Towards Personal Data Protection: A Proposed Model for the Development of 'Right to Know' in Thailand

Nakorn Serirak*

Personal data protection in Thailand under the present law and bureaucratic system was found inadequate. New law enactment has been found crucial as an efficient mechanism to protect people from intrusion into rights of privacy, of which is the matter of trespass of human dignity. Law enforcement, however, could not be effectively performed as long as society still lacks of knowledge, understanding, and consciousness of informational privacy protection. Building of public awareness is, thus, essential.

Background

Thailand, during the last decade, has witnessed a swift and continuous chain of changes in terms of economics, politics and society. The political arena itself has provided more opportunities for public participation while people have become more aware of their rights in society and seek greater involvement in politics.

In this connection, the people's Right to Know as well as Informational Privacy Right has been awaked by the Thai Information Law, Official Information Act, B.E. 2540 (1997)(OIA)[1].

The Thai Information Law guarantees the Freedom of Information and declares people's rights to have access to state

* This paper is a part of writer's PhD Dissertation in Integrated Science of Thammasat University. The research was funded by the Thai Research Fund and Deutscher Akademischer Austausch Dienst (DAAD).

[1] Official Information Act, B.E. 2540 (1997), has been announced a month before the 1997 Constitution was declared. The law has got non-significant impact from the abolishment of the Constitution by military coup de'tat on September 19, 2006.

information. This is indeed the reflection of participatory political development as the people now absolutely enjoy their freedom in expressing opinion. The utilization of people's right to access official information meets with the good operational services of providing access and is therefore a process towards transparency and accountability, key elements of the Good Governance. The Act also performs the context of Privacy Protection in the chapter of personal data.

1. Information Access and Privacy Protection under Information Law

1.1 Emerging of the Official Information Act

In the past, Freedom of Information in Thailand has been very limited. Governmental agencies have been largely practicing information closure and have been accustomed of performing as the information owner while the people are determined as those who have to make a plea to get their desired data while the owners, in most cases, tend to deny such requests.

The situation has been greatly changed after the Information Law has been effectuated. Followed by the 1997 Constitution (Government Gazette, 1997) which also affirms the people's Right to Know, the new reversed principle of *what the state knows or does, the people must have the right to know*. (Nakorn Serirak, 1999, p.15)

It has been almost 10 years since OIA was passed. (Government Gazette, 1997) The Act, however, has become increasingly popular and has been widely accepted as a new but useful tool for the public. While bringing about many contributions to the political reform agenda of the country, the Information Act also creates a significant challenge to the traditional bureaucratic system. It plays a significant role in changing the attitude of Thai government servants towards the administration of official information.

OIA was first drafted by the so-called *Transparent Govern-*

ment, under Prime Minister Anand Panyarachun, and had to wait until July 1997 for approval by the Parliament. It has been an effect since 9 December 1997. (Government Gazette, 1997(b))

The principle of the Act is the guarantee of the people's rights to have full access to government information. According to the Act, almost all official data and information should be revealed for public perusal, with only some categories of information that the State can still keep confidential constituting small exceptions. Should the state agency deny disclosure of some excepted data, the people still have the right to appeal to the Official Information Commission (OIC) to reconsider each case.

OIA ensures people's rights to know government information, ranging from the rights to inspect, to request a copy, to get advice, to make complaints and appeal, and to ask the state to correct or change personal data. Such rights are bestowed on any individual whether they have any involvement or relationship with the cause and effect of the information they request.

This new principle turned down the traditional practice of state officials whose attitude towards government information was to keep it strictly confidential for official uses only. On the other hand, in response to public demand to access, disclosure is an exception, as most data has been kept internally secret. The Act also performs the context of Privacy Protection in the part of personal data.

1.2 State Agencies Duty on Information Disclosure

According to OIA, state agencies are to execute information disclosure through three mechanisms:

1. Publish in the Government Gazette of the following official information i.e. structure and organization of its operation, summary of important powers and duties and operational methods, contacting addresses, by-laws, resolutions, regulations, orders, circulars, rules, etc. (OIA, section 7)

2. Make available at least the following official information

for public inspection i.e. a result of consideration, a decision, policy, work-plan, project, annual expenditure, manual or order relating to work procedure, concession contract, agreement, resolution of the cabinet or of committee established by law, etc. (OIA, section 9)

3. Provide information to individual request, OIA states that when any person makes a request for any official information, other than those already published in the Government Gazette, or already made available for public inspection, state agency shall provide within a reasonable period of time. (OIA, section 11)

Therefore, we can see that most of the official information is subject to disclosure while only few are declared as an exemption. According to OIA, some information, which is not subject to disclosure, are those that the disclosure may jeopardize the Royal Institution; (OIA, section 14) or the disclosure will jeopardize the national security, international relations, national economic or financial security; or will result in the decline in the efficiency of law enforcement, or will endanger the life or safety of any person; medical report or personal data the disclosure of which will unreasonably encroach upon the right of privacy.(OIA, section 15)

1.3 Personal Data Protection

One of the most important goals of the act is privacy protection stated in the Personal Information chapter. Informational privacy has been recognized as the act allows state agencies to collect, process, and use personal data of the people only when it deems necessary for its authoritative operation. Meanwhile they are obliged to provide appropriate security system for such personal data. Termination of the system will be finalized when its operation has been accomplished or when the system is no more necessary (OIA, section 23(1)).

State agencies are not normally allowed to trace and store personal data of citizens, but are obliged to, in advance, inform the data subject about the collection of such personal data. A personal

information system to be established has to be publicly informed by announcement in the government gazette. (Section 23(3))

Regarding the provision of a personal information system, Section 23 states the duties of state agencies and confirms that people's personal data has to be kept safely and state agencies has to take good care of preventing any dissemination or disclosure of personal data to other state agencies or any private individuals without consent of the data owner. Disclosure without consent is only possible in some exceptions such as to perform legal duties of the state, to serve research or academic usage, to prevent the violation of the law, to protect persons or their health, or any specific reasons justified by law. (OIA, section 24).

As far as personal data is concerned, state agencies have to make the personal information system open. It must be possible for individuals to access their own data file and to review its content (OIA, section 25).

2. Exercising the Official Information Act

2.1 Implementation of the Act

Evidence has never been explored neither how an active public exerts their Right to Know, nor how well bureaucrats respond. If the state offices responsively agree to reveal information to the individuals interested, the game is over at the agency level. Poor and non-systematic data management system, varies among each office, making it difficult to count for such scores. The best way to understand how effective the citizens exercise the Right to Know is to look at the problematic stories, when those who suffered any prejudice to his or her rights from the state then sued and appealed to the Commissioner. The available figures of confrontation in the first two years and in 2005 will be elaborated.

Year 1998-1999

In 1999, there were 122 complaints about government disclosure. This compares with only 26 complaints in 1998, the first year of OIA practices. Most of the cases were complaints about poor service by government officials and their lack of willingness to provide information to people requesting it.

The total number of 87 appeal cases compares with only six in 1998. Fifty percent of the appeal cases concern disciplinary investigation documents. Others were requests concerning information about current affairs such as the results of the investigation into corruption at the Ministry of Public Health and the asset sales by the Financial Sector Restructuring Authority (FRA), and those related to concession, contract and meeting reports

Of the overall 209 cases of public and non-public sector complaints and appeals, 175 cases happened in Bangkok while 34 happened in 75 provinces nation-wide. (Nakorn Serirak, 2000)

Year 2005

There were 478 complaints and appeals submitted to OIC in 2005. Among the total of 314 complaints, 140 cases (44.59%) were filed against central administration agencies, 115 cases (36.62%) against local government agencies, 32 cases (10.19%) independent organizations, 18 cases(5.73%)agencies under regional administration.

Considering complaints against central government agencies, 50 cases (35.71%) belonged to the Ministry of Education, 15 cases (10.71%) the Ministry of Public Health, 14 cases(10.00%) the Ministry of Finance, 12 cases (8.57%) agencies under the Prime Minister's Office.

For the total of 164 appeals, 106 cases (64.63%) were filed against agencies under central administration, 31 cases (18.90%) local administration agencies, 16 cases (9.76%) independent agencies.

Among the appeals submitted to ministerial or departmental agencies, 31 cases (29.25%) belonged to the Ministry of Education,

20 cases (18.87%) the Ministry of Labor and Social Welfare, and 13 cases (12.26%) the Ministry of Public Health.

Most of the complaints, 99 cases (31.53%), are files involving the checking and inspection of authoritative management of state agencies. 75 cases (23.89%) of the complaints concerned procurement, while 34 cases (10.83%) involved judicial proceeding. 28 cases (8.92%) were personal management documents while 26 cases (8.28%) were information related to disciplinary investigation.

Majority of the appeal, 53 cases (32.32%) are sued by those who got denials to access disciplinary investigation files, 36 cases (21.95%) were related to the checking and inspection of authoritative exercising of state agencies. 20 cases (12.20%) were those who suffered in requesting to look upon government information involving procurements.

The majority of the population who exercised OIA in 2005 was private citizens who made up most of the 125 complaints (39.81%), while 100 government officers (31.85%) and 52 businessmen (16.56%) ranked second and third. Journalists sued 16 complaints (5.10%) while less than 1% of only 3 NGOs, 2 politicians and 2 students utilized OIA.

There were 73 state officers who filed most of appeals (44.51%), while 59 private citizen (35.98%) and 23 businessmen (14.02%) ranked second and third. Only 1 journalist (0.61%) and 1 student (0.61%) were the minority in appealing. (Office of OIC, 2006)

Eight years of exercising the Right to Know

About 8 full years of the Act services, from the 9th December 1997 up to 2005, plaintiffs of grievances in state habits related to the matter of information disclosure marked to 1,373 complaints and 881 appeals.

Of the overall 2,254 cases of complaints and appeals, 1,254 cases (55.63%) belonged to the central administration level of ministerial or departmental agencies, 556 cases are those suffered

by the local government entities (24.67%), 184 cases (8.16%) agencies not attached to ministry. The remaining 129 cases (5.72%) are those belonging to the independent organizations or special function agencies and 122 cases (5.41%) are those against regional administrative bodies or provincial offices. In terms of location, 1,576 cases happened in Bangkok about double those 678 stories that happened in 75 provinces nation-wide.

Most of those who exercised their rights under OIA during the eight implementing years were government officials, while private citizens and businessmen ranked second and third. Journalists moderately enjoyed exercising the Act while NGOs, students, and politicians, were really the minority who utilized the Act.

2.2 Problems in Implementation

After the first few implementation years of OIA, major difficulties exist in government information disclosure practices:

1. Most people neither understand key elements of the Act nor realize their own rights. They do not know how to utilize the law in compliance with their demand to have access to the state information. People cannot exercise their rights, as they do not know the procedures.

2. In government agencies, both high-ranking executive and servicing-level officers, do not understand the law and do not know how to implement the Act. Furthermore, they lack adequate knowledge of the law and the main principles of information disclosure service to achieve people's rights to know. They thus cannot administer the office in accordance with the Act.

3. Bureaucrats are not used to the very new principles of information disclosure as a crucial part of their services. They have negative attitudes towards the Act. Some feel that the Act puts more burdens on them.

4. Information Act is a newly established law, the perceptions and the understanding of freedom of information and personal data

protection has been very limited. Knowledge and understanding of the two concepts, both on the law enforcement side as well as the application mode of acknowledging people, are extremely poor.

To solve the problem and overcome such difficulties, OIC has prepared strategic guidelines for the Act implementation, which have, up to now, become the blueprint for the exercising of the Right to Know promotion and work pattern of the office of OIC, as follows: (Office of OIC, 2000)

1. To promote and develop the acknowledgement of the Act's content, its utilization, the mechanism and the procedures to utilize the Act to meet people's right to access information.

2. To develop the documentary management of all government offices to be more efficient, more systematic, eventually leading to nationwide linkage in compliance with OIA implementation.

3. The monitoring and evaluation should be carried out in all state agencies, by both internal auditors and external inspectors, including academic institutions, university and NGOs.

OIC proposed guidelines to the cabinet in November 1999 (Office of OIC, 1999), and 4 measures were approved to follow up the implementation of OIA by all government agencies (Office of the Cabinet Secretary, 1999).

(1) All state agencies have to report their activities in implementing the Act to the Commission twice a year

(2) The Office of the Permanent Secretary of the Prime Minister's Office will be the main agency in charge of monitoring and evaluation

(3) All ministries and departments must take this evaluation as a significant policy by appointing the inspector general of each minister to be responsible for this mandate

(4) Inspector General of the department of local administration will be responsible for the monitoring and evaluation of local entities.

More recommendations were submitted by OIC and the Cabinet, on February 1,2000, approved the proposal and issued the

guidelines confirming that all state agencies have to speed up the strict enforcement of OIA and the Prime Minister's Office together with all state agencies should consider the development of the information management and documentary administration to be a systematic one with nationwide network in accordance with OIA. (Office of the Cabinet Secretary, 2000)

3. Reflections of Privacy Controversy

3.1 Significant cases

During the early years of Information Law implementation, there were significant cases that led to a lot of public attention. The cases created new practices concerning official information and played important roles in changing conventional values and behavior of the Thai bureaucrats and Thai society. Most importantly, the cases draw the tension between the matter of *freedom of access to information and privacy right protection.*

(1) Score and answer sheet of the primary school's entrance examination.

The case happened in 1998 when the parent of a student, who failed the entrance examination for the Demonstration School of a Public University, petitioned the primary school to disclose the examination result of her daughter and other students. After the school denied her request, the parent then submitted the appeal to OIC to force the school to disclose the requested information. The Information Disclosure Tribunal (IDT) for Social, National Administration, and Law Enforcement Information ruled that the parent had the rights to see the examination result. (Information Disclosure Tribunal for Social, National Administration, and Law Enforcement Information, 1998)

The case is also concerned with the issue of personal data intervention. As the school claimed that the score and answer sheets

were categorized as personal data and could not be revealed to anyone else apart from the owner. The parents of other students filed a lawsuit against IDT's decision to the Civil Court. The IDT's decision in ruling that the score and answer sheets of all students were official information was legally confirmed by the Civil Court, the Appeal Court and the Supreme Court eventually.

This case has given rise to the new principle of examination result disclosure, in particular the examination of public interest. The Ministry of University Affairs then ordered schools to revise the screening procedures of the examination and the process must be transparent and accountable. The case plays a significant role in the Thai education system.

(2) Corruption Investigative Report

Journalists and non-government organizations (NGOs) petitioned the Office of the Counter Corruption Commission (CCC) to disclose the investigative result report of the corruption in the Ministry of Public Health. CCC denied disclosing the requested documents; petitioners then submitted the appeal to OIC.

IDT for Social, National Administration, and Law Enforcement Information ruled that the investigation was finalized. Those involved officials were disciplinarily punished and politicians were forwarded to criminal investigation. IDT considered that the investigative report is official information, and the case has great impact on public interest and the disclosure could bring about a positive attitude to the national administration, in particular to CCC itself. IDT thus decided that CCC disclosed the requested information. (Information Disclosure Tribunal for Social, National Administration, and Law Enforcement Information, 1999)

(3) Business Contract

Journalists requested to the Financial Sector Restructuring Authority (FRA) to release the Purchasing Contract related to the Bid for sales of the Financial Sector Debts. FRA refused to release

such requested information claiming that the documents were business contracts between FRA and a private company and such a commercial deal cannot be disclosed. After considering this appeals case, IDT for Economic Information ruled that FRA had to release the contract with exceptional conditions for Initial Purchase Price and Sharing Agreement to be released after the bid date. Those documents contain personal information, such as amount and personal debts, should be protected as personal data and cannot be disclosed. (Information Disclosure Tribunal for Economic Information, 1999)

(4) Professorship Evaluation Report

Another case took place when an evaluation for academic position at a State university ended with a negative result. The evaluated candidate then requested the Ministry of University Affairs to release the concerned documents, including the name and position of the evaluators. The Ministry refused to deliver those requested file claiming that the disclosure would violate privacy of the evaluator and would affect the process of academic evaluation. The evaluated person then lodged an appeal to the Disclosure Tribunal.

The Tribunal considered the matter and ruled that the decision of the promotion for professorship essentially effects the academic career of the evaluated person and he should be entitled to defend his rights. IDT decided for disclosure of requested documents explaining that revealing of name and position of evaluators is not the violation of privacy, as the evaluation is not a personal affair but a duty authorized by law. (Information Disclosure Tribunal for Social, National Administration, and Law Enforcement Information, 2000)

3.2 Tension between Freedom of Information and Privacy Protection.

OIA is a new law, knowledge and understanding in the Freedom of Information, and Privacy Protection issue, in particular, is totally new. During the early years of the Act implementation, there were some implications of misunderstanding of and between the matter of freedom of access to information and privacy protection, since these two issues are closely related. On the academic perception, many scholars propose the two issues to be separately considered while some claim close interrelationship as two sides of the same coin.

The legal basis of Freedom of Information is the guarantee of the people's rights to have full access to information, the so-called Right to Know.

Utilization of people's right to know is the main foundation of political development as it brings about public participation. It also plays a significant role in checking the operational performance of state as the practices reflect the philosophy of what the state does, the people have the right to know. Execution of the Right to Know is the main process towards establishing accountable and transparent government, key elements of Good Governance.

Kittisak Prokati (1998, pp. 18 - 19) explains that recently most of International Organization in donor countries are concerned more about the degree of transparency the state of recipients held. He also claims one agency who defines 7 steps of political development as follow:

1. Monopolization of state power and ordering of public administration.
2. Maintaining of public order and state independency
3. Securing of individual rights
4. Protection of collective fundamental rights
5. Guarantee of Freedom of Information and Freedom of Expression

6. Guarantee participation

7. Commitment of state on the Rule of Law.

From above, Prokati declares Freedom of information as a key factor for political development in terms of participatory democracy. (Kittisak Prokati, 1998, p. 19)

On the other side of the coin, Privacy Rights means rights to live one's personal life without any intervention from others. Boundary or domain of private sphere depends on legal basis, tradition and culture of society, and social norms and values. Degree of privacy varies both socially and individually.

Privacy has been defined as a part of personal rights. (Ellen Alderson and Caroline Kennedy, 1995, p. XIV) Traditionally, privacy means the rights to stay or to live personally, to live freely in nature of non-association with others, or alienation from any social interaction. Privacy sphere means a certain area owned by individuals without any involvement, intrusion, or intervention from any others. (Raymond Wacks, 1989, p. 7)

Theoretically, Alan Westin explained boundary of privacy as the matter of solitude, secrecy and autonomy. (David Flaherty, 1984, p. 14) The most understandable explanation of privacy, widely accepted in privacy community, was first made by Samuel Warren and Louis Brandeis who defined privacy as the right to be let alone. (Ellen Alderson and Caroline Kennedy, 1995, p. 155; Samuel Warren and Louis Brandeis, 1890)

While Freedom of Information provides citizen with the right to access information held by state, the matter of informational privacy has been challenged. As government file occupies a great deal of personal data of which is indeed people's property, and more importantly, human dignity. The matter of disclosure of state data might probably cause the violation of privacy while too much privacy protection could also enable the government to escape from public eyes. The confrontation between Freedom of Information and Privacy Protection thus needs the balancing of public interest and personal privilege. The equilibrium between disclosure and

protection needs to be secured in this nature.

To the Thai experience, according to the Act, in the matter of information disclosure, discretion of state officials must be made with regards to the factors of State duties, public interests, and private interest. This is also confirmed by the constitution, which stipulated that information causing damage to a person, dignity, reputation or privacy must be prohibited. Therefore, freedom of information and privacy protection could be persistently found on each other's boundary and has become a matter of how to balance these two components. The controversy in the case of disclosure of examination scores and professorship evaluation is quite evident in this criticism.

4. Proposed Model for Personal Data Protection in Thailand

Many countries i.e. the United States, Canada, Australia, Japan, France, and Germany, have adopted national law to protect their citizens' data. Meanwhile, there have also been international laws and regional conventional measures for the control of data transfer between nations i.e. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Convention of the Council of Europe, European Union Directive, (Sirikul Puphan & Nakorn Serirak, 2001), Safe Harbour (http://www.export.gov/safeharbor), and APEC Privacy Framework (APEC Secretariat, 2005)

In Thailand, Privacy Protection has been, however, presented in the current OIA, but covers only personal data occupied by the government agencies. Yet, for the larger portion of Privacy and Personal Data of people, both those belonging to business enterprises and individuals, have never been recognized.

This paper therefore formulates and recommends a suitable mechanism for personal data protection in Thailand. The desirable proposed model will be elaborated in 3 aspects: (1) Development of Laws; (2) Policy proposal to create public awareness with regards

to privacy rights; and (3) Development of administration bodies for law enforcement and policy implementation.

4.1 Development of Law

Philosophically, human dignity comprises of two significant components, namely the right to life and to his or her corporeal; and the right to equality. Right to life emerges since man is born and has been protected by law. (Banjerd Singkaneti, 2000, p.9) This right establishes the relationship between people and State. The State must accept, respect, and cannot intervene into such rights. Any action either by the state or private citizens which results in affecting the principles of freedom and rights cannot be made as it is a violation of human dignity.

Personal data as right to life is considered as one category of the personal sphere, namely privacy rights. Man has absolute rights of his or her own discretional consideration whether or not he or she will allow the disclosure of his or her own data to anyone else or the public.

Data protection in Thailand is at the very beginning stage as a matter of personal data protection was realized 9 years ago by the emergence of OIA in 1997. But the law covers only personal data in government's files, those in private hands are not yet controlled by any specific laws. Thus, privacy right of the people is not fully protected. New law mechanisms which could control all personal data, both in the hands of the State and business is necessary. The initiative in drafting such a law is therefore the good response for such social needs.

The first draft of Personal Data Protection Law was started by National Electronics and Computer Technology Center (NECTEC) after the cabinet approved Information Technology Law Development Program in 1998. (NECTEC, 2004) The latest draft by OIC was completed in 2004. Both drafts contain somewhat similar text; however slight differences occur in the context of process, proce-

dure, rules, regulations, administration, punishments, etc., which is a matter of legal techniques. For the proposed model of the new law, Jantajira Iammayura explained the need to have these following components: (Jantajira Iammayura, 2000, pp. 20 - 21)

1. New code law should be made to protect data owner and control the management of data occupied by state, non government agency, and private enterprise.

2. In case there is any specific law providing no less standardized protection than Code Law, specific law will be given priority.

3. In the light of international practices of personal data protection, protection or closure is principle while disclosure is exception.

4. New code law should be made in relevance to OIA.

5. Only data of natural person will be protected.

6. Office of OIC will be office in charge of the new law. Implementation of the law should be undertaken by 2 commissions. One will take care of state data, another for those in the hands of private bodies. Each contains 2 organs of Regulator and Litigation Arbitrator

7. New law should clearly define the data categorization i.e. business data, security data, administration data, tax data, labor data, welfare data, etc.

8. New law must be in line with International Standards.

Desirable legal measures to protect personal data should be under the principle that the State must fully protect people with regard to their privacy by securing that people, i.e. data owners, possess the right to decide on whatever implementation, concerning their own personal data. The possibility and scope of collection, compilation, processing and utilization of personal data will be judged by data owners.

It has been 8 years since the first draft by NECTEC has been started. The latest draft by OIC was submitted to the cabinet in September 2005. (Office of OIC, 2005) Considering the present

situation of privacy violation which has been widely increased and has become more severe, while the process of legislation needs certain long period of time and procedures. The improvement or amendment of the present OIA is thus another alternative; adding data occupied or controlled by private citizens to be included under OIA enforcement. Concurrently, more detail concerning power, duty, and administrative system of the law as well as discretionary procedure of commission and tribunal, should also be amended accordingly. For this channel, informational privacy of Thai people would be potentially more secure in the foreseeable future.

The success of this model has been fruitfully developed in Australia. Australia Federal Privacy Act 1988 controlled only state agencies and covered only tax information and credit data in private agencies. The development to span the control of the Act to cover all data in private organizations was begun with the Privacy Amendment (Private Sector) Act 2000 which has been effectuated since December, 2001.(Paul Kelly, 2000)

4.2 Public Awareness Enhancement

It is difficult for legal measures and law enforcement to be effective without the enhancement of knowledge and understanding as well as public awareness on privacy and personal data protection. This paper will recommend measures to develop and enhance public awareness as follows:

1. Enhancement of law knowledge and understanding for state officials and the public

2. Conscience enhancement and attitude development concerning the awareness of informational privacy

3. Conscience enhancement and attitude development for the mass media and by the mass media

Knowing laws cannot lead to practice or exercise of rights, and law will be useless. Learning through real practice should be the learning process that can create enhancement of informational

right at its highest efficiency. Mass media will play important roles in the learning process because mass media by profession has duties to respond to public interest and people are familiar with power structure of not confronting with bureaucracy. Mass media is, therefore, fit to have leading roles in performing as people's representatives in fighting for privacy protection or exercising the right as representative of a civil society. In particular, mass media has roles in disseminating knowledge of law and creating understanding for changes in attitudes and awareness creation concerning public right because mass media has mechanisms to 'communicate' to 'the mass' in an efficient manner.

4.3 Administrative Bodies for Law Enforcement

The Official Information Commission (OIC) is the supreme policy agency in observing the information law, stipulated by the law to be chaired by a minister designated by the Prime Minister. (Kittisak Prokati, 1999) Commissioners are comprised of 23 senior officials and 9 qualified persons appointed by the cabinet. The Information Disclosure Tribunal (IDT) is also appointed by the Council of Ministers while the Office of OIC responsible for law enforcement is under the Prime Minister's Office.

It can be seen that policy management and regulation entities are all bureaucratic while policy management entities under the draft of the Personal Information Protection Act is likewise. It, therefore, can be said that at present personal data protection is purely executed by bureaucratic entities and the functions performed by OIC, IDT, and office of OIC, in structural terms, are hard to be autonomously implemented.

As the personal data protection is concerned with the context of relationship between "The State" and "The People", the scope of powers and duties of the entities in this respect inevitably cover the state because this entity has the powers to examine and supervise all state agencies.

Considering that civil society has important roles in examining to ensure transparency of state administration, through the participation process of non-government organizations, autonomous organizations, academic institutions, etc., the components of policy administration commission should, therefore, consist of representatives from various institutions and autonomous organizations with a suitable ratio for check and balance. Suitable patterns of the entity should be as follows:

1. Independent from administration and politics,

2. Policy administration commissioners should have a suitable ratio, from all parties related with personal data protection, whether it be politics, bureaucracy, private sector, autonomous organizations, specialists, academics, and civil society,

3. There should be a transparent selection system for persons appointed as commissioners so that the entity is the most specialized, neutral, autonomous and reliable.

4. The administration agency or entity which will perform law enforcement and policy implementation should be an autonomous organization.

5. Concluding remarks

Considering personal data as a part of human rights, namely informational privacy right, legal mechanism, either the enactment of new law or the amendment of the present one, is therefore inevitable. Thai people, as the same as humans of all nations, should also have mechanisms to protect human dignity and prevent any privacy violations.

Recently, there have been many observations retrospect of the intervention into privacy rights of the Thai people. It was found that police and security agencies have tried to get telephone usage data of customers from the Telephone Corporation claiming national security reasons. Telephone tapping is also another worse case. (Office of OIC, 2004) OIC is also concerned about the publicizing of

newspaper and television as it is quite often when criminal victims' pictures were printed or were broadcasted which is clearly the invasion into privacy rights of the victims as well as their relatives. (Office of OIC, 2004) The collecting and processing of personal data system, namely black list, or mafia, and those involved in narcotics, crime, gambling, and illegal business, without any consideration of privacy protection text under OIA and constitution is another evidence of breach of individual rights. (Office of OIC, 2003) Collecting and processing of people's personal data from various sources, i.e. health data, social welfare data, tax data, driver's license data, etc., in smartcard project, leave informational privacy rights of Thai people under the less, or least, privacy awareness of the government. All these reflect the severe threat to people's Right of Privacy and also insist inadequacy of the present law.

However, the Information Law and the concepts of Freedom of Information as well as Privacy Protection or Personal Data Protection are totally new, thus requiring some time to become more efficiently effective. State officials have to understand more clearly the procedures of law enforcement so that they know how to provide information services to meet public requests as well as to protect people's right of privacy. Meanwhile, people should know how to utilize the Information Act as a means to access state information. Most importantly, they should recognize their personal data as right of privacy to be respected by the State and any private citizens.

Official Information Act has been practiced for almost 10 years. Thai society needs some time to learn and recognize the "Right to Know" as an essential part of establishing transparent government and "Personal Data Protection" as an element of securing human dignity.

References

Alderman, Ellen and Kennedy, Caroline. (1995) *The Right to Privacy.* NewYork,

Alfred A. Knopf.

APEC Secretariat. (2005) *APEC Privacy Framework*. Singapore.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Flaherty, David H., (1984) *Privacy and Data Protection: An International Bibliography*. Knowledge Industry Publication Inc.

Constitution of the Kingdom of Thailand, B.E. 2540 (1997). *Government Gazette*. Vol.114, Part 55A, dated October 11, B.E.2540 (1997).

Official Information Act, B.E. 2540 (1997). *Government Gazette*. Vol.114, Part 46A, dated September 10, B.E.2540 (1997).

Information Disclosure Tribunal for Social, National Administration, and Law Enforcement Information, Decision No. 1/2541(1998).

Information Disclosure Tribunal for Economic and Financial Information, Decision No.1/2542 (1999).

Information Disclosure Tribunal for Social, National Administration, and Law Enforcement Information, Decision No.17/2542(1999).

Information Disclosure Tribunal for Social, National Administration, and Law Enforcement Information, Decision No.33/2543(2000).

Iammayura, Jantajira. (2004) Personal Information Law in Thailand, in Thammasat University Research and Consultation Institute. *Research Project on Principles and Guidelines for Personal Data Protection Law Implementation and Handbook for Personal Data Protection under the Official Information Act 1997*, submitted to Office of the Official Information Commission.

Introduction to the Safe Harbor. [Online]. Available from: http://www.export.gov/safeharbor

Kelly, Paul. (2000) Recent Development in Private-Sector Personal Data Protection in Australia: Will There be An Upside Down Under?. *John Marshall Journal of Computer and Information Law 71*.

National Electronic and Computer Technology Commission. (2001) A Draft of Personal Information Act B.E. .... *Information Technology Law Development Program Dissemination Paper*.

Nugter A.C.M. (1990) *Transborder Flow of Personal Data within the EC*.

Computer / Law Series. Deventer-Boston, Kluwer Law and Taxation Publishers.

Office of the Official Information Commission, Letter No. 1311/10634 dated November 19, 1999.

Office of the Official Information Commission, Letter No.1311/99 dated January 7, 2000.

Office of the Official Information Commission, Letter No. 1311/99 dated January 7, 2000.

Office of the Official Information Commission, Letter No. 0107/5003 dated September 30, 2005.

Office of the Official Information Commission, Official Information Commission Meeting Report, 4/2003, April 10, 2003.

Office of the Official Information Commission, Official Information Commission Meeting Report, 7/2004, November 24, 2004.

Office of the Official Information Commission, Official Information Commission Meeting Report, 8/2004, December 20, 2004.

Office of the Cabinet Secretary, Letter No. 0205/184 dated December 2, 1999.

Office of the Cabinet Secretary, Letter No. 0205/1685 dated February 7, 2000.

Office of the Council of State. 2000. A Law-consulting Note on the Disclosure of Examination Information. *Administrative Law Journal*, 19, April.

Prokati, Kittisak. (1998) *Right to Know Information under Official Information Act B.E.2540*. Bangkok, Vinyuchon.

Prokati, Kittisak. (1999) *Some Observations on Authoritative Power and Duties of the Official Information Commission*. Discussion Paper for the Official Information Commission 1999 Annual Seminar.

Puphan, Sirikul and Serirak, Nakorn. (2001) *Personal Data Protection in International Law*. Office of the Official Information Commission.

Serirak, Nakorn. (1999) *Right to Know Official Information*. Krungthepturakij, October.

_____. (2000) Two Motivating Years of Exercising the "Right to Know" in Thailand. The Nation. March.

_____. (2000, 2001) *Challenge of Freedom of Information in Thailand*. a paper presented in the Seminar on the Urgency of Freedom of Information Act, Jakarta (2000) and Conference in Freedom of Information and Civil

Society in Asia, Tokyo(2001).

_____. (2002) Making Sense of the Right to Know, *Bangkok Post*. September.

Singkaneti, Banjerd. (2000) *Basic Principles of the New Constitutional Right, Freedom, and Human Dignity*. Bangkok, Vinyuchon.

Wacks, Raymond. (1989) *Personal Information: Privacy and the Law*. Oxford Clarendon Press.

Warren, Samuel and Brandeis, Louis D. (1890) The Right to Privacy. *Harvard Law Review* 193.