other groups of citizens in the country. It is not done to defend abstract concepts such as nation, security, good morals, or allegiance to an individual, where the limits are difficult to define and which do not conform to democratic principles of governance. Restrictions on the dissemination of content follow Article 130 of the German Criminal Code. In particular the appropriateness of the ban on the expression of a belief in Nazism, also known as Auschwitz-Lüge (holocaust denial), is questioned and debated

[12] According to German law, a "child" is an individual younger than 14 years old (§ 184b StGB). A "youth" is an individual aged between 14 but not exceeding 18 years old. (§ 184c StGB)

[13] This comes from the report "Vom Rand zur Mitte" by Friedrich Ebert Stiftung published in 2006. The report tries to identify the ideological components of the violent right wing which may be found in groups with the following ideas: 1) support for right wing authoritarianism; 2) chauvinism (Chauvinismus) 3. ideologies of hatred, discrimination and xenophobia (Ausländerfeindlichkeit) 4. anti-Semitism or Judeophobia and Social Darwinism (Sozialdarwinismus), including propaganda to make the public believe that Nazism is a harmless and reasonable ideology (Decker, O. / Brhler, Vom Rand zur Mitte (2006), http://www.fes.de/rechtsextremismus/pdf/Vom__Rand__zur__Mitte.pdf, S. 20).

in academic circles since under this offence anyone who merely expresses support for Nazism or expresses the belief that the genocide of the Jews in the concentration camps did not take place faces criminal penalties. However, Germany insists that this is an offence because the expression of such opinions is telling lies and dishonouring the Jewish dead.

Measures used to block access to websites: The German Interstate Media Services Agreement (MediendiensteStaats-vertrag: MDStV) has sections on "prohibited media" and "operational measures for such media". Each state can order internet providers to block access to websites with unlawful content . An important and interesting example of this is the case where the Lord Mayor of Düsseldorf in North Rhine-Westphalia used his authority under MDStV to order internet providers to block public access to four websites namely rotten.com, front14.org, nazi-lauck-nsdapao.com and stormfront.org. The reason was that these websites have violent extremist right-wing content, violate human dignity, support war, are harmful to children and youth, and encroach on the rights and liberties of the people. After these websites were blocked, a large number of German citizens came out to protest against the action. Petitions and academic seminars were held, including a complaint to the Administrative Court in 2001. However the Supreme Administrative Court in Münster upheld the order of the governor, ruling that his action was lawful. This case shows that even in Germany access to the media was blocked, but it was not done repeatedly. The state can also pinpoint the offences under the law in websites. The affected persons are also protected and can file a complaint to the court to investigate the use of power by the state. In the past, apart from the blocking of websites in Düsseldorf, there were two other cases when Germany blocked a large number of websites. The first was in 1996 when extremist left wing websites were shut down and the second in 2006 to block illegal gambling websites during the World Cup of that year.

Duty and responsibility of internet providers: The important law on this is the Telecommunication Law (Teledienstgesetz - TDG) which specifies the duties and responsibilities of internet providers by separating them into clear types. An important case which raised many concerns was that of CompuServe where the court of first instance in Munich in 1998 sentenced the manager of a CompuServe web board to a suspended two year jail sentence for failing to block dissemination of child pornography images posted on a server in the United States. The court reasoned that CompuServe Germany knew of the pornographic images and was not only the sole internet provider connected to the website, but also the content provider. Munich Appeal Court finally overturned the original ruling on the grounds that CompuServe Germany was only the internet provider and was not in a position to know the content. The legislature in this case found a problem in the vagueness of the legal language in the TDG and MDStV since both have the same legal provisions.

The problem of legal interpretation led to additional changes with regard to the responsibility of internet providers. The interesting point on the responsibility of internet providers in telecommunications was the complaint filed jointly by more than 30,000 Germans with the Constitution Court of the Federal Republic of Germany at the end of 2007 asking the court to rule on the constitutionality of the obligation of internet providers to document traffic for at least six months with the aim of using the data in the investigation of acts of terrorism and other serious offences (Vorratsdatens-peicherung) which had been added into the Telecommunication Law. In March 2010, the Constitutional Court ruled that the obligation was unconstitutional in that it violated the constitutional principle protecting personal rights and liberties to communicate.

3. People's Republic of China

While Section 35 of the Chinese Constitution (1982) guarantees the freedom of expression of the people, in reality China has promulgated many subsidiary and special laws to set regulations and limitations on various rights and has policies that obstruct citizens from expressing opinions online and accessing news and information. The state's argument is to protect the security of the Chinese government and the Communist Party of China. Ultimately, it could be said that the Chinese people are virtually unable to express their opinions or criticise the administration of the country by the Chinese government. The intensive and varied measures to control freedom of expression can be categorised as follows.

Policies and special laws to suppress internet users: China requires writers and content providers on websites to examine the content and abstain from disseminating inappropriate information (self-filtering) on the basis that news and information on the internet should not contain content that endangers the dignity and interests of the state. Rumours and any actions that could contribute to social instability cannot be disseminated. A large number of Chinese laws state that before the content is posted on the internet, the person posting the content must be authorised by the government. Therefore, all news services, such as the creation of web boards, news broadcasts and voice broadcasts via the internet need authorisation from government agencies. The legal actions taken against people who criticise the government show that most critics face defamation charges. If they publicise information that the government does not want the public to know, they are charged with inciting misunderstanding, slandering the state, and aiming to overthrow the government. If the Chinese government sees the defamation as threatening state security, the government might proceed with charges without having to go through a complaint procedure. Since 1999, 76 internet users have been sentenced to jail terms.

Laws relating to the restriction of the freedom of expression and opinion: Apart from specific laws on online media, the Chinese government also has other laws to control opinion making in the general media such as the State Security Law (1993), which has a broad and vague meaning, prohibiting

organisations or individuals to harm the security of the government. The criminal law on National Security and State Secrets prohibits the dissemination of information on and secrets of the Chinese government. Apart from the laws that allow the government to use extensive powers, the judiciary in China does not genuinely protect the rights and freedoms of the people. There are no clear standards to differentiate between the right to freedom of opinion and what is perceived as a threat to national security.

Technological development and the creation of an agency to investigate online media: China has invested in the development of software so-called the Great Firewall of China, which aims to systematically block websites that criticise the Chinese government. China also has internet system management centres in three important cities: Beijing, Shanghai, and Guangzhou. Internet monitoring and surveillance units also operate in key cities in the country. With this system, the government can perfectly manage computer traffic and block access to information. The Chinese government also set up Bureau Five and Bureau Nine, agencies under the Office of Information, which are tasked with creating positive propaganda on the government to persuade citizens to support government policies and create a motivation for internet users and websites to cooperate in helping to monitor internet content. China has also invested budget to create tens of thousands of web boards as forums for presenting news favourable to the government.

Online media control through internet providers: The Chinese government systematically violates the right to freedom of expression by monopolising telecommunications through concessions and licensing internet providers. Currently, the Chinese government has given concessions to four main internet providers: CSTNet, ChinaNet, CERNet and CHINAGBN. These four companies franchised the concessions to 3,000 smaller internet provider companies. Through this monopoly policy, the government can fully regulate policies and practices to filter and block content. Computer shops in China are obliged to pre-install a programme called Green Dam Youth Escort as censorship software so that the government can monitor the behaviour of computer users all the time. Internet providers also have the duty to delete immoral content (such as pornography) and filter content that is critical of the Chinese government. China also requires its citizens to declare their real names and addresses when they want to post comments or messages on websites. Owners of internet cafés must abide by the Regulation on the Administration of Internet Access Service Business Establishments (Internet Cafés), which requires them to record and retain information about users and the content that is accessed by internet users for at least 60 days. This allows the Cultural and Public Security Agency to investigate any unlawful acts by internet users.

4. Malaysia

Malaysia is one of the countries in Southeast Asia, apart from Burma, Indonesia,

and Thailand with a long history of media surveillance and control by state officials. Malaysian media, especially newspapers and independent media, have been a target of the police and numerous laws that have been interpreted vaguely if information is presented that opposes the government. Many internet users have been detained and imprisoned merely for comments criticising the government. This has the effect of restricting the space for the right to freedom of expression At the same time, the rights and liberties to report news are under surveillance.

Freedom of expression as stipulated in the constitution: As with all other countries, the constitution of Malaysia guarantees not only the right to privacy, but also a number of other rights. The right to the freedom to speak and express oneself is guaranteed in Section 10 (1) (a) of the constitution. However, it is stated in the same section that these rights and liberties can be restricted as needed or appropriate to: 1) protect the interests and national security of the federation; 2) maintain diplomatic relations with other countries; 3) uphold public order and morals; and 4) protect the rights of parliament or the legislature, or the reputation of the court, and prevent defamation against the reputation of a third person, or incitement to unlawful acts. From this it can be seen that this Section of the Malaysian Constitution is no different from Section 45 of the Thai Constitution since even though the Malaysian Constitution guarantees the right to freedom of expression, parliament can issue laws to limit freedom of expression and opinion for various reasons. These rights can be limited for other reasons, such as during a state of emergency. Under a state of emergency, the executive will be given the power to pass laws that contravene the Constitution. After the riots in Malaysia in May 1969, the legislature changed the constitution to empower the state to order the people not to speak or converse on issues related to citizenship, national language, special rights, and sovereignty.

Intimidation in the cyber world: New media such as news websites (such as NutGraph, Malaysia Insider, and Malaysiakini) and blogs (such as Articulations, Zorro unmasked, People's Parliament, and Malaysia Today) have grown extensively in the past few years due to their popularity and their reputation for reliability when compared to the mainstream media (such as newspapers, radio, and websites). Access to these websites and blogs in Malaysia has been blocked by the government. Website owners, bloggers, and many online journalists have been harassed by the government. Malaysia is the first country in Southeast Asia to have a Computer Crime Act, but this does not have specific clauses that empower the government to investigate content or specifically block access to information on the internet. In the past, the Malaysian state often used other laws which granted the power to limit access to the media and interpreted those laws to include online media. The major laws that have been used to control the media at different levels include the Official Secrets Act, which makes the dissemination of official secrets a crime;

the Printing Presses and Publications Act 1984, which states that the decision of the Minister of Foreign Affairs is final in issuing and revoking publication licences; the Communications and Multimedia Act of 1998 (CMA) and Communications and Multimedia Commission Act of 1998 (CMCA), which are both used to control telecommunication technology, news broadcasts in Malaysia, internet systems, and other facilities relating to news and information services; the Internal Security Act[14], which is used by the Malaysian government as a tool to shut down the media and arrest and detain media practitioners); and the Sedition Act 1948, (drafted in 1948[15] when Malaysia was still a British colony), which has articles prohibiting the publication of media that is likely to create unrest. Violation is a criminal offence for which there is no legal excuse. All newspapers and magazines must receive authorisation from the government under this Act before publication. The Act forbids making opinion on range of sensitive subjects. In order to control online media, the Malaysian government set up a special agency called the Malaysia Communications and Multimedia Commission (MCMC), which is directly tasked to monitor online content.

5. Kingdom of Thailand, media laws, and the right to freedom of expression

Thailand has a number of laws relating to "mass media" which grant the state the power to block the access to the media even at a time when Thailand is not in a state of emergency. The first law enacted to control the media was Section 9 of the Press Act of 1941. Later in 1987, the Magnetic Tape and Television Equipment Act was enacted to control the process, format, and content of public media. Section 30 empowers the state to ban taping and television equipment in public. However, the new Film and Video Act of 2008 superseded this Act and the Film Act of 1931 (Section 4 of which empowered state officials to prohibit the showing and viewing of films contrary to national peace). However, the new law also provides powers to the Motion Picture and Film Committee to decide whether to authorise or ban the showing of motion pictures and films in the Kingdom.

Another law related to mass media

[14] This law was drafted after Malaysia received independence from the UK in 1957 when Malaysia was facing a communist threat. The ISA has been available since 1960 for the government to prevent untoward events and to counter the threat from the Communist Party of Malaya. In 1998, the police arrested four persons under the ISA, alleging that they were linked to the spreading of rumours in Kuala Lumpur. General of Police Tan Sri Abdul Rahim Noorsaid said that the suspects were arrested after the police had monitored their activities through the help of an internet service provider. In January 2001, the website of parliament was hacked. There were reports that the government might extend use of the ISA to include hackers that infiltrate government websites.

[15] Human rights organisations state that the Sedition Act has a very obscure and vague meaning. Their criticisms are that this obscurity is an "invitation for wrongdoing and the state agencies might find a way to use it as a political tool in other cases unrelated to the objective of the law". Lord Bach, Parliamentary Under-Secretary of State for Justice in the UK, once said that the Sedition Act is an obsolete law and should be revoked. However, Datuk Hussein Seri Hishammuddin, the Malaysian Minister of Science, Technology, and Innovation and Minister of Home Affairs said that there was no necessity to revoke the Act.

and the rights and liberties of the people is the Broadcast and Television Act of 1955 which gives the state the power to seize and prohibit the use of radio or television receivers for the purpose of maintaining public order and defending the Kingdom. This law was also superseded by the enactment of Film and Video Act of 2008. While this new act has improved modern content and tries to reduce the monopolistic characteristics of the broadcast media, several sections still empower the state to control media content or give an opportunity for the state to intervene (Section 35 and 37). The Computer Crime Act of 2007 is the latest law relating to mass media that is being used to control new media such as the internet and also to give the state the power to block access to internet data. However, if the Prime Minister decides to impose the Emergency Decree or other emergency laws in any part of the country, state officials can use these laws to limit rights and freedom in many ways that will affect the people. At least two other laws give the Thai state the power to block the dissemination of news and information. These are the Martial Law of 1914 and the Emergency Decree on Public Administration in Emergency Situations of 2005. These laws can be used against all sorts of media. The Criminal Code also has a number of sections that deal with the right to freedom of expression specifying legal responsibility for the dissemination of news and information. This includes Section 287 (on pornography), Sections 326 and 328 (on defamation of a third party), and especially Section 112 (on lèse majesté). In the past two or three years, Section 112 of the Criminal Code has been used together with the Computer Crime Act to prosecute internet users and block a large number of websites in a way that Thailand has never before witnessed. Information on this has already been presented in Part 1 of this report.