STATE SURVEILLANCE, PRIVACY AND SOCIAL CONTROL IN THAILAND (1350-1998)

by

Pirongrong Ramasoota

B.A. Chulalongkorn University, 1989

M.A. University of Hawaii at Manoa, 1992

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in the School

of

Communication

© Pirongrong Ramasoota 2000

SIMON FRASER UNIVERSITY

January 2000

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-51914-7

Canada

Abstract

This dissertation examines the development of state surveillance, the emergence of information privacy issues, and implications for social control in Thailand.

The analytical framework draws on western critical social theory that questions the legitimacy of modern forms of state surveillance, and discourse on privacy that argues for limits on infringements on privacy through social action and public policy. The research included documentary research for the historiography of surveillance; case studies of contemporary surveillance practices by two technologically-advanced government organizations; interviews with government administrators, policy-makers, and selected members of the Thai public; as well as analysis of information policies and laws.

Social reform and a state-engineered modernization program, brought about by western capitalism and imperialism in the late nineteenth century, introduced rationalized methods of surveillance into Thailand (Siam)'s rudimentary system of social control. The new civil registration system became an integral part in the rise of the absolutist state and later the emergence of a "bureaucratic polity," which used the consolidation of an internal security state as rationale for tight social control and suppression of democratic discourse.

The changing political economy and the emerging "civil society" since the late 1980s have undermined the "bureaucratic polity" while creating openings for relative autonomy in some areas. Meanwhile, the aspiration for industrialization has led to a massive informatization of Thai society. In a relative absence of public consciousness about privacy, information and communication technologies (ICTs) became widely exploited in personal record-keeping by the state. These new modes of surveillance helped entrench patterns of state domination and social injustice in many areas, including political elections, employment, and health. Despite the emergent regulation of state information practices and legislative attempts for personal data protection, which was brought on by penetrative international policy frameworks, implications of state surveillance and its growing interactions with private sector surveillance are still not sufficiently addressed.

The study concludes that the emerging information privacy regime may not suffice to cope with the growing technological surveillance by the state. It proposes that the issues be advanced through critical scholarship and public learning to create avenues for resistance.

For my beloved parents without whom

there would be no "kwan"

Acknowledgements

CONTENTS

TABLES

FIGURES

Figures

APPENDICES

PREFACE

This thesis is a set of exploratory studies about the development of state surveillance in Thailand, related information privacy issues, and the implications for social control. At one level, pertaining mostly to the Western audience, it represents a cross-cultural and cross-national analysis of surveillance and privacy -- two intertwining concepts that have emerged as a new subfield in Western social sciences. In recent years, these concepts have received widespread attention from across several disciplines including sociology, political science, communication, public policy, history and computer and information science. Although theoretical advance is being made through critical engagement with these concepts, little has been done outside the context of western industrialized countries. One primary objective of this study is to show whether the western theory of "surveillance has relevance to a social analysis of the Thai state and a study of social control in Thai society. It is mainly from this body of literature and the critique of its limitations that the analytical framework for the first section of this study -- focusing on state surveillance and social control -- derives. By contrast, an equally important objective is to show in the latter section of the study whether the conventional discourse on privacy, with its liberal democratic underpinnings, is applicable for dealing with the Thai political and cultural context.

At another level, addressing the Thai audience, particularly scholars of communication, this study is an effort to introduce a critical form of inquiry that draws on recorded experience of information practices in Thai society. By constructing the analytical framework around the ideas and arguments of critical communication scholars, this inquiry is intended to assume a "critical communication perspective" and to mark a decisive break from mainstream communication research that is dominant in Thailand.[1] Communication studies in Thailand have been deeply influenced by the theorizing and methodology of the American mainstream approach to communication, with its preoccupation with modernization and social stability as central theoretical concerns, and objectivity and instrumentalism as major methodological orientations.[2] In line with the biases of structural-functionalism and

---

[1] By a "critical communication perspective," I mean a perspective which is concerned with the "effectivity of communication in the exercise of social power." See more in Jennifer Daryl Slack and Martin Allor, "The Political and Epistemological Constituents of Critical Communication Research," *Journal of Communication* 33 (3, 1983): 215.

[2] The domination of American scholarship on the communication discipline in Thailand is reflected in both curriculum and research themes and methodologies undertaken by local scholars. This is largely because most of these scholars have been trained in the U.S. and most feel uncomfortable denouncing theories and approaches that were the backbone of their own educational formation. This domination is further intensified by the presence of American academics as visiting professors in major Thai universities and by the funding of many local research programs through U.S. aid agencies.

pragmatism on which it is based, American mainstream communication research has been predominantly value neutral, ahistorical, unreflective, and supporting of the status quo. These are most evidenced in the paradigms of mass media and modernization, and more recently, in the information society thesis, both of which constitute the dominant intellectual paradigm for communication studies in Thailand.

Three salient features of critical communication approaches are embraced in this study, including an emphasis on history and culture, a conceptualization of communication as a social process,[3] and a distinct epistemology that entails an informed critique of society.[4] As the readers will see, the thesis is highly historical in nature. The entire studied period spans more than seven centuries, including major portions of ancient and modern Thai civilization. To the extent that this thesis may make any contribution to understanding contemporary aspects of state surveillance, privacy, and implications for power relations in Thai society, it is by setting them in a wider context, indicating the range of variation in social control by the state and providing evidence about their early history. The thesis mainly employs an "institutional analysis" in analyzing the growth of state surveillance and the resistance it has evoked in each historical epoch. Though the importance of surveillance technologies are not neglected, the emphasis of this analytical framework is more on the social, economic, and political context surrounding the surveillance system. Much interest is also given to the perception and behaviors of people in a position to administer the surveillance and those subject to surveillance. This explains the reasons for the many

---

[3] Unlike the infamous "media effects" model of mainstream communication research in which communication is seen as a simple linear causal process, critical communication research instead redefines communication as a social process, one which is inseparably intertwined with other social institutions and processes (e.g. the state, the people, and economic organization). Similarly, the critical scholars do not conceptualize power and its effectivity in simple linear terms.

[4] Unlike mainstream communication thinkers who do not analyze the political character of epistemological choices because of their fixation on value-neutrality and objectivity, critical thinkers are acutely aware of the integral link between epistemology and politics. According to Theodore Adorno, a leading member of the Frankfurt School, where the most original form of Critical Theory was bred, epistemology is understood as "not merely a simple question of choice of methods or operationalization" because it also entails the researcher's position within the social order. Since critical approaches generally see social life as fraught with domination -- characterized by an accumulation of and an exercise of social power, critical communication researchers are expected to try to understand the sources and exercise of social power as they relate to communication processes and information practices. This is so that they could produce an informed critique of the contemporary conditions of society and ultimately map out a course of action that is necessary to transcend the current stage of social and economic practice. See, for example, Theodor W. Adorno, "Scientific Experiences of a European Scholar in America," in The Intellectual Migration: Europe and America 1930-1960, eds. D. Fleming and B. Bailyn, (Cambridge, Mass: Harvard University Press/Belknap, 1969), 343-347; and Hanno Hardt, Critical Communication Studies: Communication, History, and Theory in America (New York: Routledge, 1992), 168-172.

individual and group-based interviews undertaken with government administrators, system designers, policy-makers, and selected members of the public. In analyzing privacy, a multi-faceted and primarily exploratory approach comprising focus group interviews, a survey of anthropological evidence, and a critical analysis of legal statutes and public policy on privacy issues, particularly information privacy, is employed as analytical framework.

The thesis is divided into two broad parts. The central concern of part one will be "state surveillance" or specific ways in which the Thai state, particularly in its administrative and citizenship dimensions, influences the collection and use of personal information for social control purposes, as well as ways in which people seek to challenge this form of domination. The second part deals mainly with "privacy/data protection," delving into anthropological evidence, cultural perceptions, and public-policy discourse on the issues in contemporary Thai society and implications for future mobilization for social change in the area of information privacy.

The thesis begins with an examination of selected theoretical perspectives on surveillance, the state, and social control, concentrating on the insights of selected major western critical thinkers in addition to a brief review of two related theories -- the modernization paradigm and the information society thesis. Following a critical review of this literature, I will draw up what is perceived to be their main strengths and limitations, particularly for a cross-cultural study of surveillance, and outline my own analytical framework. The second chapter analyzes state surveillance and the resistance it provoked in ancient Thailand (Siam) covering three major periods in Thai history -- Ayutthaya, Thon Buri and early Rattanakosin (1350-1905). The third chapter undertakes the same inquiry within a context of modernizing Siam, beginning with the historic Chakkri Reformation (1905) that set the country on a state-engineered modernization program under royal absolutism and closing with the semi-democratic period of the early 1980s. The significance of foreign geo-political intervention which triggered two important events -- social reform and the war in Indochina -- are brought to bear on the spread and changing nature of state surveillance during this period. The fourth and fifth chapters discuss case studies of two major contemporary state surveillance systems within the context of early industrialization, democratization of the polity, and informatization of the society. An emphasis is given in both chapters to the ways that new information and communication technologies (ICTs) have augmented state surveillance capacities, and the public response to these improved surveillance measures. Chapter four analyzes the Ministry of Interior's Population Information Network (PIN) project which, in a little more than a decade, has grown from a

computerized databank storing crucial personal information on citizens to an integrated information network with multi-faceted links and tremendous potentials for information use and manipulation. The implications of this massive network are assessed in several aspects including democratic development and extension of citizenship rights. Chapter five examines the Police Department's criminal records database, focusing on its major component -- the Automated Fingerprints Identification System (AFIS) -- and the exploitation of the system for non-criminal justice ends, which raises questions regarding employment and social justice. Chapter six marks the beginning of the second part of the study -- privacy. It provides a brief anthropological, sociological, and public policy sketch surrounding the concept of privacy/data protection as primarily understood in the West and closes by making a linkage to the Thai context. Chapter seven summarizes the findings from five focus group sessions carried out with Thai participants on the topic of information privacy. Culture and class are highlighted as major factors that shape the perception and treatment of privacy by these individual participants. Chapter eight explores the recent emergence in Thailand of regulation of state surveillance in the information sphere as prompted by ongoing democratic movements, as well as the rise of data protection as a legal and public policy concern as provoked by the penetration of global policy networks. The ninth and last chapter concludes the study by synthesizing part one and two and by drawing out major theoretical arguments of the earlier chapters. A further evaluation of the strengths and limitations of Western theoretical perspectives on surveillance and privacy in studying Thai society is also undertaken in this chapter.

Two considerations led me to the choice of surveillance and privacy as a topic for research. Although born and raised in Thailand, I always had a nagging feeling about the widespread requirement for a national identity card and household registration document in almost all types of transactions in Thai society. After being exposed to North America's relatively loose system of state control, I realized that the social mechanisms of national identification and civil registration, always taken for granted in Thailand, are by no means universal. This realization about the uniqueness of the Thai system became more stimulated when I was introduced to the literature on surveillance and privacy during my academic pursuit at Simon Fraser University. The fascination with the insights of western thinkers about this form of social control has gradually coalesced into a well-founded interest and a desire to trace the origin and development of state surveillance systems in the Thai context. Although I personally have set quite a high value on privacy, common sense tells me it is not a prevailing value in Thai society. But with the dynamic of change that comes with the structuring of informatization now beginning to be realized by Thai society, I feel "privacy,"

especially information privacy. may indeed be a worthy and timely concept to explore.

Choosing Thailand as a context of study may strike some readers as a reflection of "convenience" on my part. While this may contain some grains of truth, it is not the only reason. Despite its emphasis on and fervent aspiration for industrialization, Thailand, as the readers will see, represents a radical particularity of history and geography, an interesting case to demonstrate empirical relevance, as well as a challenge for the Western perspectives on surveillance, privacy and social control. Throughout its extensive historical development, the Thai state has fostered a strong heritage of social control through the means of collecting information about and supervising its people, precisely the ideas underlying "surveillance." Insofar as privacy is concerned, this concept only recently emerged in Thai society as a result of the penetration of global policy on data protection. In this regard, the Thai perception and experience of privacy and data protection explored in this study may provide some interesting insights for potential readers in the Western policy community who are pressing for a globalizing convergence in privacy and data protection.

PART I: SURVEILLANCE

CHAPTER 1

INTRODUCTION TO SURVEILLANCE:
BASIC CONCEPTS, THE STATE, AND INFORMATIZATION[1]

This chapter explores three themes. First, the basic elements of the concept of surveillance as used throughout the study are outlined. Second, a critical review of theoretical arguments by four major Western thinkers on surveillance and the state is presented. Then, a brief discussion of the modernization paradigm and the information society thesis is undertaken to show how contemporary surveillance may have been eclipsed by discourse and currents promoting informatization, particularly in the context of the so-called Third World. The chapter concludes by mapping out the analytical framework used for the first part of the study by drawing on the theoretical arguments and analytical concepts reviewed earlier.

SURVEILLANCE: DEFINITION AND DIMENSIONS

Although broadly understood as the monitoring and supervision of population for specific purposes, "surveillance" as used in this study will involve one or more of the following related phenomena:

1) the accumulation and storage of "coded information" about individuals;

2) the supervision of activities of individuals by others in positions of authority;

3) the application of information-gathering activities to the task of administering the activities of individuals about whom the information is gathered.[2]

---

[1]The term "informatization" was coined by the Japanese in the 1960s and has been used as a guiding slogan for local and national public and industrial policies for more than three decades. In the 1980s, concerned with excessive concentration of economic and human resources in Tokyo metropolitan area, many policy initiatives began to promote "informatization" in local areas. See Nagy Hanna, Sandy Boyson and Shakuntala Gunaratne, *The East Asian Miracle and Information Technology: Strategic Management of Technological Learning*, World Bank Discussion Paper No. 326 (Washington DC.: World bank, 1996), 185.
[2]These definitions are compiled from contributions by three major social theorists on surveillance: Michel Foucault, *Discipline and Punish: the Birth of the Prison* (New York: Vintage Books, 1977), Anthony Giddens, *The Nation-state and Violence Volume Two of a Contemporary Critique of Historical Materialism* (Berkeley: University of California Press, 1987), Anthony Giddens, *The Consequences of Modernity* (Cambridge, Polity Press, 1990), and Christopher Dandeker, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (New York: St. Martin's Press, 1990).

The important facet of surveillance that is touched upon in this study is in its being administrative means of reproducing a social system of rule. Max Weber defines the concept of rule as "a durable system of domination regardless of its institutional location."[3] Although Weber avoids tying the concept to the state, this study will primarily examine surveillance as an administrative basis of rule only in the sphere of the state. A system of rule, as indicated by Weber and Giddens, involves durable, routinized relationships of command and obedience. It also implies that there is a high probability that commands will be obeyed in a stereotypical or predictable manner.[4] Two strategies of resource mobilization to achieve the objective of a compliant subject population can be outlined: 1) to maintain and deploy punitive sanctions against rule breakers -- a power to punish after the event; and 2) to devise mechanisms for excluding potential rule breakers from the opportunity to disobey instructions -- a prophylactic power of control. In any case, as pointed out by James B. Rule, neither of the two strategies for gaining compliance would be effective without the administrative support of a surveillance system. Surveillance, as defined above, would not only provide "a means of knowing when rules are being obeyed, when they are broken, and who is responsible for which" but also the ability "to locate and identify those responsible for misdeeds of some kind."[5]

While surveillance is clearly implicated as a crucial basis in achieving control and the capacity to rule by dominant organizations, organizations are also said to vary considerably with respect to their surveillance capacities. Dandeker voices skepticism regarding the existence of "total surveillance systems" as portrayed in literature or in sociological speculation about the authoritarian potential of modern societies. He suggests four criteria with which to measure the surveillance capacities of different organizations and to specify what the expansion of those capacities entails. They are:

1) the size of the file held in a surveillance system;
2) the centralization of those files;
3) the speed of information flow;
4) the number of points of contact between the system and its subject population.

Dandeker defines the size of the files as the numbers of persons and items of information about them that can be stored. He emphasizes the precision of the information

[3]Max Weber. *Economy and Society*. vol. 1 (Berkeley: University of California Press, 1978), 56.
[4]Ibid., 53-54, 212-216 ; Anthony Giddens, "The Nation-state and Violence ," 7-17.
[5]James B. Rule. *Private Lives and Public Surveillance* (London: Allen Lane, 1973), 21.

as the main quality affecting capacity for monitoring and/or control. As for the centralization of files. Dandeker notes that the more centralized the information files are. the more possible it is to gather information on a person at any point in the system and then use it to control that person at any other point. This. he argues, is most evident in the cross-referencing capacities of modern computer systems, which are also capable of integrating knowledge from formally separate systems. Meanwhile. the speed of information flow is said to concern "the time taken for information on subject population to be gathered, transmitted to a central point, processed and then used to supervise or manage their behavior."[6] Finally, Dandeker explains points of contact as the number of points in the lives of subject populations which are available for the collection of information and the supervision of behavior by organizations. Point of contact also includes the ease with which deviants can be identified and their behavior monitored consistently and continuously as well as the capacity to maintain a constant and detailed connection between an individual and his or her record or file.

While Dandeker's criteria may be pragmatic and potentially useful for cross-cultural or cross-national analysis of surveillance systems, they are also overly quantitative and mechanistic. The quality and nature of the information contained in the files are entirely overlooked. Furthermore. his measurement scheme also disregards the fact that any surveillance system is a part of a social system and its arrangement and capacities are bound to be shaped by institutional factors -- political, legal, cultural -- within that system. To analyze an organization's surveillance capacity out of a social context would be a disservice. In order to supplement these shortcomings, I propose that three more analytical categories be added to the above criteria: 1) the type of information that is collected and stored in the files; 2) the purpose to which this information is put; and 3) the safeguards, checks and balances that are in place in the larger social system to counteract this surveillance capacity. I borrow the third analytical category from Simon Davies, a privacy advocate, in his proposed scheme to quantify surveillance.[7] With these suggested dimensions addressed, this modified criteria should be useful as a heuristic device in exploring an organization's surveillance capacity. The analysis in the subsequent chapters will rely on this device to examine the growth of state surveillance system in Thailand.

---

[6]Christopher Dandeker, *"Surveillance. Power and Modernity."* 41.

[7]Simon G. Davies, "Surveying Surveillance: an Approach to Measuring the Extent of Surveillance." in *Computers. Surveillance and Privacy*, eds. David Lyon and Elia Zureik (Minneapolis: University of Minnesota Press. 1996). 260-273.

3

THEORIES OF SURVEILLANCE AND THE STATE

The following discussion reviews the theoretical insights of Max Weber, Michel Foucault, Anthony Giddens, and Christopher Dandeker on the nature and significance of surveillance activities conducted by the state, particularly modern states, in the process to secure administrative and social control. Their accounts vary in dimension and emphasis, though all agree that large-scale and bureaucratic forms of surveillance by the state are a product of modernity, and one that renders a more relentless form of control than its predecessors.

Max Weber on rationalization, surveillance, and the modern state

The key to understand Weber's view on state surveillance lies in his theory of rationalization. Rationalization, for Weber, entails a special formal instrumental form of rationality which assumes that everything is subject to measurement and calculation. According to Weber, the institutionalization of this type of rationality -- also known as "means-end rationality" -- in all social institutions is a constitutive feature of modernity. The transition process to modernity is thus marked by the development of scientific reasoning and instrumental calculation, the rational capitalist enterprise, and the rational-legal bureaucratic state. Inherent in these modes of behavior and organizations is a structure of domination that is perpetuated by the promise of increased efficiency.[8] Surveillance in its bureaucratic mode plays an essential role in this structure of domination, otherwise seen as a rational administration of modern organizations. In a modern state, the rational structure of domination and surveillance is expressed in the relationship between leaders and led that is mediated by a government bureaucracy.

In Weber's writings, the general exercise of surveillance by the modern state is associated mainly with two strategies: 1)the management of organized knowledge and 2) the concentration of the means of administration. Two types of knowledge -- technical knowledge and knowledge of facts -- are involved in the first strategy. Technical knowledge, used in the application of modern technology and systematic methods to

---

[8]Weber defines "domination" as the probability that certain specific commands (or all commands) will be obeyed by a given group of persons. Domination, in this sense, does not consist only of exercise of "power" or "influence" over other persons, it may also be based on diverse motives of compliance from simple habituation to rational calculation of advantage. See Max Weber, *Economy and Society*, 2 vols. (Berkeley: University of California Press, 1978), 212.

administrative tasks by expert officials, is essential to ensure higher accuracy and productivity. Knowledge of facts, which refers mainly to the ability to collect and store information about subjects and objects under centralized state control, strengthens this power even further. With access to the same information stored in official files, anyone within the bureaucracy can exploit it for administrative purposes, hence making bureaucratic action replicable and thereby rationally calculable. Weber explains the association of power with knowledge in the following terms, "bureaucratic administration means fundamentally domination through knowledge. This is the feature which makes it specifically rational."[9]

As far as the concentration of the means of administration is concerned, it involves a shift from personal and patrimonial forms of administration to the rational and bureaucratic organizations of modernity. In the former, rulers have few means of controlling their subject populations beyond their personal powers of supervision and information gathering. In feudal patterns of rule, for instance, many rulers have to rely primarily on the delegation of administrative rights to autonomous power-holders, primarily local landlords, in exchange for military service and loyalty. In lieu of financial payment, the local landlords benefit from payments in kind from the population under their control and certain privileges bestowed from the rulers. Under this strategy of rule, however, the means of administration are not only diffused to the localities but are also fused with economic and social power of the landlords. Likewise, the circuits of administrative control and information flows are prone to disruption and corruption since the local power-holders may collude with the subjects under their supervision or with each other to accumulate countervailing power and thereby weaken the power of the rulers.

In modern bureaucratic administration, on the other hand, the capacities of administrative control and information flows are considerably improved and concentrated in terms of spatial and temporal extent. This is due to permanent and rationally disciplined bureaucracies, which are made possible by the economic and technological resources of modern industrial society. Since the bureaucratization of state administration in the modern era pays its entire administrative expenses from the central budget including officials' salaries, the central state can regulate and control their bureaucratic officials more effectively than pre-modern rulers could control local lords, hence preventing accumulation of economic and political countervailing powers.[10]

---

[9]Ibid., 225.
[10]Max Weber, *Economy and Society*, 2 vols., 982.

In addition, unlike traditional states, the modern state has a recognized right to monopolize the use of force within its given territory. Its bureaucracy has the means of subjecting its territory and population to detailed surveillance, which is legitimized under the claim of public policy. As a result, the subject population became objects of surveillance through continuous administration and the ensuing penetration of everyday life in ways unparalleled by pre-modern, or pre-rational political structures. According to Weber, the subject population comply with state regulation for a variety of reasons, namely, monetary reward, convenience, and habit. That habituation is the more important may indicate a level of consent among the populace reflecting the state's legitimacy. The modern state, it is argued, draws its legitimacy of rule from the fact that its orders are established and exercised in a way that is recognized to be legal. In line with his theory of rationalization, Weber argues that the legitimation basis of the modern state is not based on certain substantive values such as freedom and democracy but on the formal logical character of legal norms, which are capable of expressing and legitimating any particular substantive end as a basis for state policy.[11]

While profoundly critical of the expansion of rationalization and bureaucratization in modern society, Weber views the social domination that these processes embody as inescapable, or in his metaphor, as "the iron-cage" of rational-legal organization.[12] This, it has been argued, is where Weber departs from subsequent writers in the tradition of the critical theory of the Frankfurt School, who not only denounce the relentless spread of instrumental means-end rationality but also make investigations of its effects in the social world the central theme of their intellectual project. According to Herbert Marcuse, a prominent member of the Frankfurt School, while Weber is pessimistic about the dangers and risks involved in this "iron-cage" of rationality, he also feels that the rationalized world is also the world which makes possible the development of social institutions tending toward law and justice that would free the arbitration of civil society from collective and individual substantive interests. But to Marcuse, Weber's conception of rational expansion as a process that is inevitable masks a "concept of fate" which "generalizes the blindness of a society which reproduces itself behind the back of individuals, of a society in which the law of domination appears as objective technological law."[13]

[11]Ibid., 809-838.

[12]Max Weber, *The Protestant Ethic and the Spirit of Capitalism* (1930), trans. Talcott Parsons (London: Allen and Unwin, 1976), 181-182.

[13]Herbert Marcuse, "Industrialization and Capitalism in the Work of Max Weber," *Negations* cf. Theodore Adorno, "Society," trans. Frederick Jameson, *Salmagundi*, nos. 10-11 (1969-1970), as quoted in David Held, *Introduction to Critical Theory : Horkheimer to Habermas* (Berkeley: University of California Press, 1980), 66.

If the key to understand Weber's thinking about surveillance and the transition to modernity is his theory of rationalization, the means to uncover Foucault's thought on the same topic is his genealogical analysis of the rise of "disciplinary society." The focus of Foucault's analysis is Western Europe from the late seventeenth century onwards. This period is generally regarded as the major period of transformation from the so-called "classical age" (the age of absolutism or, more generally the ancien régime) to the modern era. Traces of Weber's theory of rationalization and his association of power with knowledge can be found in Foucault's analysis.

According to Foucault, the modernization process in Western Europe corresponds with the development of a new mode of power, which derives from the emergence of more efficient disciplinary technologies. In absolutist regimes, monarchic power may seem absolute given the existence of public torture and execution of criminals. However, like Weber, Foucault finds this type of power to be not only personal and arbitrary but also incomplete and inefficient. Foucault particularly emphasizes the relatively weak penetration into the soul of this type of power and how it leads to ineffective control, regulation, and disciplining of society. This relative absence of effective control, argues Foucault, also creates spaces and opportunities for solidarity and spontaneous rebellion among different groups in the population.[14]

In contrast with the traditional penal system, which focuses on inflicting pain on the physical body, the modern system accentuates the power to punish more deeply within the soul. The birth of the modern prison is a key invention in this regard. For Foucault, the techniques of learning about and disciplining the souls, that are perfected in the prison, have pervaded an ever broader range of contemporary societal institutions and affect every modern individual, hence giving rise to a disciplinary society. To understand this new modality of power and the embedded disciplinary technologies, it is useful to turn to Foucault's famous discussion of the panopticon, which has become the most influential metaphor when it comes to sociological analysis of contemporary surveillance.

---

[14]Foucault mentions at least two social groups who constitute a source of counterpower and autonomous group solidarities to the monarchic regime -- the privileged groups of nobles and the underprivileged in the lower social strata.

In *Discipline and Punish*, Foucault uses the term Panopticon to designate the control mechanisms in two phenomena -- the effort to control the spread of the plague in late seventeenth-century Europe, and a prison model in the late eighteenth century. In the first case, Foucault identifies segmentation and surveillance as the major strategies in the control of the epidemic. Questioned in their individual homes, each and every resident was required to report to the syndics at the door the status of his or her health under pain of death. Foucault describes the collection and accumulation of information in this surveillance system.

> This surveillance is based on a system of permanent registration: reports from the syndics to the intendants, from the intendants to the magistrates or mayor. At the beginning of the "lock up," the role of each of the inhabitants present in the town is laid down, one by one; this document bears "the name, age, sex of everyone, notwithstanding his condition": a copy is sent to the intendant of the quarter, another to the office of the town hall, another to enable the syndic to make his daily roll call. Everything that may be observed during the course of the visits -- deaths, illnesses, complaints, irregularities -- is noted down and transmitted to the intendants and magistrates.[15]

To Foucault, the hierarchy of surveillance, the observation, the reporting, and the segmentation of individuals into confined space -- all this "constitutes a compact model of the disciplinary mechanism."[16] This disciplinary mechanism has been put to regular use in a wide range of social institutions -- the psychiatric asylum, the penitentiary, the reformatory, the factory, and the school, and to some extent, the hospital -- from the eighteenth century onwards. Gradually, the technology of discipline developed in these disparate, peripheral localizations became perfected and systematized in a corpus of knowledge, a science. Foucault labels this science, this technology of the body as an object of power, "disciplinary power."[17] The basic goal of disciplinary power is to produce a human being who could be treated as a "docile body," which is useful for both the accumulation of capital and the accumulation of power. The techniques for disciplining bodies are applied mainly to the working classes and the subproletariat, although not exclusively, since they also operated in schools and universities.[18] With the help of the objectifying sciences such as medicine, criminology, sociology, psychiatry, statistics, and demography, the authorities exercising this disciplinary power will objectify and classify the individual subject according to sets of

[15]Michel Foucault, *Discipline and Punish: the Birth of the Prison* (New York: Vintage Books, 1977), 196.
[16]Ibid., 197
[17]Foucault sometimes refers to this as "bio-power," which he describes as a modern form of power which is characterized by increasing organization of populations and welfare for the sake of increased force and productivity.
[18]Hubert L. Dreyfus and Paul Rabinow, *Michel Foucault: Beyond Structuralism and Hermeneutics* (Chicago, University of Chicago Press, 1982), 8.

dichotomies. each side of which is an effect of power, for instance, sick/healthy, mad/sane, criminal/good citizen, abnormal/normal. and deviant/good citizen.

The disciplinary techniques first developed in the case of the plague-stricken town became even more pronounced and refined in the second case -- an architectural structure from where the name "panopticon" is derived. The Panopticon is a prison model designed by Jeremy Bentham in the late eighteenth century with an underlying aim to facilitate the efficient observation or surveillance of prisoners. The guard, who would periodically be stationed in a central tower, could observe the inmates, arranged in cells around the tower with windows facing in towards it, without himself being seen by them. In effect, this design would, according to Foucault, create a "state of conscious and permanent visibility that assures the automatic functioning of power."[19] As a result of this "visible" and "unverifiable" form of power, the prisoners would be oriented towards the authority system of the prison as a step in their reformation or normalization.[20] In this reform process, the Panopticon is also a part of a broader set of mechanisms, which includes a minutely regulated schedule, a detailed system of file-keeping of each prisoner, which generates a resource of knowledge. and so forth.

In other words, there are two major elements in the Panopticon that embody the system of discipline -- its micrological details. and the way it inscribes power. For the latter element, the inscription of power is far more positive than the traditional infliction of pain or the principle of preventing or denying certain activities as in the feudal era. Through the workings of the Panopticon, the prisoners would learn to follow the prison's rule, aware that the slightest deviation could be observed and result in certain consequences. In this learning process, the behavior of these former criminals can be moulded and shaped in the direction desired by the prison's authority. By the same token, the panoptic model of discipline can allow for a norm to be continuously and systematically inscribed into a population, into its practices and its attitudes. a norm that is a result of an anonymous authority that is omnipresently present.

Foucault describes the two intertwining elements of discipline embodied in the Panopticon as follows:

---

[19]Michel Foucault, *Discipline and Punish*, 201.

[20]According to Foucault, Bentham laid down the principle that power should be visible and unverifiable. It is visible in the sense that the inmate will constantly have before his or her eyes the tall outline of the central tower from which s/he is spied upon. It is unverifiable in the sense that the inmate must never know whether s/he is being looked at any one moment but thinking s/he may always be so.

The Panopticon functions as a kind of laboratory of power. Thanks to its mechanisms of observation, it gains in efficiency and in the ability to penetrate into men's behavior; knowledge follows the advances of power, discovering new objects of knowledge over all the surfaces on which power is exercised.[21]

Although the Panopticon was never actually built, this does not stop Foucault from employing it as a metaphor for a system of social control in modernizing Western Europe. According to Foucault, the Panopticon must be understood as "a generalizable model of functioning, a way of defining power relations in terms of the everyday life of men."[22] The panoptic schema, argues Foucault, is polyvalent in its applications and may be used whenever one is dealing with a multiplicity of individuals on whom a task or a particular form of behavior must be imposed. Apart from disciplining and reforming prisoners, the panoptic strategy may also be used "to treat patients, to instruct schoolchildren, to confine the insane, to supervise workers, and to put beggars and idlers to work."[23] Its ultimate goal is not necessarily to punish, in the conventional sense of the word, but to normalize behavior toward the more desirable dyadic category; for instance, productive rather than unproductive, normal rather than abnormal, and good citizen rather than criminal or "deviant."

While Foucault feels that the panoptic model of discipline has spread and become perfected in modern societies from the eighteenth through the twentieth centuries, he also notes that the operation of this "technology of power" is not clearly visible because it is usually masked by another type of power -- juridical or sovereign -- which is embodied in the liberal discourse of law and rights. The dominant liberal orientation is to questions of legitimacy and illegitimacy rather than issues of struggle and submission, to relations of sovereignty rather than domination, and to creating norms rather than normalization. In his words,

The theory of sovereignty, and the organization of a legal code centered upon it, have allowed a system of right to be superimposed upon the mechanisms of discipline in such a way as to conceal its actual procedures, the element of domination inherent in its techniques, and to guarantee to everyone, by virtue of the sovereignty of the State, the exercise of his proper sovereign rights.[24]

---

[21]Michel Foucault, *Discipline and Punish: the Birth of the Prison* . 205.
[22]Ibid.
[23]Ibid.
[24]Michel Foucault, *Power/Knowledge: Selected Interview and other Writings (1972-1977)* (New York: Pantheon Books, 1980), 105.

In any case, Foucault states that sovereignty and disciplinary mechanisms are two absolutely integral constituents of the general mechanism of power in modern society. This is what makes social control particularly efficient and pervasive in this historical time. It must be noted that Foucault tends to idealize the incomplete control, regulation, organization and disciplining of society in the pre-modern period and the spaces for solidarity and spontaneous rebellion that this created. Some writers even view him as being nostalgic for the relative absence of efficient control in the pre-modern era that contrasts sharply with the inexorable organization, discipline, and surveillance techniques of modernity.[25] To Foucault, popular solidarities were the target of disciplinary power. The modern society that succeeds in destroying them is one "in which the principle elements are no longer the community and public life but, on the one hand, private individuals, and on the other, the state."[26]

Insofar as the state is concerned, Foucault views it as one locus of disciplinary power in modern social systems. Consistent with his insistence on the decentered and deinstitutionalized view of power, Foucault maintains that the state -- as government apparatuses -- cannot occupy the whole field of power relations. To Foucault, power relations are not exclusively located in, nor do they emanate from, any one place in modern society. Therefore, unlike many of his contemporaries, Foucault does not characterize modernity by a state that penetrates society or by socioeconomic powers that penetrate and control the state. Rather, he sees modernity as constructed in terms of the penetration of each distinct realm by disciplinary technologies and strategies of power relations. However, some commentators regard the place of the state in Foucault's analysis of power relations as ambiguous. When questioned directly about this ambiguity, Foucault responds that the state, the economy, and society are three distinct elements within modern social systems, each of which has its power relations, disciplinary technologies and modes of functioning.[27]

For his own account, Foucault does admit that the state's interests play a central role in the globalization of disciplinary power in the modernizing societies of Western Europe. As a result of a demographic upswing and an increase in wealth (following the end to the plague and starvation) in the eighteenth century, the societal preoccupation with death was replaced by a concern with managing life and accumulating people. The state thus became

[25]Jean L. Cohen and Andrew Arato, *Civil Society and Political Theory* (Cambridge, Mass: MIT Press, 1992), 274.

[26]Michel Foucault, *Discipline and Punish*, 216.

[27]Michel Foucault, *Power/Knowledge*, 188.

interested in gathering information about and supervision of individuals in order to optimize the life utility of the population under its control. Foucault points out that it was the emerging centralized apparatus of public administration that began gathering "useful" information -- demographic data on births, deaths, health, crime, poverty, welfare and so on -- on an increasingly leveled population. In the process, the subject population was turned into objects of knowledge and power. This knowledge was clearly and intimately connected with the new form of disciplinary power, which put an end to the old, incalculable, and expensive personal forms of power of the absolutist regimes.

Apart from the control of the general population through regulation and disciplinary surveillance, Foucault also grants immense importance to the development of a centralized organization of the police. To Foucault, it is the state police who took over the previously fragmented functions of surveillance of criminality, economic and political supervision, who unify these into a single administrative machine to assure continuity of control. As he describes it, "the organization of the police in the eighteenth century sanctioned a generalization of the disciplines that became co-extensive with the state itself." The police, as a part of state apparatus, assume a major function to ensure that discipline reigns over society as a whole.

In the final analysis, however, Foucault's genealogical analysis of the rise of disciplinary society that accompanies modernity, and his relentless critique of power are prone to the same flaw that plagues the rest of postmodernist discourses. On the basis of his theoretical framework, Foucault is left with no conceptual means to describe resistance, particularly at the collective level, to the contemporary form of power relations as anything other than counter-strategies of power.[28] This is because he has equated any existing institutional, normative, or personal resources that could be mobilized for resistance with strategies of control. And since all subjects are seen as being constituted through power strategies and politics that pervade modern society, they cannot escape, nor can they articulate the forms of action that escape the logic of inegalitarian strategic power relations. The traditions, solidarities, and spaces for autonomous action left open by the inefficient, discontinuous modality of power in the pre-modern era find, in Foucault's work, no modern equivalents. To challenge the modern forms of domination, to which the technologies of

---

[28] It should be noted, however, that Foucault does insist that resistance exists. In his critique of power, he argues that there are no relations of power without resistance. But he just could not tell how it is possible, what it is for, and why it merits our support. See more in Jean L. Cohen and Andrew Arato, Civil Society, 290-298.

surveillance are central, subjects would have to operate on the level of individuals and without any norms, institutions, principles, or discourses to appeal to.

Foucault's lasting legacy: from the "Panoptic Sort" to the "Superpanopticon"

Several critiques of the "information society" thesis have followed Foucault's footstep in analyzing the negative side of the supposedly emerging social formation and of the forms of domination and stratification that it brings forth.   Kevin Robins and Frank Webster refer to Foucault's Panopticon as a metaphor to explicate the contemporary nature of social control that relies on the ability of state and corporate bureaucracies to collect, process, and share massive amounts of personal information. They emphasize the importance of ICTs in augmenting surveillance capacities and thereby the power of large organizations vis-a-vis individuals. With the ongoing "information revolution," Webster and Robins feel that the entire social totality "comes to function as the hierarchical and disciplinary Panoptic machine."[29]

In the same vein, Oscar Gandy coins the term the "panoptic sort" to describe a system of disciplinary surveillance in late twentieth century America, using substantial empirical evidence from the consumer market realm.   Gandy defines the "panoptic sort" as "a kind of high-tech, cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic or political value."[30] Although it is a highly discriminatory and undemocratic technology, the "panoptic sort" has become institutionalized in the US as well as in other advanced industrial countries that espouse democracy, especially as the so-called "information revolution" sweeps through these societies.   In this process, the "panoptic sort" has victimized the poor and underprivileged whose personal records may not meet the criteria of large organizations.   In the case of the US, a racial underclass such as blacks and hispanics is prone to experience the most damage from this mode of surveillance.

A similar view of how a database system may become a hidden stratifier of social and economic power is offered in Diana Gordon's analysis of the computerized criminal record

---

[29]Kevin Robins and Frank Webster, "Cybernetic Capitalism: Information, Technology, Everyday Life," in *The Political Economy of Information* , eds. Vincent Mosco and Janet Wasko (Madison: University of Wisconsin Press, 1988), 59.

[30]Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder: Westview Press, 1993).

system in the US, a system which she feels amounts to a real-life "Electronic Panopticon."[31] Due to the lack of regulation, and the techno-bureaucratic imperatives that propelled automation of data, the computerized criminal database system has grown, unabated and unnoticed by the general public, in its scope, size, and reach. The last dimension -- reach -- is the most crucial, according to Gordon, who questions the abuse of record dissemination, particularly in its use for unauthorized employment checks. Many employers, landlords, and insurers have reportedly gained unauthorized access, through informal contacts and briberies, to the database system and, as a result, turned down many millions of job applicants who have a registered record in the database. As the linkages between this surveillance system and other systems that mediate state-citizen relationship -- education, and public welfare -- become more expansive, the impacts felt by the poor and powerless will be tantamount to a societal Panopticon, one which has crossed the symbolic threshold to become operational according to Gordon.

In the contemporary context where hi-tech enhanced surveillance has become intensified, Reg Whitaker discusses the emergence of a "Participatory Panopticon." Because of the potential offered by new ICTs, this re-engineered Panopticon is rendering individuals "visible" to multiple gazes coming from different directions and looking for different things. This new mode of surveillance features a complex crisscrossing network of data collection and supervision of behavior since multiple surveillers can act in concert with, and share information with each other. Through electronic data processing and data matching, a unified and pervasive pattern of control by these surveillers can be achieved with diminishing need for a single central tower of control as was the case in the original Panopticon. Moreover, because the new Panopticon addresses or interpellates subjects on the basis of understanding their needs and serving their desires, people thus tend to participate voluntarily because they see positive benefits from participation. This participatory nature of the new surveillance thus makes it a much more powerful mechanism of control and consent than its predecessor -- state-centered surveillance. Because of its consensual characteristic, a participatory panopticon tends to engender less resistance than earlier forms of surveillance.[32]

---

[31]Diana Gordon, "The Electronic Panopticon: a Case-Study of the Development of the National Criminal Records System," *Politics and Society* 15 (1987): 483-511
[32]See Reg Whitaker, *The End of Privacy: How Total Surveillance Is Becoming a Reality* (New York: New Press, 1999), especially chapter 6.

On a more theoretical plane, Mark Poster, a post-modernist, proposes the concept of the "Superpanopticon" to theorize about the way electronically-mediated communication (or what he calls "the mode of information") reinforces systems of domination that are emerging in a postmodern society and culture. Poster's particular interest is in computer databases. To him, databases operate as a super-Panopticon. While it systematically and continuously collects information on people and composes it into profiles, it need not confine the people into a totalizing institution like a prison. People can go about their daily lives, and the computer will automatically pick up the traces that they leave behind and transform them into information for surveillance purposes. Despite its unobtrusiveness, the super-Panopticon is very efficient in normalizing its subjects since the characteristics of an individual subject as profiled in the database can be easily identified from unusual qualities, from credit ratings, criminal records to excessive traffic violations. As earlier discussed in Diana Gordon's case study of the criminal records database, these computer-drawn attributes can seriously affect the subject's life whether or not s/he is aware of it. Furthermore, with the advent of new ICTs, information in databases can be easily exchanged and flow in cyberspace to keep tabs on people across the globe.

Just as Foucault observes that the Panopticon constitutes the individual criminals as inmates, with the discourse/practice of discipline shaping their behaviors and attitudes, Poster claims that databases, or more precisely electronically mediated communication, constitute identities for each individual subject in a new configuration that may be termed "postmodern." He explains this as follows:

> Individuals are "known" to computer databases, have distinct "personalities" for them and in relation to which the computer "treats" them in programmed ways. ...In each case, the individual is acted upon in relation to his or her identity as it is constituted in the database. Simply because this identity has no intimate connection with the internal consciousness of the individual, with his or her self-defined attributes, in no way minimizes its force or effectiveness. With the dissemination of databases, a communication technology pervades the social space and multiplies the identity of individuals, regardless of their will, intention, feeling or cognition.[33]

In sum, Poster's overall proposition behind his theory of the "mode of information" is for social theorists to take a fresh new look at the way new ICTs have altered the nature of communication and "network of social relations" in the late twentieth century.[34] By

---

[33]Mark Poster, "The Mode of Information and Postmodernity," in *Communication Theory Today*, eds. David Crowley and David Mitchell (Stanford: Stanford University Press, 1994), 183.
[34]Mark Poster, *The Mode of Information: Poststructuralism and Social Context* (Cambridge: Polity,

incorporating this "linguistic turn" of post-structuralism in their accounts of social change, he feels social thinkers can open the prospect of understanding the subject as constituted in historically concrete configurations of discourse and practice rather than always privileging modernist notions like rationality. Although his contribution is not negligible for its heuristic value, Poster has also come under criticism for exhibiting a form of technological determinism, especially in his theory's tripartite history -- oralism, writings, and electronic exchange -- and his accorded primacy to information as heralding a new and fundamentally different type of society.[35]

Anthony Giddens: Surveillance and Structuration of Social System

To date, Anthony Giddens' contribution to the theory of surveillance and the state has been most explicit and recognized. Giddens' strength lies in his effort to synthesize elements drawn from different strands of social theory, in the process supplementing the pre-existing reductionism in these theories. Most notably, he elevates "surveillance," a rather obscure concept in social theory, to the level of institutional dimension of "modernity," alongside industrialism, capitalism, and the rise of the nation-state and warfare. While Giddens perceives surveillance to be most concentrated in the modern nation-state, of all types of states, he sees phenomena involving surveillance as intrinsic in any type of social system, regardless of historical time and geographical location.

In elaborating his centerpiece theory, the theory of structuration, Giddens talks about the generation of power in human society.[36] This process, he explains, occurs in and through structures of domination. Two major types of resources constitute the structures of domination -- authoritative resources and allocative resources. The former refers to resources involved in the capacity to exercise command over persons or the social world, while the latter refers to those involved in the command over objects or material phenomena.[37]

1990), 8.
[35]Frank Webster, *Theories of the Information Society* (London: Routledge, 1995) 188.
[36]See more in Anthony Giddens, *The Constitution of Society: Outline of the Theory of Structuration* (Cambridge: Polity Press, 1984).
[37]Anthony Giddens, *A Contemporary Critique of Historical Materialism: Vol. 1 Power, Property and the State* (Berkeley: University of California Press, 1981), 41

The generation of power through the control of these resources is inextricably linked with the articulation of time-space relations in social systems. Giddens is notable for his association of time-space relations with modernizing processes. The liberation of time and space or what he calls "time-space distanciation" is entirely a modern development. This is because in pre-modern social formations, most social relations are largely limited within the confines of immediate co-presence, and the ability of authority to stretch its administrative control is restrained by primitive means of transportation and communication. As Giddens puts it, in such societies there is a limited "storage capacity" for authoritative resources. The storage of authoritative resources involves above all *"the retention and control of information or knowledge."*[38] In this light, all modes of information storage are seen as "simultaneously forms of communication, cutting across the face-to-face communication that is exhaustive of human interaction in oral cultures."[39] In pre-modern or what he calls class-divided societies,[40] the primary mode of information storage is in the form of writing and notation. Writing marks a significant departure from non-literate tribal societies in which knowledge is stored through its incorporation in traditional practices including myth and story-telling. In tribal societies, the only storage "container" for such resources is the human memory. The time-space distanciation made possible by writing is thus much greater. Giddens describes the development of writing and its implications for surveillance activities in non-modern societies.

> Writing seems everywhere to have originated as direct mode of storage: as a means of recoding of information relevant to the administration of societies of an increasing scale.... The keeping of written "accounts" -- regularized information about persons, objects and events -- generates power that is unavailable in oral cultures. The list is the most elementary form of information coding, and therefore of information storing.[41]

The increased capacity for surveillance with the invention of writing pertains directly to the state. Writing, argues Giddens, provides a means of coding information, which can be used to expand the range of administrative control exercised by a state apparatus over both objects and persons, while storage of information allows for standardizing and coordinating. Although the keeping of detailed "official statistics," case histories and other quite exhaustive

[38]Anthony Giddens. "A Contemporary Critique of Historical Materialism: Vol. 1." 94.

[39]Anthony Giddens, *The Nation-state and Violence: Volume Two of a Contemporary Critique of Historical Materialism* (Berkeley: University of California Press, 1987) 14.

[40]While referring interchangeably with traditional society, Giddens defines "class-divided society as "a society in which there are classes, but where class analysis does not serve as a basis for identifying the basic structural principle of organization of that society." See more in Anthony Giddens. "A Contemporary Critique of Historical Materialism: Vol. 1 ." 7.

[41]Anthony Giddens, "The Nation-state and Violence." 95.

forms of documentation on the day-to-day lives of individuals did not become a common practice until after the rise of the modern state. Giddens confirms that the more diffuse versions can already be found in all types of traditional states. In this light, it is clear that Giddens' conception of surveillance is a modified version from Foucault. "Surveillance," in Giddens' writing, encompasses the idea that coded information can be used as a resource in the supervision of subordinates and collectivities even when the superordinate authority is distant in time-space.

While the development of writing as a primary technology for surveillance is significant to the rise of the traditional (non-modern) states, the invention of printing is a phenomenon as important to the formation of the so-called absolutist state.[42] According to Giddens, this state system, which arises in Western Europe between the seventeenth century and the mid-eighteenth century, marks a watershed that divides the then embryonic modern nation-state system from prior systems of rule. As far as the state apparatuses are concerned, the implication of printing for the enlargement of their administrative power is apparent. As Giddens explains,

> What printing made possible, and what it was increasingly used for during the phase of the consolidation of absolutism, was a very profound furtherance of the surveillance operations of the state. It was essential to the codification of law on which Weber rightly places so much stress.... But the sphere of law is only one area in which such changes can be observed. Records, reports and routine data collection become part of the day-to-day operation of the state, although of course not limited to it.[43]

During the period of the absolutist state, data gathering by the state is particularly concentrated in two areas -- 1) finance and taxation and 2) the keeping of population statistics. The latter is directly relevant to the preoccupation of the centralizing state with maintaining internal order with regard to rebellion and crime. In any case, the information collection and storage by the state in this period tends to be localized rather than centralized. It was not until the middle of the eighteenth century, also marking the movement from the absolutist to the modern nation-state in Western Europe, that the centralized collation and systematization of population information began to take form. According to Giddens, the

---

[42]Giddens explains the absolutist states as "hybrid compositions," which still retain large elements of the feudal order that preceded it and yet have characteristics that are generally associated with modernity. Among the "modern" elements emphasized by Giddens in the absolutist state are: the development of sovereignty; the formation of heightened bureaucratic centralism; the emergence of a guaranteed, centralized legal order; the formation of new modes of fiscal management, and a greater reliance on information for the reflexive monitoring of the state system.

[43]Anthony Giddens, "The Nation-state and Violence," 179.

official statistics that Western European states began to keep from the mid-eighteenth century onwards range over many sectors of social life and, for the first time, were detailed, systematic, and nearly complete. They include the centralized collation of materials registering births, marriages, death; statistics pertaining to residence, ethnic background, and occupation, as well as so-called "moral statistics," which relate to suicide, delinquency, divorce and so on.[44] This information base and the surveillance capacity it renders, argues Giddens, are the primary means of the modern nation-state's concentration of authoritative resources whereby the state's administrative power is generated.

In the nineteenth and early twentieth centuries, when the modern nation-state became more established in Western Europe, there was an ongoing effort to consolidate its administrative unity. According to Giddens, several factors were deeply involved in this process including 1)the mechanization of transportation; 2) the severance of communication from transportation by the invention of electronic media; and 3) the expansion of the "documentary" activities of the state -- involving an upsurge in the collection and collation of information devoted to administrative purposes. The second and third, says Giddens, have increasingly merged especially in the late twentieth century as a result of the growing sophistication of new technologies and the available electronic modes of recording -- tapes, records, discs, etc. The results are, as he describes,

> Administrative power now increasingly enters into the minutiae of daily life and the most intimate of personal actions and relationships. In an age more and more invaded by electronic modes of the storage, collation and dissemination of information, the possibilities of accumulating information relevant to the practice of government are almost endless.[45]

Besides discussing surveillance in terms of information storage and control, Giddens also stresses surveillance in terms of supervision of the activities of individuals. As far as the state is concerned, this form of surveillance is most clearly articulated as part of the process of "internal pacification." Although Giddens notes that "internal pacification" is inherent in any type of state system, he particularly focuses his attention on the processes of large-scale societal transformation which began unfolding along with the development of industrialism from the eighteenth century onwards. These processes involve several related phenomena, but all of which have to do with the progressive diminution of violence in the internal affairs of the modern nation-states.[46] Here, Giddens borrows heavily from

---

[44]Ibid., 180.
[45]Ibid., 309.
[46]Ibid., 181, 187.

Foucault's account of the rise of the disciplinary society in modernizing Western Europe with particular emphasis on two elements -- the replacement of violent forms of punishment with the establishment of the modern prison and the growth of the disciplinary power of state apparatuses. particularly in sanctioning those considered "deviant." This second element manifested in the policing of the routine activities of the mass of the population by specialized agencies separate from the main body of the armed forces.

In England, for instance, due to the growth of crime and processes of criminalization associated with urbanization and commercialization during the eighteenth century, the police force was organized as a professional and bureaucratized arm of the state. The formation of the new police, from a surveillance vantage point, represented a considerable improvement over traditional administrative and disciplinary mechanisms in which the state relied upon patronage arrangements and bribery of informants who reported on offenders, and contracts with private agencies to track felons. Modern policing, on the other hand, is a fully rationalized administrative organization, which employs a mixture of informational and supervisory elements of surveillance in their crime control endeavor. The more effective means of police surveillance, in conjunction with the sanctioning mechanisms of codified law and imprisonment, made "criminal" activities clearly distinct and provided a rational basis for the apprehension of offenders.

In his accounts, Giddens also warns against the use of surveillance in intensified policing which, he says, could lead to terror and totalitarian tendencies. Criminal suppression aside, such use of surveillance, which is often combined with the use of violence, is also found in contexts where subjects hold a "deviant" political view and need to be repressed, in the view of the state. In such instances, surveillance is clearly a key element of a totalitarian rule.[47] It must be noted that Giddens does not see totalitarianism as a characteristic of a certain type of state such as former Soviet-style or Eastern-European states, but instead as a *type of rule* -- as witnessed in Italian Fascism, Nazism, Stalinism, and Kampuchea during the Pol Pot regime.[48] All these totalitarian regimes, according to Giddens, exhibit characteristics of modern nation-states, although to a varying extent. By the same token, Giddens argues that there is no type of nation-state in the contemporary world which is completely immune from the potentiality of being subject to totalitarian rule.

"Totalitarianism," argues Giddens, only thrives in modern nation-states where the maximizing of surveillance, which, in combination with internal pacification, generates an administrative unity corresponding to definitive borders. It cannot exist in traditional states because these states' segmental character is incompatible with the necessary mobilization of concentrated resources. The ability of the state apparatuses to penetrate into the day-to-day activities of most of its subject population is a fundamental basis for the possibilities of totalitarian rule. In his words,

> Totalitarianism is, first of all, an extreme focusing of surveillance, devoted to the securing of political ends deemed by the state authorities to demand urgent political mobilization. Surveillance tends to become concentrated (a) in respect of a multiplication of modes of the documenting of the subject population by the state -- identity cards, permits of all sorts, and other kinds of official papers, have to be held by all members of the population and used to follow even the most ordinary of activities; and b) this is the basis of an

---

[47] According to Giddens, elements of totalitarian rule include the following:
1) focusing of surveillance in both dimensions -- a) information coding, documentation of activities of the population; and b) supervision of activities, intensified policing;
2) moral totalism: fate of the political community as embedded in the historicity of the people;
3) terror: maximizing of police power, allied to disposal of the means of waging industrialized war and sequestration; and
4) prominence of a leader figure: appropriation of power by leader depending not upon a professionalized military role, but the generation of mass support. Ibid., 303-304.
[48] Ibid., 302.

expanded supervision of those activities, carried out by the police or their agents.[49]

Although Giddens views the expansion of surveillance in the modern political order as conducive to political oppression and totalitarian rule, he, unlike Foucault, does not conclude that this maximized effect is characteristic of the general nature of administrative power within modern states. Totalitarianism is one end to which the exercise of administrative power may be put, but it is certainly not the only end, argues Giddens. In fact, he even sees Foucault as mistaken in his use of the panoptic metaphor to express the nature of power relations between the state authority and the governed population in the modern social system. According to Giddens, disciplinary surveillance, as epitomized in Foucault's panopticism, can only be realized in specialized locales where the use of techniques of surveillance are applied to subjects in an enclosed space and under a time-tabled arrangement. As far as state administration is concerned, the exercise of power is far more diffuse and there also exists what Giddens calls a "dialectic of control" that mitigates possibilities of totalitarian rule.

Dialectic of control and citizenship

Giddens' notion of a "dialectic of control" is another central concept in his theory of structuration, which deals specifically with the question of power relations between structure and agents in society.[50] According to this theory, structuration is seen as a process rather than a static framework. This is because "structured properties of social systems are simultaneously the medium and outcome of social acts,"[51] which "consist of social practices, situated in time-space, and organized in a skilled and knowledgeable fashion by human agents."[52] It is the knowledgeable agents who produce and reproduce the social system. Human beings, Giddens contends, are knowledgeable and will act on the basis of an understanding and analysis of circumstances and options which are available to them.

Giddens' emphasis on "knowledgeable agents" provides an entry point to the notion of "dialectic of control" in a power relation. All power relations in a social system, he says, can be regarded as relations of autonomy and dependence. But no matter how imbalanced

---

[49]Ibid., 303.
[50]According to Giddens, to be a human agent is to have power, to be able to "make a difference" in the world.
[51]Anthony Giddens, "A Contemporary Critique." 19.
[52]Ibid.

they may be in terms of power, actors in subordinate positions are never wholly dependent and are often very adept at converting whatever resources they possess into some degree of control over the system's conditions of reproduction. In other words, there is a "dialectic of control" in all social systems such that there are normally continually shifting balances of resources, altering the overall distribution of power.[53] Insofar as surveillance situations are concerned, knowledgeable agents can always find a way to answer back to their surveillers. hence making grounds for resistance.

In traditional or class-divided societies, Giddens explains the dialectic of control as a matter of "segmental autonomy." Since these types of societies had limited population dispersed into relatively self-sufficient agricultural communities, the level of interdependence between the political center and its subject population was thus relatively low. The local community was able to maintain a large amount of autonomy so long as certain obligations to the state were met. In other words, as there was no "government" in the modern sense, the administrative reach of state authorities was largely limited (low time-space distanciation), leaving the day-to-day life of the mass of people in the local communities more or less untouched. To sustain its administrative reach, the state apparatus in these types of societies tended to resort to threat or the use of military power.

By contrast, in modern nation-states the state's dependence upon the control of the means of violence as a medium of rule is relatively diminished as the build-up of administrative power becomes fortified through the more extensive means and modes of surveillance and the improved "storage" capacity. This development, argues Giddens, also opens way for a "dialectic of control" on the part of the subject population. In his words,

> The administrative power that depends upon the mobilization of social activities via the expansion of surveillance necessarily increases the reciprocal relations between those who govern and those who are governed. The more reciprocity is involved, the greater the possibilities the dialectic of control offers subordinate groups to influence the rulers.[54]

This "dialectic of control" can set off contingent conditions that might be counteractive to the operation of power by the ruler or the dominating force in society. Such contingent conditions are expressed in the modern nation-states most clearly in the struggle over three basic types of citizenship rights. Here, Giddens draws upon T. H.

---

[53]Anthony Giddens. *Central Problems in Social Theory: Action, Structure, and Contradiction in Social Analysis* (Berkeley: University of California Press, 1979), 145.
[54]Anthony Giddens. "The Nation-state and Violence," 202.

Marshall's account of the formation of three forms of citizenship rights -- civil right, political right and economic right -- as a point of departure.[55] Marshall's discussion, as Giddens points out, is explicitly focused on Britain and has quite limited relevance to other contexts other than as an exemplary case. While Marshall sees the three categories of citizenship rights as phases in the overall development of citizenship, Giddens suggests that these rights be viewed, particularly in the context of modern capitalist societies, as clustering in particular institutional sectors. Each institutional sector presents an arena of contestation or conflict, each linked to a distinctive type of surveillance that is both necessary to the power of superordinate groups and an axis for the operation of the dialectic of control by subordinate groups.

For instance, civil rights are focused on the relations between citizens and the policing authorities of the state. Surveillance in this context consists of the apparatus of judicial and punitive organizations whereby "deviant" conduct is controlled. While the law court is a prototypical institutionalized locale where "civil rights" can be defended and advanced, Giddens argues that the struggles over the form and bounds of policing may also take place in virtually all situations in which surveillance of this type is carried out including the secluded contexts of disciplinary power.

Political rights are generated in the context of relations between government and electorate. Surveillance in this context necessarily involves the collation and retention of information about the subject population by the administrative arms of the state bureaucracy. The parliament or council chamber may be the formal setting for the discursive representation of these rights, but Giddens suggests that a whole variety of extra-parliamentary contestations are also possible.

As for economic rights, these hinge on the relations between capital and labor particularly in business enterprises. Giddens suggests that the locale in which struggles over economic rights are focused is the work-place, the surveillance in question being that of "management" over a labor force. See Figure 1.1. In essence, Giddens urges us to view the three forms of citizenship rights as outlined by Marshall as double-edged and the aspects of surveillance associated thereto as having a Janus face. While the intensification of surveillance in each sphere promotes the consolidation of power in the hands of the dominant classes or elites, this process is also intimately connected with the actualization of citizenship

---

[55]See T. H. Marshall, *Class, Citizenship and Social Development* (Westport: Greenwood Press, 1973).

rights that set off conditions for the emergence of tendencies and pressures towards democratic participation. In the sphere of political rights, for instance, the surveillance operations conducted by the state -- the collection and keeping of information about the subject population -- can also be seen as the *sine qua non* of the realization of this right. The electoral process in a parliamentary democracy regime cannot be organized unless there is a substantial information base held by the state to identify each individual subject as a legitimate elector. Similarly, in welfare states, the provision of welfare or what Giddens considers as an extending of economic/social citizenship rights cannot be organized or funded unless there is a close and detailed monitoring of many characteristics of the lives of the population, whether or not they are actually welfare recipients.

Figure 1.1: Correspondence of types of rights, spheres of surveillance, and institutional locale of contestation

Types of rights	Type/sphere of surveillance	Institutionalized locale of contestation
Civil rights	Surveillance as policing	Law court, secluded contexts of disciplinary power
Political rights	Surveillance as stretching of state administrative power	Parliament, council chambers, extra-parliamentary activities
Economic rights	Surveillance as "management" of production	Work-place
Social rights[56]	Surveillance as monitoring of welfare processes	State administrative offices

Source: adapted from Anthony Giddens, The Nation-state and Violence Volume Two of a Contemporary Critique of Historical Materialism , 206.

In other words, the extension of citizenship rights in the modern nation-state has been dependent on the concentration of political authority. The allocation of equal rights to citizens presupposes the development of an agency above those individuals, as evidenced in the development of the extensive web of state bureaucracy. Similar to the notion of

---

[56]It should be noted that this type of right is particularly underdeveloped in Giddens' writings. In some writings social rights are themselves referred to as economic rights although in others they are not. See for instance, Anthony Giddens, *Profiles and Critiques in Social Theory* (London: Macmillan, 1982), chapter 12, Giddens, "The Nation-State," chapter 8, and an interesting critique in David Held, *Political Theory and the Modern State* (Stanford, Calif: Stanford University Press, 1989), chapter 7.

surveillance having a Janus-face, the modern bureaucracy ought to be viewed as having dual functions -- as a mode of public administration and as a means of surveillance.

As for the struggle for citizenship rights. Giddens argues that it be understood in the context of the expansion of state sovereignty and the ideological context of nationalism. The expansion of state sovereignty helps foster the identity of subjects as members of a political community or as citizens. Nationalism is a crucial force in the development of this new identity since it constitutes for the citizens a union between cultural diversity and concepts of a universal political organization. Cognizant of the fact that nationalism has frequently been fostered and manipulated by dominant groups to support their sectional interests, Giddens notes that the conditions involved in the creation of the modern state, as a "surveillance apparatus," are "the same as those that help generate nationalism."[57] Nationalism is closely linked to the administrative unification of the state and citizenship mediates this process.

In Giddens' assessment, class conflict has been the most important medium for the development of citizenship rights. Drawing on the experience in Western Europe, he points out how the forging of state sovereignty was a critical impetus to the struggle for rights and to the remoulding of citizenship. The increase in state administrative power led to the creation of new aspirations and demands and to the development of institutions which were responsive to them. For instance, the class conflict of the bourgeoisie in the eighteenth century against the remnants of feudal privilege led to the progressive freeing of the economy, and more generally civil society, from the direct political interference of the state through the establishment of civil and political rights. And the success of the working classes in the late nineteenth and twentieth centuries in struggling for social and economic rights produced the welfare state, which has helped ameliorate the worst consequences of the worker-citizen's lack of formal control of his or her activities in the work-place. These struggles for rights are intrinsically linked to distinctive types of surveillance and their dual nature.

---

[57] Anthony Giddens, "The Nation-State." 220.

In his book, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, Christopher Dandeker tries to synthesize different strands of social theory that deal with surveillance in modern capitalist states. One of the original contributions that came out of this endeavor was his mapping of typologies of bureaucratic surveillance systems. According to Dandeker, surveillance systems can be broadly analyzed in terms of two cross-cutting dimensions: 1) whether their capacities are rooted in informal personalized or formal bureaucratic administrative structures; and 2) whether those systems reproduce autocratic or liberal systems of rule. See Figure 2.

While the first dimension is quite self-explanatory, a few remarks may be helpful for the second dimension. Dandeker's main concern here is in the ways in which surveillance activities reproduce systems of rule. He stresses that a distinction needs to be drawn between *rule over* and *rule on behalf of* subject population. This is another way of distinguishing between ideal types of autocratic versus liberal principles of rule. The two regimes, argues Dandeker, differ necessarily in two important matters: 1) the degree to which the ruled can exercise supervision over rulers and their administrative staffs; and 2) the extent to which the prerogatives of rulers are concentrated so as to facilitate arbitrary rule.

In addition to the two cross-cutting axes, Dandeker also refers to a zone of "patronage" with transitional modes of surveillance located mid-way between personal and bureaucratic systems on the one hand and autocratic and liberal principles on the other. He defines patronage in two senses: 1) to refer to a social relation and 2) to a social system. Patronage relations are defined as durable, reciprocal relations of vertical or lop-sided friendship between a patron and a client, that can be identified in all societies.[58] In this sense, Dandeker feels that patronage is a universal feature of all bureaucratic organizations. The key issue here is whether patronage is the key strategic principle of organizational behavior. In other words, a society in which patronage relations play a strategic role can be identified as a patronage system. Dandeker defines this as complex, hierarchically organized chains of patronage relationships that provide the socio-economic and administrative basis of a system of rule. In this type of system, patronage also constitutes a means of surveillance.

---

[58]Patrons are generally those in a position to bestow favors by reason of their property and control of appointments, while clients are those who could claim to be friends and kinsmen of a patron. These claims, according to Dandeker, rest on property and personal connection, either directly with the patron or through the activity of a third party.

Figure 1.2: Different modes of surveillance in different systems of rule.

	Personal Administration		Bureaucratic Administration
Autocratic principles	Petty tyranny		Bureaucratic dictatorship
		Patronage	
Liberal principles	Direct democracy		Rational-legal bureaucracy

Source: Christopher Dandeker, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (New York: St. Martin's Press, 1990), 45.

In Figure 1.2 above, Dandeker distinguishes four modes of surveillance in ideal typical form. They are described as petty tyranny, direct democracy, bureaucratic dictatorship and rational-legal bureaucracy in addition to surveillance which falls within the zone of patronage. In the first two modes -- petty tyranny and direct democracy, the nature of surveillance is both personal and informal and is performed with little or no recourse to intermediate specialist officials. However, they differ significantly with regard to the underlying interests which the surveillance serves. In petty tyranny, surveillance is a means of sustaining autocratic power over a subject population by a single person. Based on personal capacities, however, the extension of information gathering and supervision is inherently limited to a local area and population. On the other hand, surveillance in direct democracies is carried out by all members of the collectivity in pursuit of popular interests. Dandeker points to the example of gossip networks as one method some communities use to ensure a degree of compliance with normative standards.

As for rational-legal bureaucracy and bureaucratic dictatorship, the modes of surveillance in these administrative systems reflect the broader institutional differences between capitalist and most state socialist societies. Major institutional points of contrast

28

amongst these systems concern: first, the availability of means for ensuring the accountability to the subject population for bureaucratic behavior; and second, the effective enforcement of a code of correct behavior on bureaucratic officials by the central authorities. This means ensuring that such officials apply an impersonal code to particular cases and that the possibilities for arbitrary behavior are minimized.

In bureaucratic dictatorships, neither the rulers nor the bureaucracy itself are accountable to the subject population as there are few established means of interest representation that would guarantee the accountability. Autocratic rulers, Dandeker notes, are likely to become in practice accountable only to the bureaucracy on which he or she depends for the maintenance of a system of rule rather than to the subject population. In cases of bureaucratic resistance, these rulers may resort to a strategy of patronage to manage the bureaucracy rather than adhering to a legal code or some form of formal rules. Meanwhile, the subject populations, who have few means of guaranteeing bureaucratic accountability to themselves, "have only the choice of accepting arbitrary behavior or joining in the patronage game of bribery and corruption in order to divert scarce organizational resources their way."[59]

By contrast, in surveillance systems that help reproduce rational-legal bureaucracies, both ruler and bureaucracy are accountable effectively to the subject population. They also adhere to a widely held ethic of acceptable bureaucratic behavior in administering the population. The ethic is enshrined in the legal and wider value system and secured through liberal structures of interest representation.

According to Dandeker, the contrast laid out between the two systems of rule and the corresponding systems of surveillance is an ideal-typical one. It is a way of contrasting different ways in which surveillance reproduces different systems of rule in different types of society -- liberal capitalist, state socialist, and authoritarian capitalist. Dandeker's view is that the organizations of modernity in the West have managed to come closer to approximating the ideal type of rational-legal bureaucracy than their equivalents in state socialist societies have managed to do so far.

With respect to the last mode of surveillance which falls within the zone of patronage, Dandeker outlines two important structural features of a patronage system. First, there is a

---

[59]Christopher Dandeker, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (New York: St. Martin's Press, 1990), 50.

dominance of hierarchical vertical relations over horizontal relations of social solidarity. Secondly, the voluntary formation of personalized ties has the effect of inhibiting the formation of inherited forms of power holding.

According to Dandeker, the existence of vertical relations between patrons and clients in a deferential social hierarchy dilutes the social significance of class or status forms of horizontal solidarity as well as undermining the potential legitimacy of egalitarian forms of ideology. While communal, status, or class actions do exist, their salience as a means of group mobilization and integration has been weakened by patronage ties and loyalties.

Meanwhile, the voluntary nature of the formation of personal ties between patrons and clients has a generalized effect of undermining the emergence of stable, hereditary structures of power holding. Because of this voluntarism, clients are neither owned nor totally controlled. They can therefore shift their client loyalties or have multiple patrons, hence figuring themselves as a significant resource and dynamic in the system. At the same time, patrons who position themselves as entrepreneurs can compete for clients and in this way do not need to be members of a hereditary status nor disciplined bureaucratic subordinates of a ruler to enjoy economic and political power.

Dandeker sees societies based on a patronage system as associated mainly with transitional phases in state development and the wider process of modernization. Patronage, he claims, provides the administrative basis of systems of rule in the following circumstances:

> where political integration and social mediation are limited by the weakness of market forces and the ineffectiveness of central government. ... It emerges to facilitate economic and political relationships where the personal ties of kinship are no longer effective and the integrative and distributional effects of the market and rational-legal state cannot operate.[60]

Although Dandeker's classification of modes of surveillance according to systems of rule may be illustrative and convenient for labelling purposes, in reality there are bound to be clear overlaps among these categories. Considering that all societies are dynamic and constantly changing, it will be difficult to pigeonhole any society and any system of surveillance neatly and snugly into one of these categories. In addition, Dandeker seems to imply that rational-legal bureaucracies and their associated modes of surveillance are less

---

[60]Christopher Dandeker, "Surveillance, Power and Modernity," 47.

likely to produce arbitrary behaviors and thereby domination of the subordinate population. This idea essentially reverses the central argument of scores of critical theorists that rationalization usually entails domination. Dandeker's idea of "rational" apparently reflects a fundamentally liberal understanding and partiality. While he may be right in identifying important organizational and institutional characteristics that are associated with each system of rule and surveillance, Dandeker seems to lose sight of other factors -- technical, geographical, and cultural -- that may be more forceful in shaping the functioning of systems of surveillance in any given society.

INFORMATIZATION, MODERNIZATION
AND IMPLICATIONS FOR SURVEILLANCE

A great deal has been written on the "information society" thesis with a central argument that a new social formation centering on information and ICTs is superseding the current industrial era in highly industrialized countries. Scholarly writings first set the trend by pointing to increases in information work and a greater availability of professional occupations as marking a distinctive break between industrial and "post-industrial" societies.[61] This post-industrial society, which is also seen as "an information society," is argued to be "a major feature of the twenty-first century in the social structures of the United States, Japan, the Soviet Union, and Western Europe."[62] It is also regarded as a superior form of society, one at a higher stage of development than its predecessors. Subsequently, a number of national policy studies on the same theme were launched,[63] in addition to a succession of works in the scholarly and popular discourses.[64] The mainstream argument usually advocates massive informatization of all sectors of society, associating this process

[61]See, for example, Daniel Bell, *The Coming of Post-industrial Society: A Venture in Social Forecasting* (New York: Basic Books, 1973). Marc Uri Porat, "Global Implications of the Information Society," *Journal of Communication* 28 (1, 1978): 70-80. Daniel Bell, "The Social Framework of the Information Society" in *The Computer Age: A Twenty- Year View*, eds. Michael L. Dertouzos and Joel Moses (Cambridge, MA: MIT Press, 1979). Yoneji Masuda, *The Information Society as Post-Industrial Society* (Washington, DC: World Future Society, 1981).

[62]Daniel Bell, "The Coming of," x.

[63]For example, Simon Nora and Alain Minc, *The Computerization of Society* (Cambridge: MIT Press, 1981). and Science Council of Canada, *Planning Now for an Information Society: Tomorrow is Too Late* (Ottawa: Science Council of Canada, 1982)

[64]See, for example, James Martin, *The Wired Society* (New Jersey: Prentice Hall, 1978); Simon Valaskakis, *The Information Society: the Issue and the Choices* (Montreal: Gamma, 1979); Anthony G. Oettinger, "Information Resources: Knowledge and Power in the 21st Century," *Science* 209 (1980): 191-198; Alvin Toffler, *The Third Wave* (New York: Morrow, 1980); W.P. Dizard, *The Coming Information Age* (New York: Longman, 1982); Tom Stonier, *The Wealth of Information* (London: Methuen, 1983) and Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge: Harvard University Press, 1983), among others.

with beneficial social and economic transformations while ignoring adverse impacts. The optimistic claims regarding the social implications of the "information revolution" are based solely on the properties of the new technologies. and little attempt is made to explore the significance of ICTs in terms of their genealogy.

However, a more nuanced interpretation sees the emergent information society as a struggle to overcome crises of control in manufacturing and transportation during the nineteenth and twentieth centuries. The development of new ICTs is considered part of the technological efforts -- or the "control revolution" -- to increase efficiency in production, distribution, and consumption through rationalized control of information.[65]

In a related vein, the ascendance of information and ICTs is seen by a group of French intellectuals as an integral part of a structural change in capitalism. This change is described as a transitional process from one regime of capitalist accumulation to another -- from Fordism to post-Fordism.[66] Fordism was the dominant regime of accumulation during the post-war years until about 1973. Its distinguishing features include mass production of goods, mass consumption, the predominance of industrial workers in employment, the nation-state as the locus of economic activity, and social welfare programs.[67] The ongoing globalization process, which was propelled mainly by the expansion of multinational corporations, is said to have brought Fordism to its downfall . The emerging regime of accumulation, which is generally identified as post-Fordism, has ICTs at its core. Because of their "time-space compression" character, ICTs are essential to the acceleration of the turnover time of capital -- one of the keys to capitalist profitability -- in production, distribution, and consumption in the new regime of accumulation.[68]

[65]See more in James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press, 1992).

[66]See. for instance. Michel Aglietta, *A Theory of Capitalist Regulation* (London: New Left Books. 1979). and David Harvey, *The Condition of Postmodernity: an Enquiry into the Origins of Cultural Change* (Oxford: Blackwell. 1989).

[67]The regime was named after Henry Ford because he was the pioneer of mass production techniques which allowed the manufacture of goods at a price that could encourage mass consumption. Ford was also credited for having initiated the payment of reasonably high wages in order to secure worker compliance with the discipline required to work the highly-productive assembly-line system. and to provide them with sufficient income and leisure time to purchase the mass-produced products.

[68]For instance, automation and robotics cut down production time, while new organizational forms like Just-in-Time inventory delivery system help eliminate unnecessary stock. Moreover, ICTs are also said to be enabling capitalism to become a more tightly organized system through dispersal, geographical mobility, and flexible response in labor markets. See more in David Harvey. *The Condition of Postmodernity.* 159.

Gradually, the mainstream notion about a post-industrial information society as the next stage of development spread worldwide as transnational corporations made their global presence felt and the emergent "globalization" process gained momentum. In the case of the so-called Third World, several writings emerged that argue for an integration of "developing countries" into the "new world information economy"[69] or the "global information society."[70] Viewing technology as the prime social dynamic, works under these currents usually urge Third World societies to speed up the diffusion of ICTs and informatization of their societies so that any opportunities opened up by this new "technological revolution" will not be missed.[71] While this technological determinist undertone may sound peculiarly familiar, few works have explicitly linked it to another equally dominant theoretical project which posits a fundamentally similar argument about development, that is, the modernization paradigm.

In a nutshell, the "modernization paradigm" features a dominant world view and conceptual model of social change based on the idea of material progress, science, technology, and a set of institutional arrangements associated with modern (Western) society and/or industrial civilization. Although its root can be traced back to the Enlightenment with initial institutionalization in Western Europe, this model of social change has spread internationally through colonialism and imperialism and has influenced the course of development of countries worldwide. Ever since the period following World War II, the social engineering project to "modernize" the so-called Third World countries became even more intensified. International organizations together with political elites and technocrats in the Third World were engaging in the transfer of technology to Third World countries to bring about higher productivity and expanded provision of "basic needs," which are taken to be indicators of a better "quality of life." Such a transfer, it is argued, has to be facilitated by other forms of institutional and structural change. For instance, the process of state-building, which generally refers to the expansion of state power conjointly with the introduction of parliamentary and democratic institutions, and the inculcation of a particular set of development-enhancing "modern" (western) values and ideas among the people of traditional societies.[72]

---

[69]Martin Carnoy, Manuel Castells, Stephen S. Cohen, and Fernando Henrique Cardoso, *The New Global Economy in the Information Age: Reflections on Our Changing World* (University Park, PA: Pennsylvania State University Press, 1993), 6

[70]Yoneji Masuda, "The Global Information Society," in *Information Technology: Impact on the Way of Life*, ed. Liam Bannon, Ursula Barry, and Olay Holst (Dublin: Tycooly International, 1982).

[71]Manuel Castells, "The Informational Economy and the New International Division of Labor," in Martin Carnoy et al (eds.), *The New Global Economy in the Information Age*, 27.

[72]Tariq Banuri, "Development and the Politics of Knowledge: a Critical Interpretation of the Social Role of

As far as the information and communication realm is concerned, the modernization paradigm promotes mass media, both the conduit and the content, as powerful agents of modernization. Through the introduction of mass media, traditional societies are said to become stimulated and diffused with values and institutions that are favorable to achieving a "superior" stage of development after the Western model.[73] In other words, static societies of the Third World are seen as brought to life by the injection of "modern" values and ideas such as equality, mobility, innovation, and consumption which together will engender positive change.

The unbounded and largely unquestioned optimism of the modernization paradigm began to subside in the 1970s in the face of the extremely uneven record of development, rising poverty and unemployment, political tension and conflict, and increasing ecological disasters associated with development projects in many Third World countries. This period is also a watershed when the "information economy/society" thesis began its circulation in the US, Japan, and Western Europe before reaching its height in the early 1980s. By the mid-1980s, a worldwide recession following the oil crisis left a large number of Third World scholars, particularly those working in Latin America and Africa, disillusioned with the modernization paradigm.[74] Their discontent had to do with the paradigm's epistemological assumption of a universal linear model of social change, its underlying western ethnocentrism, its preoccupation with economic growth, and its promotion of market capitalism at the expense of social equity. In the area of communication, the widely promoted notion linking mass media with modernization has also been criticized as failing to stimulate a real process of development other than boosting people's consumption appetite and aspirations for a "western life-style."[75] In other words, a direct causal relationship

Modernization," in *Dominating Knowledge: Development, Culture, and Resistance*, ed. Frederique Apffel Marglin and Stephen Marglin (Oxford: Clarendon, 1990), 29.

[73]For works which support this assumption, see, for example, Daniel Lerner and L.W. Pevsner, *The Passing of Traditional Societies: Modernizing the Middle East* (New York: Free Press, 1958); Everett Rogers, *Diffusion of Innovations* (New York: Free Press, 1962); Ithiel de Sola Pool "Communication and Development," in *Modernization: the Dynamics of Growth*, ed. M. Weiner (Washington, DC: Voice of America, 1966); and Wilbur Schramm, *Mass Media and National Development* (Paris: UNESCO, 1979). Lerner is primarily concerned with individual value and attitude change, while Rogers is more interested in the process of diffusion and adaptation of innovations. On the other hand, Pool and Schramm's main inquiry has to do with the relationship between mass communication and modernization practices and institutions.

[74]See for example, A. G. Frank, *Reflections on the Economic Crisis* (New York: Monthly Review Press, 1981), and Tariq Banuri, "Development and the politics of knowledge: a critical interpretation of the social role of modernization," in *Dominating Knowledge: Development, Culture, and Resistance*, eds. Frederique Apffel Marglin and Stephen Marglin, (Oxford: Clarendon, 1990).

[75]The mass media and modernization paradigm has also been criticized as a whole or partially by several researchers. Aside from its empirical discrepancy, the other main points of criticisms include: positivist-behaviorist assumptions about linear rational sequence of change; ethnocentric (Western) approach to assess

between mass media campaigns and actual economic take-off or social betterment has been found not to exist in practice.[76]

While the basis of the "modernization paradigm" has been challenged by critics in light of the Latin American and African experiences. anomalies appeared in Asia that may have contributed to the continued influence of the paradigm, although in a modified version, into the next decade. The anomalous "Asian tigers," or the famous East Asian newly-industrialized countries (NICs) -- Hong Kong, South Korea, Taiwan and Singapore and the near NICs -- Indonesia, Malaysia and Thailand -- seemed to confirm the assumptions of the modernization paradigm. These countries and the East Asian region in general had experienced, until recently, three decades of economic growth, averaging almost eight per cent (or 5.5 per cent per capita) a year.[77] Relying mainly on economic criteria, the World Bank in the early 1990s presented these countries as exemplars of development -- "miracle" models of economies to be emulated.[78]

Swept by the enormous progress in ICTs and the worldwide currents promoting informatization, the East Asian NICs stood next in line after highly industrialized countries to adopt the "information economy/society" thesis for their macro-economic policy framework. Singapore, for instance, identified ICTs as a potential niche industry in 1980 and developed its highly coordinated National Information Technology Plan (NITP) throughout that decade to become one of the world's leading computer software developers by the mid-1990s.[79] This type of success has been capitalized upon by technocratic international organizations to promote the diffusion of ICTs and, thereby, the circulation of the "information society" thesis in developing countries. Not foreseeing the current economic recession in Asia that began in mid-1997, a 1996 World Bank publication attributes the economic expansion of Japan and the four East Asian NICs to their ability to exploit the opportunities made possible by the information revolution.[80]

Third World circumstances: and static and ahistorical expectation that communication processes take place in the Third World in a stable social system, devoid of conflict. See, for example, Jan Servaes, "Communication and Development for Whom and for What?," paper presented at the International Association for Mass Communication Research (IAMCR), Prague, 27-31 August 1984.

[76]M. Isabel Valdés, "Third World Countries and Conflicting Ideologies in the Information Age," in *The Ideology of the Information Age*, ed. Jennifer D. Slack and F. Fejes (norwood, NJ: Ablex), 1987), 203.

[77]Staff writers, "East Asian Economies Survey: Tigers Adrift," *The Economist*, 7 March 1998, 4.

[78]World Bank, *The East Asian Miracle: Economic Growth and Public Policy* (Oxford: Oxford University Press, 1993).

[79]See, for example, Wong Seng Hon. "Exploiting Information Technology: a Case Study of Singapore," *World Development* 20, vol. 12 (1992): 1817-1818.

[80]Nagy Hanna et al, "The East Asian Miracle and Information," 2.

Through their dominant access to the Third World's public policy community, international organizations such as the World Bank and the UN have played a prominent role in promoting the linkage between ICTs and development. This support has been ongoing since even before the "information economy/society" idea began to circulate widely in countries of the South. One study claims that it was actually in one of the United Nations' forums in the 1960s that the Third World was introduced to the euphoric ideas about the role of ICTs in development under the umbrella of the "modernization paradigm."[81] A United Nations (UN) report in this period was quoted as saying:

> Thus an ever accelerating communication revolution is taking place in the world today, as much in developing nations as in the developed ones, but to some degree the developing nations are not reaping the full advantages. The UN in its planning for the second "Development Decade" should reaffirm the high priority that must be given to the development of communication facilities for developing nations.[82]

As for the World Bank, besides its research facility, this powerful international organization has also helped spur the "information economy/society" thesis in the Third World through its lending activity. Since the early 1970s, the Bank began to look more carefully at the ICT sector as part of the Third World state's requisite development infrastructure. It already envisioned "telecommunication networks functioning...as the central nervous systems of complex societies, transmitting information and commands between their various parts."[83] Through its advisory and lending capacity, the Bank has guided "the developing World" in the direction of extensive telecommunications development, and its guidance has been taken seriously by most "developing" countries worldwide. According to one study, the World Bank is able to exert a great amount of influence over developing countries because its stamp of loan approval is an indispensable credit rating for Third World governments wishing to avail themselves of other sources of loans and of transnational trade and investment.[84] Over the past decade, the World Bank's lending activity for ICTs projects has become highly prioritized. In the 1960s the Bank's support for Third World telecommunications constituted a mere three per cent of its total lending. By 1998, the Bank's lending for ICTs was growing at six times the rate of

[81]M. Isabel Valdés, "Third World Countries and," 208.
[82]Ithiel de Sola Pool, Philip Stone, and Alexander Szalai, *Communications, Computer and Automation for Development* (New York: United Nations, 1971), UNITAR Report No. 6, R/RR. 6.
[83]World Bank, *Telecommunications Sector working paper* (Washington DC: World Bank, 1971), 5.
[84]Gerald Sussman, "The World Bank in the Philippines," in *Transnational Communication: Wiring the Third World*, eds. Gerald Sussman and John A. Lent (London: Sage, 1991), 45.

expansion of total Bank lending, with Asia being the region with the second largest volume of lending for ICTs after Eastern Europe.

The linkage between the modernization paradigm and the "information economy/society" thesis is not only found in historical evidence; the connection between the two projects is also ideological. Evidently, the underlying linear technological determinist model of change and the ideological perception of development as a race that one needs to rush into are red threads that run through both the "mass media and modernization paradigm" and the "information economy/society" thesis. The resemblance is so uncanny that the latter is deemed a re-emergence of the former. As Gerald Sussman and John A. Lent note,

> The ideology of contemporary American (technological) "diffusionists" varies little from that of the earlier "modernizers," the prime difference being perhaps a somewhat more circumspect attitude toward the cultural impact of mass media transfers, without being less effusively supportive of the spread of capitalism and technology to the Third World -- and no more critical of the self-serving political economic agenda of U.S. assistance programs. Other differences are that earlier modernizers were social scientists pushing radio and television in the Third World, while contemporary diffusionists are predominantly technocrats uncritically extolling the virtues of computers and satellites.[85]

Implicit in this ideology, of course, is the endorsement of a convergence theory of development that sees all societies as set on the same developmental journey in this case to the post-industrial stage. This theory ignores, or at least makes subordinate to its rationalization of social change, differences in politics, culture, and history.

Although a number of critiques have emerged to counteract the strong currents promoting informatization in the Third World, there has been virtually no mention of problems of rising surveillance as a result of ICTs use in personal data-collection and in the monitoring of people. Most critiques focus on an international level of conflict by raising questions about the possibility of heightened technological dependency and new dimensions of North-South domination as a result of the application of ICTs. Those that concentrate on a local level of analysis usually draw out the political character of ICTs and the imbalance in public access to the new technologies.

That surveillance or privacy intrusion by means of ICTs is not perceived to be a problem in the Third World is not entirely surprising. At the most basic level, the

---

[85]Gerald Sussman and John A. Lent. (eds.). *Transnational Communication: Wiring the Third World*, 16-17.

problem can be conceptual. Privacy, as I shall later argue, is a loaded concept and the political aspect of the term -- private rights against holders of authority or other members of society -- has strong philosophical roots in western liberal democracy with the emphasis on individualism, limited government, and the like. With the cultural and political variations of societies in the Third World, it is highly likely that these Western nuances of privacy or its converse, surveillance, may not be perceived in the same way.

On a more theoretical plane, the predominance in the Third World of the modernization paradigm and, subsequently, the information society thesis may partially account for the lack of interest in these issues. A good entry point to consider surveillance in the modernization paradigm would be in modernization theory's subdiscipline of "political development" theory. This theoretical strand is concerned with the issues of state-building in the "developing world." It generally advocates a progress towards the "superior" Western political institutions as characterized by electoral democracy, professional bureaucracies, pluralist associations and acceptance of abstract political rights. In order for Third World countries to achieve such political development, a major prescriptive content of this theory is the advice to strengthen the institutions of the state or, in Gunnar Myrdal's term, to increase the "hardness" of the state.[86] According to Myrdal, most Asian states, with the exception of China and Japan, have "soft" states -- meaning the absence of "social discipline" necessary for modernization. In keeping with the general trend of modernization theory and its preoccupation with economic effects, Myrdal sees a "hard" state, or political stability, as a prerequisite for effective execution of macro-economic growth-oriented policies.

In essence, the process of state-building or state-hardening involves the establishment of institutions that help "expand" the level of power in a society, as well as increase the legitimacy of its exercise. Expansion of power requires the strengthening of bureaucratic machinery through technological efficiency and methods, as well as rationalized processes in staff selection and training. Legitimization of power requires an acceptance of the exercise of state power by the populace either by expanded public participation or by elite dominance, depending on the specific circumstances of each country. Evidently, we can see the elements of "surveillance" at work in both processes, which are reminiscent of Max Weber's analysis of rationalization of administration. The strengthening of bureaucratic machinery will most likely require large-scale surveillance of citizens as part of the bureaucracy's collation of facts and knowledge about the populace. Meanwhile,

---

[86]Gunnar Myrdal, "The Beam in Our Eyes," in *Asian Drama: an Inquiry into the Wealth of Nations* (Harmondsworth: Penguin Books, 1968), 5-35.

legitimization of state power may entail an extreme focusing of surveillance as found in authoritarian regimes or surveillance of eligible voters as present in democratic regimes.

In any case, just as large-scale state "surveillance" is seen by Western social theorists as a product of modernity, the same notion is also implicated in the process of political development or modernization of the state in the Third World. The highly linear view of political development notwithstanding, the integration of "surveillance" as a constituent element of rapid modernization may overshadow its constraining faces and the authoritarian inclination or purposes to which it may be put. In the context of most of the Third World where participation in civic or political affairs does not necessarily increase with the establishment of the nation-state, there is also bound to be fewer and less ineffectual mechanisms to question and counterbalance this aspect of state power.

In the case of the information society thesis, or what I consider to be "the modernization paradigm with an information turn," the problem of surveillance is likely to be bracketed even more. The much-advocated process of informatization of society would definitely involve an expansion of bureaucratization through automation of record-keeping in both the public and private sectors. While this movement has provoked public interest in privacy protection in several highly industrialized countries, such may not always be the case in Third World countries due in part to lower sensitivity towards surveillance schemes in some cultural contexts. Besides, privacy concerns are likely to be overridden by forceful technocratic arguments about the coming of the "information age," the promise of tremendous economic and social benefits, and the increased efficiency in public services which comes with computerization. As far as the policy elites and bureaucratic officials are concerned, increased surveillance is not likely to strike them as a major concern. Their preoccupation lies more in promoting the diffusion of ICTs under claims that it will foster national development and promote industrialization rather than in limiting their use in any way. Although the implications of surveillance can be multi-faceted, these are likely to be perceived as intangible when compared with the obvious potential benefits that informatization processes can render.

CONCLUSION
INSTITUTIONAL ANALYSIS AS ANALYTICAL FRAMEWORK
FOR SURVEILLANCE IN A THAI SETTING

Although I limited the scope of analysis in this first part of the study to surveillance in the realms of state administration and policing, I deliberately cast the net as widely as possible when searching for a suitable analytical framework. The extensive review of the theoretical insights above is testament to such an approach. These theoretical sources have helped me to construct an understanding of "surveillance" as a means of social control for a cross-cultural setting like Thai society.

Weber's obvious strength lies in his discussion of surveillance as an administrative basis in any given social system of rule and as an integral part in the process of rationalization of a modern state. Even more illuminating is his linking of this rationalization process with an embedded structure of domination that is concealed under the technocratic promise of increased efficiency. Understanding "surveillance" in this light makes sense since it captures historical patterns across many, if not most, societies. It also does not necessarily limit the explanation of surveillance to only one logic, as does Marxist perspective on surveillance.[87] To understand a complex process of rationalization, Weberians argue that "one must examine each situation in its own right to discover its nature and consequences in that location."[88]

As for Foucault, his idea of the "Panopticon" has contributed to the sense of disciplinary power that is inherently a part of the operation of surveillance. Many writers have alluded to it as a powerful metaphorical resource for representing several contemporary practices of information collection and use, focusing especially on the normalizing of individuals' behavior. Foucault's description of the way power is inscribed in panoptic scenarios seems to have a universal appeal and it will be interesting to see if this is applicable to the ensuing analysis of surveillance in the Thai state-society sphere.

---

[87]According to David Lyon and Elia Zureik, for instance, the Marxian perspective on surveillance always connects the process with the capitalist drive for greater profit. Weberians, on the other hand, insist that surveillance is part of the processes of rationalization that characterize the development of modern organizations -- capitalist firms as much as government bureaucracy. Therefore, the whole process could not be reduced to having an economic logic alone. David Lyon and Elia Zureik, eds. *Computers, Surveillance and Privacy* (Minneapolis: University of Minnesota Press, 1996), 6.
[88]Ibid., 7.

Meanwhile, Anthony Giddens' theory of structuration plays a crucial part in shaping the direction of analysis in this study. According to Oscar Gandy, "the theory of structuration provides a useful analytical framework through which one might begin to examine the relations between entities in a way that does not deny the possibility of assessing the nature of influence or power within those relations."[89] This is because the concept of structuration, as mentioned, implies a dynamic rather than a static vision of influence. It also involves the crucial idea of the expansion of social relations across the dimensions of time and space and the way that this "time-space distanciation" may influence the extent of social control. Correspondingly, the notions of "knowledgeable agents" and "dialectic of control" show that the agency of individual human beings is accentuated as opposed to that of institutional structure. These concepts broaden the horizon for resistance from something Foucault only hints at and invite efforts by students of surveillance to demonstrate their empirical relevance. In addition, his insistence upon the "janus-face" of surveillance -- both its enabling and constraining features -- is also useful for assessing the possibilities of surveillance in a given social setting.

Apart from their analytical potential, the reviewed analytical insights also acknowledge the importance of history. Following this trend, I have designed an analytical framework that is highly historical in nature. This historical reflection is necessary for a definition of society and culture that centers on the presence of groups and individuals and their participation in the process of producing and reproducing a social system. The Weberian approach, which is also adopted by Giddens, directs the research to institutional factors that influence the development of surveillance systems throughout the extensive history of the Thai state. While concurring that information and technology may have taken on a special significance in the modern era, I, following Giddens, maintain that the central feature of the present is its continuities with the past. So the emphasis that traditionally has been given to the revolutionary character of technological change in analyses of information practices is reduced. Technological change is treated in this study as an integral part of the larger social, economic, and political system.

In addition, key ideas and concepts, including the outlined dimensions of surveillance, rationalization, the Panopticon, the "dialectic of control," and the typologies of surveillance system, are used to explore the growth of surveillance, the resistance it may

---

[89]Oscar Gandy. "The Panoptic Sort." 11.

invoke, as well as to chart the political and cultural significance of this growth and resistance in different periods of Thai history.

As for the literature on the modernization paradigm and the information society thesis, they serve as an ideological context for a contemporary analysis of surveillance in this study. The case studies which follow the extensive historical analysis suggest that Thailand, in its aspiration for industrialization and economic expansion, has pursued a widespread informatization of the society by using the public sector as a model for the diffusion of new ICTs. The influence of this technocratic thinking and action is examined in light of the growth of electronic surveillance in public administration and the growing interactions between public and private sector surveillance.

Combined together, these analytical concepts and arguments give rise to an institutional analysis that recognizes that the means and modes of surveillance as well as the information requirements of political and economic systems are changing in directions that are not without historical and ideological precedents. By studying selected government institutions, their incentives, and their structural relationships to the citizens via information practices, this approach facilitates examination of dynamic changes in that relationship and provides a foundation for a critical analysis that is applicable for Thai society and comparable setting.

CHAPTER 2

STATE SURVEILLANCE IN TRADITIONAL THAILAND
(1350 - 1905)

This chapter provides the history and development of state surveillance systems in Thailand (or Siam at the time) prior to the first wave of modernization between the mid-nineteenth and early twentieth centuries.[1] This history spans more than five centuries of Thai history. Although prior ancient communities are believed to have been dominated by people of Thai descent, this historical analysis will begin with the kingdom of Ayutthaya (1350-1767), which is widely regarded by scholars of Thai studies as the cradle of Thai civilization. The analysis covers the 417 years of the Ayutthaya period, the brief Thon Buri (1767-1782) period and a good part of the early Rattanakosin (Bangkok) period (1782-1905).

Prior to examining the characteristics of state surveillance and the types of resistance invoked by it in this pre-modern period, it is important to first understand the nature of the social structure and the social relations which shaped the regime of social control. "Surveillance" is treated in this study as a core technology of social control, one that enables the restructuring of social systems -- traditional and modern -- and their expansion over a larger range of space and time than that of tribal cultures.[2] Surveillance is also seen as a process that cannot be adequately understood by one conceptual logic or by detaching it from its historical and social context. Since each society has important particularities, it is crucial that one examine each social situation in its own right to discover its nature and consequences for the exercise of state surveillance. Therefore, in the following historical analyses, in this chapter as well as the next two, the same architecture of discussion will be used. A brief sketch of the social structure, state-society relations, economy, and system of state administration in each historical period will be provided before delving into the account of state surveillance systems that were in use and the resistance they invoked in that period. As will be demonstrated, the two accounts are inextricably linked. Without an understanding of the characteristic of power relations in Thai society in any given period, one would not be able to decipher the existence of a "dialectic of control" in surveillance situations. This "dialectic of control," I argue, is exhibited through the way in which the subject populations

---

[1]Thailand was called Siam up until 1959 when a nationalist government changed its name to Thailand to signify the superiority of the Thai ethnicity over others. In this chapter, I will use both Thailand and Siam interchangeably.

[2]Anthony Giddens, *The Nation-State and Violence* , 2.

"answer back" to their "surveillers" who seek to control information about them and to supervise their conduct based on that information.[3]

The information contained in this chapter, as well as the next, which concerns state surveillance systems during the early modernizing years, is gathered primarily from archives and secondary reviews of existing literature. Some anecdotal evidence and special insights were obtained from interviews with experts in related fields.

THE AYUTTHAYA PERIOD (1350-1767)

For 417 years the kingdom of Ayutthaya was the dominant power in the fertile Chao Phraya river basin. The kingdom was named after its capital -- Ayutthaya, which grew to be one of Southeast Asia's most renowned metropolises in that period. The early Ayutthaya kingdom was by no means a single kingdom. It comprised a number of city states with one dominant city state, Ayutthaya. Other city states, after being conquered by the many Ayutthaya warrior kings, became tributaries of Ayutthaya. The history of Ayutthaya was filled with warfare with its neighbors, particularly Burma, Ayutthaya's powerful neighbor to the west. Burmese power fluctuated in cycles reflecting levels of administrative efficiency in the control of manpower. Whenever Burma was in an expansionist mode, Ayutthaya suffered. In 1569, Ayutthaya was defeated, initiating a decade of subjection to the Burmese. In 1669, a capable Thai king named King Naresuan emerged to declare Ayutthaya's independence, defeat the Burmese, and reclaim the lost territory. During the 18th century, war again disrupted relations between the two kingdoms. In 1767, after a 15-month siege, Ayutthaya finally succumbed to the Burmese, who sacked and burnt the city, putting an end to one of the most politically powerful and culturally influential epochs in Thai history.

Like other traditional societies in Southeast Asia, Ayutthaya thrived mainly on agriculture and on the richness of natural resources that yielded forest, tin and other mineral products. At the base of the economy were self-sufficient, and self-contained villages. Exchange of goods was done mainly by barter. In the early Ayutthaya period, internal trade was limited, and monetary exchange was not fully developed. Even so, the village economy bore direct relation to the state as a tax unit. State extraction was mainly in the form of

---

[3]David Lyon and Elia Zureik , eds. *Computers, Surveillance and Privacy* , 8.

forced levies of produce and corvée labor. Although the productive capacities of Ayutthaya were most likely at a lower level than those in England or France during the same historical period, Ayutthaya was still considered to be a remarkably prosperous kingdom by many European visitors. According to one account,

> The Dominion and revenue of the crown is great, amounting yearly to many millions, arising out of in-land commodities as rice, sappang, tin, lead, salt, petu; as also the profits of the Sand and Mountain Gold, which are only sold by the Kings Factors to foreign Merchants.[4]

The kingdom's prosperity is indeed something to wonder about considering that humanpower was scarce[5] and that the location of the villages in the kingdom was very scattered, making centralized taxation and payment of tributes from the hinterlands difficult. Some scholars attribute the exceptional productivity of Ayutthaya to the predominant *sakdina* social organization system which was consolidated in 1454.[6] This system, it is argued, enabled the ruling class of aristocrats to effectively extract surplus-product from the peasantry, both for their own consumption and for submission to the prosperous royal reserve. Although extensive accounts have been written on *sakdina* and its social and political implications, there remains a lot of ambiguity and controversy over the interpretation of *sakdina*. Many historians argue that *sakdina* emerged as a land allocation scheme and a means of social classification based on royally bestowed titles and royally designated usufruct rights on land. Marxist historians, who belong to this group, also see *sakdina* as a mode of production which made possible class exploitation in the Ayutthaya period and beyond. Other historians, less concerned about class exploitation, see it simply as an elaborated means of control of manpower on the basis of the hierarchical structure of the land/social status allocation scheme.

It would be beyond the scope of this study to elaborate extensively the complexities of the *sakdina* system and its evolution over time. Nonetheless, it is essential to discuss some salient aspects of the system and its development, given its profound and long-lasting implications even in the modern era. Prior to delving into *sakdina* itself, it is important to

---

[4] CR Boxer, ed., *A True Description of the Mighty Kingdoms of Japan and Siam* (Amsterdam: N. Israel, 1971), 25.

[5] According to La Loubère, a French ambassador to Ayutthaya in 1688, the kingdom rolls listed 1.9 million *phrais* (commoners) which did not include old men, women, children, slaves and corvée evaders. Virginia Thompson, *Thailand: the New Siam* (New York: Macmillan, 1941), 320.

[6] See, for example, Kevin Hewison, The Structure of *Sakdina* Society and the Emergence of Capitalism in Thailand prior to 1932, *Bankers and Bureaucrats: Capital and the Role of the State in Thailand.* Monograph Series 24 (Yale University: Southeast Asia Studies, 1989).

shed some light on a more fundamental social organization and manpower control system that gave rise to the consolidation of the *sakdina* system. This system is referred to in this study as the *mun nai- phrai* system.

The mun nai-phrai system

Phrai refer to all male commoners aged between 18 and 70 years old and taller than 125 centimeters.[7] Women and children were counted as *phrai*'s dependents and were the ones who actually had to provide for means of subsistence when *phrai* were recruited for corvée labor or to fight in wars. The earliest reference to *phrai* is said to be in a famous Ramkhamhaeng inscription of the preceding Sukhothai period, dated around 1292 A.D.[8]

The social structure in the Ayutthaya period was divided into four classes -- the king and the princes of royal blood; aristocrats; freemen commoners or *phrai* ; and slaves or *that*. Each group of *phrai* (commoners) was controlled by a leader, called *mun nai* (noble). They were princes and aristocratic officials. *Phrai* were required by law to be enlisted under a *mun nai* in return for legal protection. A clause in the Law on Litigation, dated 1356, decreed: "Do not accept any litigation put forward by a citizen who has no *mun nai*."[9]

During its early period, the Ayutthaya kingdom was vulnerable to war. Since there was no standing army at the time, this forced labor system provided the necessary soldiers. The *mun nai* were charged with responsibility for furnishing as many men under their control as required by the king. If they failed to do so, for whatever reason, they would be penalized.[10] During the early Ayutthaya period, this forced labor system was also employed to recruit labor for government corvée duties such as building and repairing palaces and temples.

---

[7] Sirilak Sakkriengkrai. The Economic System in the Ayuddhaya Period. ed. Chatthip Nartsupha and Sompop Manarangsan, *The Economic History of Thailand Until 2484 B.E.* (Bangkok: Thammasart University Press. 1984), 35.

[8] Sukhothai is regarded by Thai historical tradition as the first Thai kingdom which lasted from the 13th to 15th century. The most famous king of this period was Ramkhamhaeng. Much of what is known about Sukhothai in the 13th century derives from King Ramkhamhaeng's stone inscription.

[9] Law on Litigation (*Phra aiyakan rapphong*). article 10, Law of the Three Seals (*kotmai trasamduang*) quoted in Chatchai Panananon. "*Phrai*, Neither Free nor Bonded." *Asian Review* 2 (1988): 1-23.

[10] According to the Decree concerning Punishment for Crimes against the Government (*phra aiyakan laksana acha lung*). dated 1352. if a *mun nai* was found taking bribes from his *phrai* and not recruiting them for that reason. the *mun nai* was subject to eight types of punishment. Ibid., 2.

Laws dated before 1454 reveal that two types of *phrai* existed – *phrai luang and phrai som*. *Phrai luang* were *phrai* attached to the king while *phrai som* were *phrai* attached to the nobles. An observation was also made that *phrai luang* were those commoners who failed to register under a *mun nai* when they were mobilized to fight in war.[11] As a result, these people were deemed as criminals, and when they were arrested, they were made *phrai luang* who had to do government corvée labor for six months in a year.[12] But since the king could not personally control them himself, he thus assigned this task to the *mun nai*. Nevertheless, *phrai luang* were not supposed to be attached to the *mun nai*. *Phrai som*, on the other hand, were fixed to the *mun nai*. All *phrai* were different from *that* (slaves) since they had the right to select the nobles with whom they wanted to be enlisted.[13] *That*, on the other hand, were more directly bound to their *mun nai* through slavery or debt-bondage and owed all of their labor to their *nai*. Yet, mobility out of the *phrai* status was difficult except for a few rare cases when *phrai* who were capable warriors were promoted into a low nobility status during wartime. In times of peace, such opportunities appear to have been very limited because of the rigidity of the social structure.[14]

Much historical evidence suggests that the life of *phrai luang*, particularly in the later Ayutthaya period was harsher and more burdensome than that of *phrai som*. Unlike the latter, *phrai luang* were required to do corvée for six months each in alternating months.[15] Although *phrai som* could also be recruited for government corvée, they primarily took turns and worked in shorter shifts for their *mun nai*, thus allowing them more independent time to earn a living. When *phrai luang* went to do their corvée service, they also had to bring their own tools and their own food. As most *phrai* were farming peasants, the time lost for farming due to the forced corvée obviously wreaked havoc on their paddy cultivation, which was the source of their own subsistence and the taxes to be paid to the nobles. It was thus common for *phrai luang* to seek ways to avoid corvée or to avoid being enlisted as *phrai luang* altogether. Since all *phrai luang* had to be have their names entered into registration rolls, many *phrai* used all sorts of subterfuges to avoid this procedure. Some nobles, aware of the *phrai*'s reluctance, took advantage of the situation. Many laws in the later Ayutthaya

[11] Similarly, Kachorn argues that *phrai luang* originated from those stray *phrai* who had no *mun nai*. See Kachorn Sukphanit. *Status of Commoners (Thanandorn Phrai)* (Bangkok: Khurusapha, 1962), 28.

[12] Akin Rabibhadana. The Organization of Thai Society in the Early Bangkok Period (1782-1873), ed. Clark D. Neher, *Modern Thai Politics: from Village to Nation* (Cambridge: Schenkman, 1976), 41.

[13] Kachorn. *"Status."* 38-39.

[14] In the Ayutthaya period, there was a regulation that limited the types of people who could become government officials to only those from noble family background. See more in Akin, "The Organization," 45.

[15] Corvée duties ranged from building and repairing palaces and temples to craft making, farming royal land, and soldiering.

period imply that officials accepted bribes from *phrai* to drop their names from the registration rolls by not listing their names at all, by keeping them as their own *phrai som*, by switching them to other groups that had lighter duty, or by registering them as pseudo *that*.[16] Such relationships between the *mun nai* and *phrai* began to grow and gradually formed a dominant patron-client relationship that increasingly threatened the king's political power. For those *phrai* who could not get cooperation from the *mun nai*, they also had the option of running away to another town, hiding in the wilderness, becoming a monk, or selling themselves as *that*. Neither *that* nor monks were subject to corvée. In the late Ayutthaya period, when trade with foreign merchants became more widespread, *phrai* were allowed to pay a commutation fee in lieu of corvée service. The fee could be in the form of money or rare items that could be sold as exports.[17] *Phrai* who chose to pay in money and produce were called *phrai suai*.

The sakdina system

Sakdina literally means "the power of control over the rice field." Put most simply, it is a system of status ranking based on royally-bestowed *usufruct* rights to *use* the king's land and enjoy its *fruits* but not to own it, sell it, or damage it. In return for their service to the king, the nobles would be given elaborate titles with numerical ranks of *sakdina* attached thereto.[18] For example, royal aristocracy were each allotted a *sakdina* rank up to 100,000; high-ranking government officials were allotted *sakdina* of 400 - 10,000; and lower nobility -- 50-300. *Phrai* were also designated a *sakdina* of 25 while *that* did not have any *sakdina*. There are various interpretations as to what the numerical ranking actually referred to. The most common version would regard it as the amount of field land one is entitled to as the literal meaning of the word *sakdina* suggests. A similar interpretation sees it as signifying the maximum limits on the number of *rai* one *might* hold,[19] but not the actual total of land allotted.[20] Other more recent writings on *sakdina* argue that the number attached

---

[16] See more in Chatchai, "*Phrai*, " 12. According to Chatchai, the term pseudo *that* is used to designate a practice by which a patron and a client mutually agreed that the client would be registered as a phony *that* of the patron to avoid government corvée. In this agreement the client might have to bribe the patron in one form or another.

[17] It is believed that monetary commutation began since the reign of King Narai (1656-1688) which saw the peak of trade and when money became widely used to replace barter exchange.

[18] In *sakdina* society, the king claimed to be the sole owner of all land, though in practice he granted usufruct right on the land to the princes and the nobles who were at his service.

[19] One rai equals 0.4 acre or 0.16 hectare.

[20] Damrong Rachanuphap. Prince. *Ancient Administration of Siam (Lak sana kan pokkrong prathet siam tae boran* (Bangkok, 1927).

to the *sakdina* title had nothing to do with land holdings. Instead, it was simply a means of classifying people on a numerical scale signifying the scope of rights, duties, and privileges that each person was entitled to as well as one's standing in any social interaction.[21]

Social classification aside, more recent writings on *sakdina*, regardless of theoretical grounding and academic disciplines, commonly view it as a means of control of scarce humanpower, which was a more important resource than land and the actual basis for political and economic power in this period. It is argued, for instance, that the original intent of King Trailok in 1454 in establishing the *sakdina* system was not merely to devise a scale of social hierarchy but to impose a clear limit to the appropriate political and economic power of the nobles. By 1454, the Ayutthaya kingdom had been evolving for more than a century and many of the higher-status *mun nai* would likely have accumulated considerable wealth and power from the control of their *phrai*. Some could well have posed a threat to the king. By systematizing *sakdina*, these nobles were endowed with elaborate titles, usufruct right over land, and the right to control a number of *phrai* in correlation with the amount of their *sakdina*. As there were no salaries or other material rewards in this period, *sakdina* was deemed a type of compensation for the nobles' service in controlling the *phrai* and in channelling the taxes generated by the *phrai* to the royal reserve. Since the nobles lived mainly on the material support and services rendered them by the *phrai* under their control. they would suffer a significant loss if this privilege were withdrawn. Thus, through his power of *sakdina* appointment, the king derived security from his power to deprive any *mun nai* suspected of being disloyal to him. In addition, the king also derived legitimacy, through the erection of *sakdina*, to monitor the size of the manpower under the control of each noble.

As a famous local historian Akin Rabibhadana aptly notes, the lack of manpower has played a prominent role in the development of Thai social and political organization, as it has in the histories of other countries in mainland Southeast Asia. Like the rest of the golden peninsula, Ayutthaya was sparsely populated. Land was not a problem for there were plenty of jungles, which one could turn into cultivated paddy fields. The real issue was the control of manpower. In the absence of technology, labor power was vital for cultivation and public construction. Of even more significance was the need to control manpower for self-defense in time of war and as the base of political power in time of peace. Not only did the control of

---

[21] Historians holding such view include Busakorn Karnchanacharee, Kukrit Pramoj, and Kachorn Sukpanich. For more details, see Pornpirom Iamtham, "*Phrai* during the Ayutthaya Period," ed. Chatthip Nartsupha and Sompop Manarangsan, *The Economic History of Thailand Until 2484 B.E. (prawatsart settakit thai chontheung pho sor 2484)* (Bangkok: Thammasart University Press, 1984), 74.

manpower relate closely to the possession of wealth, the amount of manpower possessed by an individual also indicated the extent of one's political power. Under the prevailing patron-client structure, *phrai* under a *mun nai* had the duty to obey the *mun nai'* s command and the *mun nai* therefore could use them for his own political ends. It should come as no surprise, then, that any ruling king felt the need to ensure that *phrai luang* always outnumbered *phrai som*. Several laws passed in the Ayutthaya period indicate the kings' effort to boost the number of *phrai luang* vis-a-vis *phrai som*.[22] There were at least two times in Ayutthaya history when the imbalance in the number of *phrai* caused two kings to be dethroned. In fact, the fall of Ayutthaya in 1767 was widely attributed to the weakened power of the king due to the heavy loss of *phrai luang* and the existence of groups of informal clients and patrons, who were ready to turn into factions fighting against each other at any time. Thus they could not mount a cohesive resistance to outside attack.

<div align="center">

STATE SURVEILLANCE AND RESISTANCE
DURING THE AYUTTHAYA PERIOD

</div>

Registration of *phrai* is said to have begun in the early Ayutthaya period (1350-1569).[23] For the purpose of mobilization, all *phrai* were required to register under a *mun nai* -- a prince or a government official. Each town appeared to have had a registrar, who held the roster of *phrai* of the town. This registration process must have been quite poorly handled considering that the administrative structure of government in this early period was not very unified. It was in the reign of King Trailok when the administrative reform and the *sakdina* system were introduced, that a more systematic form of civil registration was conducted.[24] It is important to note that this reform featured an attempt to centralize the administration by turning various existing tributary states into towns and cities of different ranking and by sending out the king's brothers and sons to rule these new towns and cities. At the center, the basic unit of administration was the *krom* (department or a central

---

[22] For example, a law was passed which made the children from a *phrai luang - phrai som* couple automatically *phrai luang*. Another law indicated that when a noble with *phrai som* died, all his *phrai* became *phrai luang*. During the reign of King Narai, monks were required to be tested on their religious knowledge and were forced to become phrai *luang* if they failed.

[23] Akin, "The Organization," 41.

[24] Prior to the reform, the early Ayutthaya kingdom comprised a number of city-states with one dominant city-state, Ayutthaya. Other city-states such as Suphanburi, Lopburi, and Phitsanulok, were tributaries to Ayutthaya. The rulers of these tributary states were more or less autonomous, and there was a significant accumulation of manpower under these rulers. Whenever Ayutthaya showed signs of weakness, especially at times of succession, when there were splits among those nobles controlling manpower, a ruler of one of the stronger city-states would move his troops to Ayutthaya and attempt to take over the city.

<div align="center">

50

</div>

government body). Four large *krom* – *wiang* (city). *wang* (palace), *khlang* (treasury), and *na* (fields) were dominant. The whole structure was divided into military and civil sections whose affairs were later taken up by two even more powerful grand ministers -- the *mahatthai* (interior) *and the kalahom.* (defense). All nobles – princes and officials – were supposed to be attached to a *krom* and so were their *phrai*, who would be assigned to the same *krom* as their *mun nai.* Therefore, each *krom* would have a registrar, who was in charge of registering all nobles and their *phrai.* The basic premise was that all people had a duty to serve the king in return for *sakdina*, in the case of the nobles, and for legal protection, in the case of the *phrai.* Evidently, in introducing this reform, King Trailok was attempting to ensure Ayutthaya's, and thereby his, domination by the use of kinship obligations as well as manipulation of manpower through a more systematic means of surveillance.

While this administrative reform and the erection of *sakdina* should have consolidated the throne's stability, in practice the control of distribution of manpower was anything but smooth. Even after the reform, the nobles were found to be concealing the number of *phrai luang* under their designated control and to have turned some *phrai luang* into *phrai som* for their own personal use. Thus, in the reign of King Ramathibodi II (1491-1529), a law was passed which established a new administrative unit and new approaches of surveillance to improve the control of *phrai luang.* In 1527, the so-called *krom phra surasawadee* or Registration Department was set up and assigned the task of carrying out a population survey and keeping tally on the entire populace of commoners in the kingdom.[25] Each *krom* thus handed over its *phrai luang* registration and record-keeping task to the Registration Department instead. The Registration Department was divided into three major sections – the central registration, the right registration, and the left registration. The central registration section oversaw record-keeping and registration in the metropolis -- Ayutthaya and the inner-circle cities -- those adjacent former city-states. The right registration section was responsible for the cities and towns in the North of the kingdom, and the left registration section was in charge of the southern towns and cities.[26]

The Registration Department operated somewhat like the modern Census Bureau as their designated registrars would be dispatched to and stationed in major cities and towns to undertake the registration. The registration record not only included information on each *phrai luang* -- name, location, and the *krom* that the *phrai* was assigned to -- but also

---

[25] See more in Pornpirom. *"Phrai* ." 54; and Kachorn. "Status." 19.
[26] Ibid.

51

information on their family members. If there was incongruity in the information on the *phrai* and their family members – different location of residences or different *krom*, for instance, the registrar was required to verify the fact with the other registrars who oversaw the registration in different locations. Should there be evidence suggesting that *phrai* under investigation had escaped from their assigned *krom* or their supposed location of origin, the *phrai* would be subject to penalty. Those for whom there was no prior record, meaning they had escaped registration before, would also be punished. Capital punishment involving the infliction of severe pain was in use during Ayutthaya. According to the penal code in the Ayutthaya Law of the Three Seals, six penal categories were outlined in order of severity:[27]

1) execution by cutting off the head with a sword;

2) inflicting body pain by cutting off legs and hands, plucking eyeballs, cutting off tongue;

3) lancing and tattooing bodies and faces, and displaying punished bodies to the public;

4) chaining, putting into stocks and pillary;

5) fine and expropriation of wealth; and

6) probation and imprisonment.

Aside from keeping a record on each *phrai luang*, the registrars were also assigned the task of tattooing a certain mark on each *phrai luang*'s wrist to signify their status. *Phrai luang* assigned to different *krom* would be tattooed with a different mark or sets of marks. Their tattooed wrists not only branded *phrai luang* as different from *phrai som* and the unmarked nobles but also made it more difficult for *phrai luang* to escape compulsory corvée and for their *mun nai* to extort them for his own benefit. In effect, these measures were meant to boost the power of the king to control his manpower.

Different interpretations exist regarding the intentions behind the introduction of the new registration system by King Ramathibodi II. According to an interpretation by Prince Damrong-rachanuphap, the so-called father of Thai historical studies, the establishment of the Registration Department and the introduction of wrist tattooing were the first effort in Thai history to create a systematic process for military conscription.[28] While King Trailok was concerned with civil registration, King Ramathibodi II, argues Prince Damrong, was more preoccupied with military registration and drafting. With the centralized control of *phrai luang* records in all *krom*, the Registration Department would be able to mobilize

---

[27]Ibid.
[28] Ibid., 449.

manpower, even at short notice, for soldiering and for other official functions. The recruit order would be issued from the Registration Department to all concerned *krom*, which would in turn do the recruitment as required. On the other hand, another noted local historian, Kachorn Sukpanich, looked at the law enforcing the new record-keeping approach and the wrist tattooing with some misgiving. To Kachorn, King Ramathibodi's new surveillance approach had disturbing repercussions for the populace at large. In his words,

> After less than 200 years since the beginning of the Ayutthaya kingdom, the people's freedom of mobility had become very limited. If one was born in a certain town, then one had to settle there for the rest of his life. To move and settle somewhere else would be a crime....it seemed that the convenience of the state (in mobilizing manpower) overrode the people's freedom of mobility.[29]

Historical evidence shows that the registration of *phrai* continued throughout the Ayutthaya period, both for military and corvée purposes. La Loubère, a French envoy who stayed in Ayutthaya during the years 1687-1688, recorded the following observation:

> The *Siamese* people is a Militia, where every particular person is registered: They are all Soldiers, in Siamese *tahan*, and do all owe six months service annually to their Prince...And as the Prince never employs all his Subjects in his Armies, and that often times he sends no Army into the Field, though he be at War with some of his neighbors, yet for six months in the year he employs in such a service as pleases him, those Subjects which he employs not in the War. Wherefore, to the end that no person may escape the personal service of the Prince, there is kept an exact account of the people.[30]

La Loubère also noted that although monks and women were not required to perform corvée, they were still required to register. Children born to *phrai luang* would also continue to be *phrai luang*. Boys were registered under the same *krom* as their fathers once they reached the required age of registration.

About half a century after La Loubère's observations, the controls on *phrai* became even more stringent, the reason being the king's heavy loss of *phrai luang* and his concerns for political stability. In the reign of King Baromakot (1732-1758), a population survey was carried out every 10 years to keep the *phrai* 's rosters as up to date as possible. Aside from the increased frequency, the survey also involved generating detailed information on the *phrai* to prevent escape, fraud, and other possible abuses as a result of the prevailing

---

[29] Kachorn. "Status." 20.

[30] Simon de la Loubère, *The Kingdom of Siam*, trans. A.P. Geun. R.S.S. (Kuala Lumpur: Oxford University Press, 1969), 78.

clientelist relations between the *mun nai* and their *phrai*. Each *phrai*'s record in this survey included the following fields of information:

appearance: height, skin color, complexion, and build;

names: of the *phrai* as well as of parents, spouse, and children;

status: alive, dead, insane, or escaped.

For those *phrai* who died, went insane, or escaped, it was required that the date and time of such incidents be recorded in detail. Each record was also required to be stamped by four different officials to maximize reliability. [31]

This new population registration law, which was passed in 1733, also introduced changes in the organization of responsibility for record keeping for different kinds of *phrai*. *Phrai luang* continued to be enlisted with the Registration Department, while the registration of *phrai som* remained under the care of their *mun nai* . For those *phrai* in the remote towns and provinces, the *krom kalahom* (defense) and *mahatthai* (interior) would be the caretaker of their records. During this reign, another law was also passed in 1748 which imposed a high penalty on *phrai luang* who escaped from their corvée and became enlisted as *phrai som*. According to this law, the *mun nai* were also instructed to look into the record of each *phrai* who asked to be enlisted as their subordinate *(phrai som)* before admitting any newcomer. The nobles were indeed told to look into the family history and the *krom* that the *phrai* and their ancestors were registered under. If the *phrai* turned out to be a *phrai luang*, the *mun nai* was required to submit him/her to the authority of the *krom* that the *phrai* was originally assigned to. Otherwise, the *mun nai* would also be liable and subject to penalty.[32]

In the face of this rather tight and centralized administrative control of the state, there were fewer rebellions staged by the *phrai* than in many other feudal societies. Historical evidence indicates there were only three violent uprising by *phrai* during the entire 417 years of Ayutthaya rule. The movements failed to obtain in any concessions from the ruling groups -- the royal court and the aristocrats. Many more smaller unrecorded uprisings might have also taken place. According to another local historian Pompirom Iamtham, the *phrai*'s seeming acceptance of the ruler's oppressive control was attributed to two main reasons, one being belief in the Buddhist concept of *karma*. Since the law of *karma* describes people's lives as contingent upon or predetermined by deeds done in a past life, believers tend to

---

[31] Pompirom,"*Phrai*," 54; Kachorn. "Status," 25.
[32]Ibid., 29.

54

docilely accept the existing social hierarchy without challenge. Moreover, with the abundance of natural resources and small population, the *phrai* were far from destitute despite the various means of exploitation and extraction by the *mun nai*. [33]

In any case, the stringent and centralized control of the *sakdina* system and the mandatory corvée are widely regarded by contemporary Thai historians as one of the root causes of backwardness and lack of innovation in ancient Siam. *Phrai*, who formed the majority of the population, were discouraged from developing, let alone exhibiting, their skills and craftsmanship for fear that they would be subject to even more exploitation by the *nai*. Likewise, any path to innovation was inhibited by this fear of additional exploitation. Besides, since *phrai* were required to pay a large amount of taxes, which were channeled by the *mun nai* to the royal court, they were technically too preoccupied with rural farming to do anything else during their time free from corvée.

THE THONBURI – EARLY RATTANAKOSIN PERIOD (1768 - 1905)

The Thonburi period – reconstruction and mandatory tattooing for all phrai (1767-1782)

Towards the end of the Ayutthaya period, it is quite clear that the corvée labor system, which was required of all *phrai luang*, was undermined by various devices to avoid corvée and subterfuges to avoid being registered as *phrai luang*. As a result, Ayutthaya's manpower organization system was deficient and poorly organized. Facing the massive Burmese invasion in 1765-1767, this situation and the existence of political factions very likely contributed to Ayutthaya's downfall. King Taksin, who was responsible for expelling the Burmese and moving the capital to Thonburi, must have learnt this lesson from Ayutthaya's collapse. [34] Faced with the shortage of labor after the wars with Burma, he took steps to rectify the corvée system. During this period, manpower was crucial both for military and rebuilding purposes so there was a need for an effective means to keep track of all the *phrai*. In a law passed in 1774, the king mandated that every adult male be tattooed on the wrist with his name, name of the town where he resided, and the name of the *mun nai*

---

[33]Pornpirom,"*Phrai*," 63, 67.

[34] Since Ayutthaya was completely destroyed by the Burmese, King Taksin chose to establish Thonburi, a small town situated near the mouth of the Chao Phraya river, as the new capital.

with whom he was registered.[35] The same law also imposed a high penalty on those who attempted tattooing frauds either by faking a tattoo or by stealing the official device to do the tattooing themselves. Those who were charged with this crime would be executed along with all their relatives and living ancestors.[36] In addition, all *phrai*, both *phrai luang* and *phrai som*, were required to provide corvée service of six months out of the year. This requirement of six-month service caused much discontent among the *phrai*, the majority of whom were peasants. They found it most difficult to farm effectively under such conditions.

The pre-modern Rattanakosin (Bangkok) period (1782-1905) -- a period of continuity and change and manpower reform

The organization of Thai society during the early years of the Bangkok kingdom was not fundamentally different from that of the late Ayutthaya period. Emphasis was still placed on manpower control and on an extensive system of political and social patronage. In fact, the early Bangkok rulers were trying to rebuild the social structure of the Ayutthaya era. The forced corvée labor, which had caused *phrai* so much suffering during the Ayutthaya period, was still practiced although some changes had been introduced. In the first reign of the new Chakkri dynasties, King Rama I (1782-1809) reduced the required corvée time from six months to four months, thus allowing the *phrai* more free time to do their rice farming.[37] Similarly, Rama II eased the corvée burden further to only three months, freeing up nine months for the *phrai*.[38] The reduction in corvée was due to a number of factors that will be discussed below. It did not mean, however, that control on labor had been relaxed. On the contrary, systems for registering *phrai* were tightened and wrist tattooing continued until the late nineteenth century.

From the second quarter of the nineteenth century, the foundations of the Rattanakosin economy and society began to experience a major shift. Indeed, the nineteenth century was a period of important transition in Thai history. The changes and continuities in this period culminated in the great reform of King Chulalongkorn, which not only formally

---

[35] Chatchai, "*Phrai*," 13, Kachorn, "Status," 30-31.

[36] Ibid., 31.

[37] After annexing power from King Taksin in 1782, Rama I founded the Chakkri dynasty and established Bangkok or Rattanakosin as the capital of the new Siamese kingdom. There have been nine kings of the Chakkri dynasty including the present one, Bhumibhol Adulyadej.

[38] Under this new corvée arrangement, *phrai* were required to work for one month, and be free for the next two months, then return to work another month, before going off the corvée again. The arrangement introduced by Rama II followed the same cyclical basis except that the *phrai* got three months off instead of two.

launched Thailand on a modernization path but also liberated the *phrai* to become citizens and ended the traditional means and modes of surveillance on all commoners.

The most important change, which had profound economic and social impacts on the organization of labor in this period and on Thai social structure in the century beyond, was the influx of Chinese immigrants beginning in the 1800s.[39] To meet the shortage of labor outside agriculture, the Thai state, particularly the kings, encouraged Chinese immigration.[40] Unlike the Thai peasants, the Chinese immigrants were exempt from the corvée and other forms of bondage although they did have to pay a light poll tax.[41] There had been since the late Ayutthaya period a number of Chinese immigrants who acted as merchants, tax-farmers, officials and small traders. Many also worked as coolies and were increasingly sought after in this period for public works. For such ventures as canal digging, there was a high demand for this type of labor.[42] With the increasing availability of Chinese wage laborers, it was possible for the Thai state to dispense with a large part of corvée labor. By the reign of King Rama III, the Siamese state had developed a preference for tax payment in cash rather than taxes-in-kind since the former could be used to hire Chinese labor. In addition, Chinese wage laborers were said to be more efficient and reliable than the unmotivated and reluctant Siamese *phrai* peasants. This probably contributed in part to the reduction in corvée time for the Thai *phrai*. In the end, the alternative of Chinese labor undermined the economic rationale for the old corvée labor system, leading to its elimination in 1905.

Closely related to the hiring of Chinese labor and the reduced corvée was the change in the method of revenue collection. During the reign of Rama I (1782-1809), trade, particularly with China, provided the king, who monopolized foreign trade, part of the cash required to hire Chinese labor.[43] In the reign of Rama II (1809-1824), trade with China

---

[39]The number of Chinese entering Thailand increased significantly during the reigns of King Rama II (1809-1824) and III (1824-1851). In 1830, it was estimated that some six to eight thousand Chinese were entering Siam each year. By 1855, at the historic time of the signing of the Bowring Treaty with Britain, the number of Chinese was estimated at around 300,000, or 5-6 per cent of Siam's total population of 5-6 million.

[40] It is important to note that despite various measures to monitor and control *phrai luang*, the king kept losing his labor to powerful nobles through various forms of corruption. Some *phrai luang* also avoided registration by absconding and hiding in the jungles, while others were already paying a money tax to commute labor services.

[41] The Chinese immigrants paid a head of tax of 4.5 baht once every three years from 1828 to 1909. After compulsory male corvée labor was finally abolished for the Siamese in 1899, the Siamese *phrai* had to pay a head tax of 4-6 baht every year. Lysa Hong, "The Evolution of the Thai Economy in the Early Bangkok Period and its Historiography" (Ph.D. diss., University of Sydney, 1981). 197-198.

[42] For instance, during the reign of King Rama I, the construction of the *ropkrung* (around the capital) canal required 10,000 laborers. See in Kevin Hewison. "Bankers." 39.

[43] Trade was profitable during the first reign of the Bangkok period, with chronicles stating that the greatest revenues in that era came from the Chinese junk trade. This provided considerable revenues for the king and

diminished after China was assaulted by Western imperialism.[44] Declining trade earnings prompted the king to bolster revenues by changing the system of tax collection and by raising more taxes internally. From the 1800s, the king gradually replaced tax payments due in kind with tax farms and revenues payable in cash.[45] Over the next six decades, the government extended tax farming to an ever broad range of items, which included forest goods, agricultural goods, artisanal manufactures, fisheries, some forms of gambling, and even entertainment such as theatre, among others.[46] The replacement of the old system of revenue extraction with the tax farming system directly undermined the material base of many of the old nobles, hence weakening their status as patrons and subsequently, their political power.

Along with internal factors, there were also external forces that induced internal change. The nineteenth century was indeed a high time for western imperialism. Siam was not exempted from this external threat. In 1855, Siam was pressured to sign an unequal commercial treaty with the British, entitled the Bowring treaty after Sir John Bowring, the British diplomatic official who initiated the treaty.[47] This year is widely regarded by historians and scholars of other disciplines as marking the border line between Thai pre-modern and modern economic history. It was also seen as the beginning of western capitalist penetration into the Thai social formation.[48] Economically, the importance of the Bowring Treaty lies in its abolition of the royal trade monopoly, in its agreement that export goods could only be taxed once according to fixed rates, and in the introduction of a flat custom duty of 3% of market value on all goods imported by the British into Siam. The

his treasury, the aristocrats, and the Chinese merchants.

[44] Also, technological changes were overtaking Asia trade, as junks could no longer compete with the faster and larger Western ships. The Treaty of Nanking, in 1842, opened Chinese ports to square-rigged, Western vessels, thus adding to the decline of the junk trade and making the Thai king's trading ships obsolete. For more details, see Kevin Hewison, "Bankers," 38.

[45] Tax farming differed significantly from the traditional revenue extraction system in which the mun nai passively extracted payments in kind from the phrai and channelled the payments to the crown while controlling the phrai labor on the crown's behalf. The most important difference was that the new system promoted entrepreneurship, while the old one did not. In the new system, the Crown allocated or auctioned to the tax farmer the right to collect a tax on a specific commodity in a specific area. The tax farmer was remunerated by collecting more than what the Crown required. The tax farmers thus had an interest in promoting production of items to be taxed. Many of the tax farmers or nai akorn were immigrant Chinese who were more keen on commerce than the traditional nobles. Some of them were given by the king official titles and administrative positions.

[46]See more in Pasuk and Baker, "Thailand," 94 - 95.

[47] After the Bowring treaty was signed, the Siamese state was obliged to sign similar unequal treaties with other foreign powers including France, the United States, Denmark, Portugal, the Netherlands, Germany, and Japan, among others.

[48]Although western nations had established diplomatic and trade relations with Siam long before 1855, they had never penetrated deeply into the country's economic structure largely due to the king's monopoly of external trade and Siamese freedom from direct colonial rule.

treaty also removed a ban on the sale of rice, fish and salt.[49]   Politically, the treaty granted the British the right of extraterritoriality, which had significant legal implications for the Siamese.

As a result of trade liberalization imposed by the Bowring treaty, Siam was incorporated into the capitalist world economy. The subsistence economy was transformed into a commodity production economy. Foreign demand for certain local produce, notably rice, led to greater exports, particularly to those British colonies in Asia that focused on non-food production. Consequently, land and labor on the supply side were drawn into production of more rice for export.[50] In 1867, the Thai government established a system of entitlement for use of rice land for which taxes were based on harvested area. The most fertile area of the Central Plains along the Chao Phraya river was mainly expropriated by the king, his close relatives, and a few aristocratic families. These ruling elites later turned the land into development projects with canal digging and land allotment for rent farming. The *phrai* peasantry was also permitted to take up unoccupied land in the fringe area of the Central Plains or to settle as tenants in the area of canal projects. At this stage, the growth of the rice export economy began to generate a society of landlords and tenant farmers in place of *mun nai* and *phrai*.

The expanding and increasingly high-yield rice cultivation had lured *phrai* away from the traditional systems of labor control. The *phrai* had always resented the corvée. Many *phrai* lawfully bought their exemption from corvée by paying commutation payments or head tax, a practice allowed since the 1810s. Despite the high exemption fees, many *phrai* were prepared to pay so that they could get on with their rice farming. By the 1850s, the returns from these exemption fees became one of the biggest revenue sources for the royal reserve. Those who could not afford the exemption fee sought other ways to evade the corvée from bribing officials to escaping into the jungles. By the 1870s, as much as eighty per cent of the *phrai* population was estimated to be evading the corvée registration. Corvée had become a useless method even for raising an army.[51] The king and the nobles, in fact,

---

[49] Prior to the Bowring treaty, Thai law required that a three year's supply of rice should remain in the country before any was allowed to be exported. The law was abolished in 1855.

[50] Thai rice exports increased 25 fold between the 1850s and 1930s, jumping from the average of 990,000 piculs per year (1 picul is equal to 60 kilograms) in 1857-1859 to the average of 25,720,000 piculs per year in 1930-1934.   Meanwhile, rice farmland had expanded from 5.8 million rai in 1850 to 11.5 million rai in 1910-1914 to 34.6 million rai in 1950. Half of this was in the Central Region. J.C. Ingram, *Economic Change in Thailand since 1850* (Stanford: Stanford University Press, 1955), 204-205.

[51] During this period, the military forces mobilized in the face of increasing pressure from the French were comprised almost wholly of Mon, Lao, Vietnamese – mostly war prisoners, *that* bondsmen, and other immigrants who were still bound by special ties of servitude. See more in Pasuk Phongphaichit and Chris

might have also contributed to this evasion. Their budding capitalist instincts seem to have outweighed their demand to maintain corvée for supplies of household labor. Once the canal investment began, the king and nobles, who wanted tenants to occupy their land, were said to be uninterested in checking the *phrai's* tattoo.[52] With the availability of the Chinese immigrants and the state's repeated failure in corvée mobilization, the famous King Chulalongkorn (1868-1910) began the process of dismantling the systems of forced labor during the 1870s. This process was carried out as part of the Chakkri Reformation to pave the way for the country's modernization.

As a centerpiece in the great reform, the manpower reform carried one broad objective -- to centralize political power. By this time the *sakdina* and its associated corvée system were already in an advanced state of decay. The divisive tendencies of the system intensified political tensions between the monarch and the nobility. The gradual emancipation of *that* (slave) and *phrai* by King Chulalongkorn between 1874 and 1905 was, in fact, part of the royal strategy to undermine the old nobility and to encourage the formation of a new independent peasantry. Besides, with the growing monetization of the economy, the government felt a need to shift to a more effective system of resource mobilization based on taxes paid in cash rather than labor or produce. The presence of the Chinese immigrants and the unleashing of *phrai* to become farmers may have also led to an awareness that neither slavery nor corvée were as efficient as a labor market system based on freemen, that is, on free farmers and money wages.[53]

Internal political issues aside, the abolitions of corvée and slavery are often interpreted as a response to the influx of western ideas and, more importantly, to the colonial challenge. With many young princes and nobles returning home from education in Europe, there emerged in the royal court a growing recognition that both institutions – corvée and slavery -- were anachronisms and "uncivilized" by western standards.[54] In the meantime, with the surrounding threat of colonial powers like Britain and France, King Chulalongkorn felt it was important to centralize the control of manpower as much as possible. Concentration of power to the extent of constructing an internal colonialism was regarded as the key to evade western colonialism.

Baker, *Thailand, Economy and Politics*. (Oxford: Oxford University Press, 1995), 24.
[52] Ibid., 25.
[53] Muscat, "The Fifth," 22-23.
[54] Ibid., 22.

One of the steps taken to achieve this concentration of manpower was to set up a modern military force in the same fashion as the European model, something that was non-existent before in Siam. The *krom tahan na,* which literally means the department of front-line ground troops, was founded in 1880. This department recruited its soldiers from *phrai* whose *mun nai* had passed away and from those "white-wristed *phrai.*" who had evaded corvée and the required tattooing in the past. This latter group were given an amnesty for their crime if they turned themselves in for registration as ground soldiers. Besides, each newly-registered soldier was also entitled to a financial bonus and a free uniform, which were given as incentives to encourage registration. The first military legislation passed in 1888 had a provision that entitled each new soldier to a salary and an exemption from corvée without having to pay head tax. In 1905, the first military conscription law was enacted, enforcing, with few exceptions, a mandatory two-year military service on all Thai males when they turn eighteen.[55]

Along with introducing a modernized military system, King Chulalongkorn also continued with traditional measures to centralize manpower organization. For instance, those white-wristed *phrai* who did not register with the ground troops were forcibly tattooed as *phrai luang,* if caught. Several schemes were undertaken to boost the number of *phrai luang,* while at the same time encouraging a gradual extinction of *phrai som.* According to conventional traditions, all *phrai som* whose *mun nai* have passed away or have been convicted of crimes against the state were automatically turned into *phrai luang.*[56] With lengthy funeral proceedings, which could last more than a year, many *phrai som* managed during the lapsed time to disappear or to become registered under a different *mun nai* to avoid becoming *phrai luang.* In an 1887 law, however, all *phrai som* who fell into the category above were required to be retattooed as *phrai luang* within eight months after the death of their *mun nai.* Shortly after, the king also demanded that the nobles within the metropolis and outlying cities pay up arrears due to him from commutation payments received from their *phrai som* or else surrender control over the men. Most surrendered their men. Within the same year, the king, through the Registration Department, reduced the commutation payment (or head tax) from eighteen baht to six baht annually. By the turn of the century, corvée had virtually been replaced by a head tax. The formal abolition of the

---

[55] According to this law, all Thai people, with the exception of Chinese, tribal people, and the royal family members at the rank of prince upwards, were required to register.
[56] Muscat, "The Fifth." 48.

corvée system took place in 1905 and coincided with the enforcement of the military conscription law.[57]

By liberating the *phrai* and *that* from the corvée and bondage and by creating a modern military organization. King Chulalongkorn had achieved a major centralization of power, creating a powerful monarchy over a society of independent peasants and uniformed men, while undermining the rivaling power of the nobles. Yet, struggles over power with the nobles were far from over. While the formal hierarchical system of *sakdina* disappeared (except for residual titles among royal descendants and high-level aristocrats), the predilection to hierarchy and to a social system in which people group themselves in patron-client networks had become deeply embedded in Thai society. This is a legacy which continues to be characteristic of Thai bureaucratic and political behavior even in the modern period.

STATE SURVEILLANCE AND RESISTANCE
IN THE PRE-MODERN RATTANAKOSIN PERIOD

In the first and second reigns of the Rattanakosin kingdom, due to the wars with Burma and the subsequent Siamese conquests, Siam became even more sparsely populated.[58] While tighter control over labor was deemed necessary in this period, it had also become obvious to the king that most *phrai* resented corvée, particularly after the Thon Buri period when they were forced to serve six long arduous months every year. The laws regarding *phrai* in this period thus reflected both the need of the state to improve their surveillance over the *phrai* and the effort to minimize the resistance to corvée. A law passed by King Rama II in 1810 decreed an entirely new tattoo marking for the entire commoner population (including women and children) and promised amnesty for *phrai* and *that* who had escaped corvée in the past if they turned themselves in for registration (new tattooing).

---

[57]Meanwhile, King Chulalongkorn. through several decrees. gradually abolished slavery. In 1874, he decreed that children born to *that* after 1868 automatically gained their freedom on reaching the age of twenty-one. This meant that the supply of slaves would gradually diminish over two decades. By the 1890s, *that* who had been freed or who had fled from the continued control of their masters were in great demand as prospective tenants in the Rangsit tract, the largest of all canal projects in the Central Plains.

[58] King Yotfa or Rama I was a capable warrior. He engaged aggressively in military activity to establish almost unchallenged domination over other states in Indochina. During his reign, he took back several northern states from the Burmese and established control over much of the Khmer region and the key Laotian city of Luang Prabang. In the 1830s, his son, Rama II, managed to gain control over the outlying regions. Bangkok then dominated a hinterland that included all of modern-day Thailand. Laos. and Cambodia plus the northeast corner of Burma and the northern states of Malaysia.

The law gave all *phrai* the right to choose to be registered with any *mun nai* or even to change *nai*.. This law also reduced the required corvée period for *phrai luang* to three months.[59] It was also in this reign that a commutation fee was first allowed in place of corvée for those *phrai* who did not want to perform the service. Those who could afford it were required to pay a fee from 6 to 8 baht per month of service not rendered. They were also allowed to pay in produce.[60]

Despite the measures to appease the *phrai*, escapes and abuses of the corvée system continued, particularly the phenomenon of *phrai* selling themselves as *that*. Several decrees were passed during the reign of Rama II to combat such practices, but to little avail. The general attitude of the populace toward corvée was so hostile that it seemed *phrai* would risk anything to evade it. This attitude of resistance was well captured in a passage in a famous romantic Thai poem written during Rama II's reign (1809-1824). One of the fictional characters, Plaikaew, informed the abbot of a temple that he desired to leave the monastery, and the latter responded:

> "Why are you leaving the monkhood, to get tattooed? With marked wrist, you will suffer all the time. You will have to carry a heavy machete until your shoulders are sore. If the group leader likes you, then you are lucky for he will be kind and not order you to do heavy work. Otherwise, he will employ you in all arduous work such as sawing and drawing log..."[61]

By the mid-nineteenth century, the influx of Chinese immigrants was so high that Chinese wage labor became the mainstay for large public works projects, construction and general urban labor. Nevertheless, the crown still wished to maintain corvée to ensure regular supplies of labor to work on the royal estates, in the royal household, and in menial government tasks.[62] By 1857, the number of *phrai luang* must have reached its historic low because the reigning king, King Mongkut or Rama IV, convened a meeting of his top officials to discuss the problem. He was quoted as saying: "at present no individual *phrai luang* or group of *phrai luang* want to serve in the corvée." The king thus appointed agents to round up unattached labor and add them to the labor reserve of *phrai luang*. In the 1860s,

---

[59]"The Royal History of the Rattanakosin Period during Rama II," (*Phraratchapongsawadarn krung rattanakosin*, the second reign) dated December 2, 1810, quoted in Kachorn, "Status," 37.

[60] John Crawford, *Journal of an Embassy to the Courts of Siam and Cochin China* (Kuala Lumpur: Oxford University Press, 1967), 374-375.

[61] Krom Sinlapakorn, *Khun Chang Khun Phaen*. (Bangkok: Khurusapha, 1962). 119, as quoted in Chatchai, "*Phrai*." 18. It should be noted that there is no exact record of when this folklore-turned poetic novel was written since the story was transmitted orally. However, the scene on which the story was based is estimated to have taken place in the reigns of Rama II (1809-1824) and Rama III (1824-1851).

[62] Pasuk and Baker, "Thailand," 24.

there was a major effort on the part of the crown to send tattooing parties out into the provinces to register anyone they could find.[63] When King Chulalongkorn came to the throne in 1868, this policy continued. Bureaucratic-minded Chulalongkorn also issued new rules affecting where *phrai* were to register based upon a new zoning system that reflected the new system of bureaucratic planning and administration.

All these desperate measures to mobilize and register *phrai* in both reigns met with nothing but resentment, abuses, and corruption. On the part of the *phrai*, they developed many ways to evade the registration. Some disguised themselves as non-*phrai* -- foreigners, prisoners, monks, and handicapped. Others bribed officials to classify them into exempt categories. An example of one local registration station in 1867 might be illustrative. Of a total of 3,906 adult males, three-fifths were classified as exempt. This included 626 who claimed an official rank, 550 who claimed to be monks, 486 who claimed to be slaves, and 385 who were disabled, destitute, mentally ill, or possessed by evil spirits.[64] Indeed, corruption among officials must have been rampant. A law passed in the reign of Chulalongkorn indicates corrupt practices at tattoo stations:

> ...let it be the order that (officials) tattoo all the *phrai* and not conceal them. [Officials] must not oppress *phrai* such as if (any *phrai*) does not have money (to bribe) the officials tattoo big letter until it causes a lot of bleeding. If [any *phrai*] gives bribes, then [the officials] tattoo him with very tiny letters until they are almost invisible. Let the director of the registration station keep an eye on these practices and do not allow them to happen.[65]

Not only was the tattoo compulsory for all registered *phrai*, the *phrai* were also required to pay a tattooing fee of 1 baht and 1 fu'ang (1.25 baht).[66] This system of tattooing phrai as a means to keep track of them continued well into the end of the nineteenth century.

CONCLUSION

In retrospect, it is evident that the expansion of surveillance in its two primary senses -- information gathering about subjects and supervision of their conduct -- was of key

[63] Chatthip and Suthy, "The Political," 317.

[64] Junko Koizumi, "The Commutation of *Suai* from Northeast Siam in the Middle of the Nineteenth Century," *Journal of Southeast Asian Studies* 23 (1992): 282.

[65] National Archives of Thailand. the Fifth Reign: K-3., dated 1869-1871., 25. quoted in Chatchai , "*Phrai*, Neither Free nor Bonded," 20.

[66] Ibid.

importance to the sustained existence of the traditional states of Ayutthaya, Thon Buri and early Rattanakosin. Shaped by centuries of warfare and the basic resource configuration of land abundance and labor scarcity, the priority facing these pre-modern states was the mobilization and control of humanpower which was essential for the generation of both economic and political power. The *sakdina* system was thus developed to answer this need of the state and it was also through this means that state surveillance thrived for more than five centuries. Without the establishment of such hierarchical systems of supervision that allowed the *phrai* populations to be monitored, and more importantly, tattooed by the *mun nai*, it is doubtful if any significant amount of social control could have been achieved in a vast frontier of scattered village settlements like Ayutthaya and Rattanakosin. In the absence of a defined territory, modern transportation, and information and communication technologies, Ayutthaya did not fare too poorly in its administrative competence -- the capacity to establish co-ordinated control over what the state considered its population. The prosperity of the Crown, which relied mainly on revenue extraction from *phrai* , and more than five centuries of the kingdom's prosperity, although beset by warfare, provide good evidence of the system's administrative success.

In attempting a social analysis of surveillance, one needs to consider specific practices within their specific social context. Take wrist-tattooing, which was a major surveillance technology during these periods, for instance. This technique, which involves an indelible marking of a body part, not only suggests a rudimentary level of technological development but also indicates an extreme asymmetry in power relations between the state -- the king and the nobles -- and the majority of the society -- the *phrai* or common people. For the former, the tattooing was simply a method of information collection and a device that facilitated monitoring of the *phrai*. For the *phrai*, being tattooed meant being a legal person eligible for protection from representatives of the state -- the *mun nai* -- through the culturally embedded patronage system. Not being tattooed or being a "white-wristed *phrai*," on the other hand, meant criminality as well as ineligibility for state protection. Whether it was this contingency of state protection or other factors that made many *phrai* conform to this pervasive technology of surveillance is difficult to assess. Although tattooing was traditionally a common practice among superstitious Thai men, it had been mainly voluntary.[67] Historical evidence suggests that mandatory tattooing was abhorred just as much as mandatory corvée was resented. Yet, the practice lasted for centuries. Some

---

[67]From the ancient times, tattooing had always been a popular practice among village men in Siam. It was, and still is in the rural area at present, believed that tattoos and amulets are repositories of spirit power and capable of rendering bearers with invulnerability.

analysts suggest that the overpowering state was able to maneuver this surveillance scheme on the populace because of the people's subservient attitudes to the state. This, it is argued. stems from the people's religious beliefs, the deep-rooted political tradition of paternalism. and the rigid social structure, which made it almost impossible for the ruled to break free from social obligations to the rulers.[68]

Historical evidence also shows, however, that despite the pervasiveness of wrist-tattooing, routine information-gathering, and monitoring of the activities of *phrai* for social control purposes, there still remained significant limits to the degree of control realized. Although only a few revolts against the state were recorded during this extensive period. evasions of corvée were rampant and grew in number and significance over time. While the individual *phrai* might have been powerless vis-a-vis the king, who was at the helm of social control, their resistance efforts collectively created a "dialectic of control," one that was powerful enough to contribute to an eventual social reform. The *phrai*'s resistance was most evident in the strategic patron-client relations they formed with the nobles. This resulted in uncontrolled corruption and cooptation at the expense of the Crown. The experiences of certain reigns during Ayutthaya and early Rattanakosin illustrates what Christopher Dandeker refers to as "ineffective bureaucratic surveillance," which rested on the personal and informal patronage system. In such instances, the state would be ill equipped to supervise and gather information about the subject population and thereby to sustain the system of rule.

Along with patron-client relations, another important factor which contributed to the existence of a "dialectic of control" during these pre-modern periods (particularly Ayutthaya) was the essentially segmental character of the society. Notably, Siam before the late nineteenth century remained without a defined border and was made up of city-states and a hinterland of scattered villages, situated in a mass of mountains and jungles. Many of the local overlords in the frontier areas owed multiple allegiances, and some constantly sought to evade Siamese control. This fragmented and relatively autonomous character of the frontier areas significantly hindered direct supervision of the activities of the populace by the Ayutthaya and early Rattanakosin (Bangkok) rulers. As can be inferred from Foucault's discussion of the panopticon, the concentration of activities within a clearly bounded setting greatly enlarges the degree to which these activities can be monitored and thus controlled.

---

[68]Thanes Apornsuwan, "The Rights of Thais in the Thai State," (*sitthi khon thai nai rat thai*) ed. Chaiwai Satha-anand, *New Paradigms for Thai Studies in the Year 2000* (Bangkok: Thailand Research Fund, 1996), 205-207.

Apparently, a primarily rural society without a defined border and scattered frontiers like Ayutthaya and early Rattanakosin in no way constituted an established locale in which the regularized observation of activities could be carried out. As a result, this "segmental autonomy" of the frontiers, together with the patronage system, provided the subordinate *phrai* a chance to struggle against the pervading disciplinary surveillance executed through the centralized *sakdina* system.

Aside from social and geographical factors that gave *phrai* some leeway vis-a-vis the state, the technical property of surveillance technologies in this period might also have contributed to the limited success of administrative control. From Ayutthaya to early Rattanakosin, the primary technologies used in the collection, storage and dissemination of information about *phrai* in these societies did not change much. Two types of technologies could be delineated — tattooing and writing. The former apparently relied on the use of tattooing equipment that should not have been difficult to duplicate considering the popularity of tattooing among Thai men. As a few laws passed during the Thon Buri and early Rattanakosin suggested, fake tattooing — either by using unofficial tattooing equipment or by stealing the official tools — was such a common practice among the *phrai* to avoid corvée that it finally became outlawed. As for writing, which was used to list the name, number and affiliation, and other attributes of *phrai* in the rosters, there were also some major shortcomings.[69] Although writing provided a means of coding information and information storage, which was unprecedented in oral cultures, its "storage" capacity or the capacity to enhance time-space distanciation also depends substantially on the property of the material used to record the listing. This reflects Harold Innis's famous notion of the "bias" of communication media.[70] In the Ayutthaya case, there is historical evidence that shows that paper made from palm tree leaves was used for documentation.[71] Paper, as Innis would argue, is a space-binding type of medium since it is light, easily transportable, and easily reproducible. Yet, it also tends to be less long-lasting or time-binding when compared to such media as stone and parchment. So while palm tree paper was used widely to record administrative documentation such as the *phrai* rosters that enabled the Ayutthaya state to hold together administratively across vast spaces, its lack of durability could also have been a

[69]According to the famous Ramkhamhaeng inscription of the Sukhothai period dated 1292 A.D., the invention of the Thai script which preceded writing took place in 1283. King Ramkhamhaeng adapted the new script from a type of ancient Khmer script.

[70]See Harold Innis, *The Bias of Communication* (Toronto: University of Toronto Press, 1951), especially 33-60.

[71]Vicharn Panich, " Science and Technology in Thailand's Health Sector," in *Science and Technology in Thailand: Lessons from a Developing Economy* eds. Yongyuth Yuthavong and Angela M. Wojcik (Bangkok: NSTDA/UNESCO Publishing), 1997), 76.

constraint. Aside from the daily wear and tear, these paper *phrai* rosters were bound to perish in the raids and burning during the two conquests of Ayutthaya by Burma.

In the final analysis, it is quite clear that a combination of factors culminated in a social reform that put an end to many traditional social practices including the corvée and traditional state surveillance systems. Siam in the nineteenth century saw a gradual shift in political economy stimulated by the availability of Chinese labor to replace corvée labor, the penetration of western capitalism, the growth of farming peasantry, the introduction of a new system of revenue extraction, and the penetration of western ideas and values. There was also the external aggression of western imperialism and the internal decline of the *sakdina* as a system of social organization, which was partly reflected in the widespread and active resistance against the corvée by the *phrai*. Siamese rulers' main strategic response to these pressures was to launch a series of modernization programs, which became known as the Chakkri Reformation. As far as the *phrai* were concerned, they were liberated from corvée obligation, and most entered into a new type of social relations as farming tenants and as free wage laborers. Wrist-tattooing was later eliminated as a method of surveillance and instead replaced with more bureaucratic techniques. Despite these changes, the nature of the relationship between the former *phrai*, the independent peasantry and the former *mun nai*, the new bureaucrats, did not drastically change. As will be shown in the next chapter, the ensuing period of modernization and absolutism that followed the Chakkri Reformation saw a continuing legacy of a tight system of political and administrative control as well as social and political patronage in a fashion that remained reminiscent of the preceding *sakdina* system. Through many new surveillance activities executed in the name of state-building, the state was attempting an even more stringent mode of social control than before. The task of getting information about and supervising the masses of the subject population now fell into the hands of a newly established bureaucracy that would form the basis of an emerging power structure for most of the twentieth century.

CHAPTER 3

STATE SURVEILLANCE IN THAILAND -- THE MODERNIZING YEARS
(1892 - 1983)

This chapter discusses the institutional context and the development of state surveillance in Thailand from 1905 to 1983. This is a period of important transition in Thai history. During these decades, the country experienced various significant events including a social reform, a major change in political regime, an insurgency problem, and wars. Beginning with the Chakkri Reformation of 1892, the country witnessed an extensive and far-reaching administrative reform along the pattern of modern Western state-building.[1] This set the stage for forty independent years of rule under the absolute monarchy, which was brought down by a bureaucrat-led coup d'état in 1932. This year marked the starting point for modern Thai politics, which opened with a trial period for bureaucratic democracy (1933-1957), a period of dictatorial rule (1958-1973), and finally a somewhat rocky journey to the parliamentary democracy of the present.

In order to understand the development of state surveillance during this period, it is essential to first understand the central mechanism for administration of population surveillance, that is, the emerging state bureaucracy, and the purpose these surveillance schemes were designed to serve. Initially, the new bureaucracy was conceived as part of a royal plan to augment administrative competence, which was being increasingly eroded by both internal and external threats. The former being the rise of new social classes and their struggles against government control, and the latter being the expansion of western colonialism during the nineteenth and early twentieth century. As the twentieth century progressed, the more central issues for the Thai bureaucracy became "security" problems, which were increasingly apparent in the post-war years. From the mid-1960s to the early 1980s, combatting communism was the top priority for the government bureaucracy, which in turn prioritized national security and rationalized its domination on that ground. According to one school of thought in Thai studies, the government bureaucracy was so powerful that it overshadowed all other social forces for several decades. During much of the period between

---

[1]The Chakkri Reformation, which began formally in 1892, took more than two decades to complete. Aside from a major bureaucratic reform, King Chulalongkorn also launched a series of other reforms including the emancipation of slaves, the abolition of the corvée system and outdated customs, establishment of a modern military force, legal reform, education reform, and creation of new and modern means of transportation and communication such as highways and telegraph.

1932 and 1973, Thailand came to be known among these studies as a classic case of a "bureaucratic polity."[2]

FROM THE 1892 BUREAUCRATIC REFORM TO THE 1932 COUP

Although most accounts of the Chakkri Reformation identify western imperialism as the major progenitor, another important causal factor is believed to be internal disorder. This disorder emerged as a by-product of the expansion of commerce and agriculture in the nineteenth century. As a result of this expansion, new social groups were created that stood outside traditional social and political control. For instance, the new peasantry, particularly those in the frontier, were no longer tied by the old indenture bonds, while the trading and laboring groups of urban Chinese immigrants simply grew up outside the *sakdina* system. Both groups developed internal cohesive solidarity with which they resisted government control. While the expanding peasantry relied on the influence of local overlords who staged various forms of resistance against state authority seeking to control them, the relatively independent Chinese had a powerful internal organization acting as an effective buffer and negotiator with the government.[3] One of the more concerted forms of resistance against government intervention was a spate of "banditry" perpetrated by local overlords in the countryside in the Central Plain where government authority penetrated most deeply in the 1890s.[4] State officials were often subject to highway robbery by these "bandits" when transporting tax collections from new agricultural tracts in the central districts around Bangkok to the Crown Treasury in Bangkok.

In the late nineteenth century, these internal threats became evident and were directly weakening the old systems of labor and revenue extraction. As discussed in the previous

---

[2]Frederick Riggs, *Thailand: The Modernization of a Bureaucratic Polity* (Honolulu: East-West Center Press, 1966). According to Riggs, a "bureaucratic polity" refers to a political regime in which the bureaucracy is highly dominant in politics and policy-making. Such a polity, argued Riggs, is neither a traditional nor a modern system. Unlike a traditional system, it develops a wide range of differentiated bureaucratic structures. Unlike a modern political system, it fails to create a non-bureaucratic mechanism to hold the bureaucracy accountable.

[3]Unlike the case of the rural farmers, the relations between the rulers and the urban Chinese were much more complex. Because of their strong reliance on the Chinese for commercial growth and for their own revenue, the rulers found it difficult to govern them through traditional techniques of patronage and intimidation.

[4]Unlike conventional bandits, these "bandits" who were local "tough men" usually carried out a series of raids and assaults against officials and noble landlords in the countryside. Since they robbed only the rich and often helped the poor with the stolen money, they enjoyed a local popularity and were sheltered from the authority by the local community for more than a decade. Many of them were portrayed as romantic local rebels against the authority of government in folklore. See more in Pasuk and Baker, "Thailand," 218-219.

70

chapter, by this time the king as well as many of the old nobles were suffering tremendously from the decline of the *sakdina* and the corvée systems, which were the bases of their political and economic power. Consequently, from the 1880s, the newly-constructed army made regular campaigns against the so-called "bandits" of the rural frontier one of their major occupations. Although these campaigns resulted in hundreds of arrests, the battle against local disorder was far from over. The task of suppression of these bandits was later transferred to a new police force, which was created in the 1890s as a direct effort to bring under control the banditry which dominated the central region.

Apart from the use of force, the Chulalongkorn government was also planning the control of the new peasantry through a new administrative system that would penetrate more thoroughly into the fabric of the frontier society.[5] The newly-launched administrative reform essentially transformed the traditional state administration into functionally specialized ministries along western lines. The two grand ministries -- civil and military affairs -- were abolished. All the officials who used to derive benefits from the labor of their indentured *phrai* became salaried government officials. In addition, as a means of creating a centralized state, provincial administration, which had been until then largely autonomous and problematic, was brought under Bangkok's control. The newly-established Ministry of Interior was charged with the centralization of power.

Under Prince Damrong, Chulalongkorn's half brother, the Ministry of Interior was able to extend the reach of the central government into the newly-created provinces which were formerly towns and city-states.[6] The key to this new network of control was the *monthon* or region. It was developed from 1892 onwards as a network of general government, blanketing the entire nation, mainly responsible for internal pacification and serving as a mainstay for other specialized administrative activities. In essence, the *monthon* were the power centers representing the central government at key points across the nation. They were under the jurisdiction of the *monthon* commissioners (appointed by the Minister of Interior), who were intended to supplant the hereditary rulers and nobles in the provinces. Often, the commissioners would bring in administrators from Bangkok, who worked alongside the

---

[5]Up until 1892, one of the major problems facing Siam was the inability of the government to exert control over provincial administrations in the peripheral regions. The consistent effort to centralize control was weakened by poor transportation and communication. This made a large degree of decentralization of power inevitable. In general, the degree of control maintained by the central government over the provinces decreased as the distance from the capital increased.

[6]In Bangkok-centric Thailand, the term "the provinces" generally refers to provinces outside Bangkok or currently the Bangkok Metropolitan Administration (BMA) which includes Bangkok and the provinces in the outskirts of the city.

provincial nobles and gradually sapped their powers.[7] In addition, with the promulgation of the Provincial Administration Act in 1898, which established a salaried national administrator for each province, the independence of provincial powerholders was weakened tremendously. The same law also laid down a centralized administrative pyramid of regional, provincial, and district jurisdictions as a standardized system for the whole nation.

Despite lack of resources and opposition from local powers, particularly at the village level, this new administrative structure developed slowly and unevenly across the country, producing a considerable centralization of control from Bangkok. The Ministry of Interior was the center of this administrative expansion. Its main task was not only general administration -- maintaining order and peace -- but also integrating and overseeing other state activities including revenue collection, policing, and surveillance of people throughout Siam.[8] Through this Ministry, the Crown built a system of governmental control to replace *sakdina*.[9]

In a related development, since the 1880s the Siamese state had come under increasing pressure from the British and the French, the two dominant colonial powers in the region, to define exact borders between Siam and their colonial territories in Burma, Malaya, and the eastern frontier (what are now Laos and Cambodia). As a result, over the next three decades, Siam engaged with France and Britain "scrambling" to enclose the outer regions of the hinterland and to draw borders around areas that were empty of people or that had people who owed multiple allegiances. Through diplomatic and military coercion from the western colonialists, the borders were gradually drawn, hence turning Siam into a territorially-defined state for the first time. With the borders defined, Bangkok was able to protect its hinterland and to extend tighter control over the areas enclosed. The new territory also made possible a reorganization of provincial administration under the *monthon* system.

Despite the many changes and reforms introduced during the Chakkri Reformation, the political system remained unchanged. The technocratic king and his brothers were selective in their construction of a western-style system of administration; they adopted the idea of the

[7]Pasuk and Baker, "Thailand," 225.
[8]Chai-anan Samudavanij, *roi pi haeng kanpatirup rabop ratchakan* (TheCo-Evolution of State and Political Power in Thailand) (Bangkok: Chulalongkorn University Press, 1992), 52-53.
[9]It should be noted also that alongside the administrative reform, a financial reform was also launched. In the 1900s, a standard head tax was introduced which applied to all residents of Siam even the Chinese. In 1906-1907, the Treasury Department, which was then under the Ministry of Interior, introduced a new and higher structure of land tax. The expanding rice economy was the main target of this tax. By the 1910s, the land and head taxes delivered 20 per cent of the government revenue and thereafter this figure was continually on the rise as better administration helped generate revenues to the Treasury more effectively than ever before.

bureaucracy while abandoning the concept of a parliament.[10] For that matter, these reforms were part of a "state-building" and not a "nation-building" effort. Tremendous resources were mobilized to expand centralized bureaucratic power without any participation from other forces outside of the royal family and a handful of the former *sakdina* nobility. The reformed bureaucratic apparatus only made the state much more effective and powerful in extracting the resources from the populace to achieve its goals and needs. In creating this unitary and centralized state, dual and mutually-reinforcing objectives were met. One was a higher level of internal stability throughout the country. This was essential for coping with colonial encroachment. The other was the consolidation and strengthening of the political and economic power of the Crown.

Along with expanding its material foundations mainly from the surplus of the enlarging rice economy, the royal leaders also made certain of the peasantry's allegiance to the throne by constructing a mythology of Siam as a "nation" of Thai peasants owing allegiance to a king. It was King Vajiravudh, Chulalongkorn's son and successor, who combined King Mongkut (Rama IV)'s version of Buddhist kingship with the new concept of *chat* (nation) in this powerful ideology.[11] He contended that modern man could function as a political being only through allegiance to a nation. *Chat thai* or the Thai nation was defined by three unique characteristics -- the Thai language, the Buddhist religion, and the institution of kingship. In so doing, the distinctions of various ethnicities that were present in the Siamese kingdom at the time -- Mon, Lao, Malay, Khmer -- were submerged within the ideology of a seamless "Thai" people.[12]

The next forty years after the Chakkri Reformation are widely regarded by scholars on Thailand as the period of the absolutist state.[13] The Siamese absolutist state was a hybrid of modern western state-building and the traditional *sakdina* system. On the one hand, the western concept of a territorially-defined state and a centralized administration extending out

[10]It was most likely the British constitutional monarchy from which the Thai monarchs derived their model. Most of the princes were sent to be educated there.

[11]Previously, the word "*chat*" conveyed the idea of birth, race, or ethnic identity. Only in the last decade of the nineteenth century was it transmuted to express the idea of a "nation" -- a population enclosed within a given territory and owing political allegiance to a common authority.

[12]Pasuk and Baker, 234-235.

[13]According to Pasuk and Baker (1995), for instance, the Siamese absolutist state had some parallels with absolutist states in early Europe. In Europe, they argue, absolutist states emerged from declining feudalism, as peasantries fought free from feudal dues and ties, weakening the land-owning feudal nobility, and creating the opportunity for royal aggrandizement. As for nineteenth-century Siam, the new peasantry escaped the old bonds of labor indenture by commutation and evasion, hence weakening the *sakdina* nobility, and creating the opportunity for the king to construct a centralized and absolutist rule.

from the authority of an absolute king replaced the old and relatively loose networks of political authority that had exercised control over a large hinterland. On the other hand, traditional elements of the *sakdina* officialdom were still strong and were most apparent in the organization of the newly-constructed bureaucracy. It was common to see the higher echelons of the civilian and military bureaucracy monopolized by members of the royal family. This was not by virtue of their merit but of their lineage. While some non-royal *sakdina* nobility continued to maintain their political prominence, most of the hereditary nobles, particularly those in the hinterland provinces, were swept aside several royal aggrandizement projects during the Chakkri Reformation.[14] As this royal promotion practice continued in the reigns after Chulalongkom, it created much resentment among those bureaucrats who emerged from the ranks of the commoners. As early as the reign of Chulalongkom, there were already signs of change and demand for a political reform, albeit unsuccessful. An abortive coup was staged in 1912 during the reign of King Rama VI, Chulalongkom's son.[15] A major political shift was definitely in the process as it finally led to the coup of June 24, 1932 by a group of civil and military bureaucrats. Ironically, the bureaucracy created by the king had boomeranged and toppled the monarchy.[16]

STATE SURVEILLANCE AND RESISTANCE DURING THE ABSOLUTIST STATE (1892-1932)

Aggregate Surveillance Of The Populace

A modern system of aggregate surveillance in Siam can be roughly demarcated as having been initiated by the 1892 Reformation with the replacement of the traditional militia system by a modern military organization, the abolition of corvée, and the promulgation of the 1898 Provincial Administration Act. According to this 1898 law, a countrywide register-based population survey was to be carried out which would count and classify residents in every household based on their age group, instead of their affiliated *krom* (department) or their *mun nai*. The Siamese were for the first time surveyed and identified as individuals. This

---

[14]Although the hierarchical *sakdina* grades were abolished, members of the royal family and some of the nobles still maintained their elaborate aristocratic titles and ranks and were thus clearly distinguished from the commoners.

[15]This coup was led by a group of junior army officers who had graduated from the military academy founded by King Chulalongkom.

[16]Likit Dheeravegin, ed., *Thai Politics: Selected Aspects* (Bangkok: Tri-Sciences Publishing House, 1983), 265.

survey did not list in detail the name of each resident in the household since the commune[17] chiefs and the village headsmen. who were supposed to be carrying out the survey, were mostly illiterate. However, in 1903, another population survey was conducted by trained district chiefs and clerical staff in all the districts of the 12 *monthon*. With the exception of hill tribes and other tribal people who resided in the wilderness, every Siamese was to be registered in this survey. This was regarded as the first population survey since the great reform and was used as a guideline for many surveys that followed.

In 1909, King Chulalongkorn passed a new law which enforced registration of all people in the Siamese kingdom. This act empowered the ministers of the Ministry of Interior and the Metropolitan Ministry to be the caretakers of three population registration tasks -- household registration, birth and death registration, and immigration. The Ministry of Interior was charged with registration of the people in the provinces, while the Metropolitan Ministry was responsible for registering the Bangkok populace. The passing of this registration law and the administering of the countrywide population survey during this decade coincided with the introduction of capitation and land tax on all Siamese residents. Although the connection was rarely made explicit, it is quite clear that with the abolition of corvée and the end of dependence on nobles for control of manpower and channelling of revenues, the Crown needed new devices to identify and to monitor the now liberated *phrai* and *that* from whom the government revenue was extracted. Furthermore, with newly-drawn borders, the *phrai* rosters of the past could no longer furnish accurate and updated information about people in the new territory. In this light, the population survey could give the new bureaucracy a rough idea of how many people were residents of Siam and how many of them were subject to taxes -- by holding land or by being in the age group that was subject to the capitation tax. Similarly, the registration law of 1909 would enable the bureaucracy to collect more information about the people and to keep track of their movement, if necessary.

As the registration of population grew in its scope and size, the staff must have faced a lot of difficulties since most Siamese people did not have family names. Their first names were usually short and many people had common identical names.[18] In 1913, King Vajiravudh or Rama VI enacted a Surname Act primarily for the purpose of civil registration. This legalizing

---

[17]Communes or *tambon* in Thai refer to a group of villages or an official administrative subdivision under *amphoe* , which is equivalent to district or an administrative subdivision of province.

[18]Common Thai names were then short and had usually only one or two syllables. This is, of course, with the exception of the royalty and aristocrats who had long elaborate titles. It was not until the nationalist regime of Field Marshal Plaek Pibulsongkram in the 1950s that Thai people began to adopt longer and more elaborate names as is still the case at present.

of a last name made possible several subsequent civil registration tasks. Among them was the issuing of identity cum travel papers in 1914, the first of their kind in Thai history. This identity/travel document was enforced under another Provincial Administration Act passed in the same year. The objective of the document was declared as "to identify each and every individual as to who he/she is and his/her area of origin while traveling to unfamiliar territories in the kingdom" and "to serve as an official proof of innocence."[19] District officials were responsible for issuing such papers. The papers were required for travelling anywhere in the kingdom and became widely used. Before issuing the papers, the district chief would examine the number of travelers, vehicle, accompanying animals and weapons (if any), list them accordingly, and sign the documents to indicate approval. In the course of the journey, interior officials had the right to ask to see such papers from any traveler. This identity/travel paper was valid for one year only unless renewed.

Besides the enforcement of the requirement to carry identity/travel papers, at least three civil registration laws were passed between 1913 and 1917 that gradually systematized the methods of registration. The focus was mainly on three types of registration -- household, birth and death, and mobility between regions. In 1919 and again in 1929, two nationwide population surveys were conducted. In 1929, the Ministry of Interior was in charge of the overall survey as the Metropolitan Ministry had been abolished. In the Bangkok *monthon* and other not too distant *monthon*, school teachers and boy scouts carried out the survey, while in the peripheral *monthon*, commune chiefs and village headsmen were assigned this task with major assistance from teachers, students and provincial officials.

Despite the effort of the central government to enforce such civil registration in the peripheral regions, this was to little avail, particularly in remote units of communes or villages. Similar to their predecessors -- the *phrai* , the rural populations' main strategy in response to government penetration was evasion. Village communities regularly reacted to taxes and registration by fleeing to more remote areas of the frontier beyond the reach of the government. Many rural residents also colluded with village headmen on whom the government relied for the assessment and collection of revenue as well as record-keeping. At the turn of the century, the government became well aware that the rolls for the capitation tax showed remarkable numbers in certain categories -- monks, disabled, and mentally ill -- all of which qualified for exemption.[20] It is worth noting that the administrative reach of the newly-constructed Ministry

[19]Tiang Chalermchuang, "Citizen control and the national security." (*karn kuap kum polla muang kab khwam mankhong khong chat*). (Special degree thesis., National College of Defense. 1965), 11.
[20]Pasuk and Baker, "Thailand," 72.

of Interior in this period tended to stop short at the village gates. The Ministry's effort to co-opt village leaders into the lower rung of the centralized bureaucratic structure met with resistance even in the Central Plain where the government penetrated more deeply and rapidly.

Apart from changes in the administration, economy and geography, there was also an important technical innovation that possibly affected the information-gathering capacity of the Siamese state during the nineteenth century. This was the introduction of the first printing press in Thai language by a group of American missionaries in 1835.[21] Early Thai-language printing presses were used mainly to reproduce religious tracts and hymns to spread faith in Christianity among the Thai populace. Although most accounts of early printing in Siam tend to focus only on the printing of newspapers and the publishing of books, particularly literary works, there is also evidence which suggests that printing gradually became important for a wide range of administrative purposes -- printing rules and regulations and producing standardized forms for bureaucratic purposes including those used in civil registration. For instance, the first official document printed was a royal edict in 1839 forbidding the smoking and importing of opium, of which 9,000 copies were produced. As printing progressed over the years and the cost went down, so did the increase in its use for a wide range of bureaucratic ends including the collection and storage of personal documentary information by the state.

The population surveys and civil registration practices which began during the Chakkri Reformation corresponded in many ways with fundamental changes in the economy and society at the time. First, they were "civilized" methods, ones that were also used in the West, which epitomized modernity for the "modernizing" Siam. Secondly, when enforced through the new and "modern" bureaucratic structure of the state, this new mode of information gathering and supervisory control made possible and more effective many large-scale administrative activities including tax collection, conscription, and policing. Moreover, with a newly demarcated boundary, population surveys and civil registration became appropriate tools to assess population statistics and demography within the newly-defined territory. In this light, the identified geographical map of the country also furnished the Thai state with a political justification to supervise the administration of many border areas. Partly through civil registration, Bangkok was able to extend new forms of direct rule over local rulers in remote provinces and tighten its control further. Now, it was no longer only able-

---

[21] Although there is evidence that printing began in 1662 during the Ayutthaya era, this press was using Roman characters and not Thai characters. See Sukanya Teeravanich, History of Thai Newspapers under the Absolute Monarchy (1782-1932) (pra wat karn nangseupim nai prathethat paitai rabob sombonnarayasitthirat 2325-2475 B.E.) (Bangkok: Thai Wattanapanich, 1977), 6-8.

bodied males who were required to register. The birth, death, and relocation of every resident in the Siamese territory was supposed to be duly registered.

To conclude, the story of aggregate surveillance by the royal absolutist state is very much like "an old whiskey in a new bottle." While modern methods and bureaucratic approaches replaced the traditional wrist-tattooing, the purposes they served had hardly changed -- to improve the state's administrative competence and thereby to ensure their domination over society. By relying on bureaucratic surveillance as a basis for administrative and thereby social control, the newly-founded *kharatchakarn* (bureaucracy) was assuming the same function that the *mun nai* (nobles) had before.[22] In other words, in running the absolutist state, the crown transformed the old *phrai* - controlling aristocracy into the new people-controlling bureaucracy. The Ministry of the Interior was the centerpiece of this new absolutist state. It ran the provinces, kept the peace, and collected the taxes while also supplying the Ministry of Defence with lists of names for males who reached conscription age. Unlike the European colonial nations, which founded their state systems more on the control of land, the Thai absolutist state was founded on the local heritage of controlling people.

Surveillance Of Criminality

Apart from the establishment of the Ministry of Interior as the administrative core of aggregate surveillance on the Siamese citizens, the rise of the modern Siamese state in the early twentieth century was also accompanied by the birth of another type of surveillance which was less prominent and more focused in nature -- that associated with criminality. This realm of surveillance was organized as part of the policing and rehabilitating activities of the emerging modern criminal justice system. Between 1897 and 1908, the brutal capital punishment practised since the Ayutthaya era was gradually replaced with a new penal code which emphasized "rational" justice procedures involving the police, district attorneys, the court, and prisons.[23] As far as surveillance of criminality was concerned, an outstanding innovation during this period was the setting up of a bureaucratic entity to gather information about criminals. Created in 1901, the so-called Fingerprints Division within the then Department of

[22]Although translated in English as civil servants, *kharatchakarn* literally means the servants of the (royal) state. To be a *kharatcharkarn* conventionally means one works on behalf of the king and is thus an instrument of the absolutist state.

[23]Department of Corrections. *History of Penal System in Thailand* (Bangkok: Department of Corrections, 1996), 3. (draft). It should be noted that under *sakdina*, most judicial functions were entrusted to the *mun nai* and local officials.

78

Criminal Penalization (now the Department of Corrections) was responsible for collecting prisoners' fingerprints and histories of arrests in severe criminal cases so that repeat offenders could be singled out for heavier sentences.[24]   Soon after, the collection of fingerprints was expanded to cover *all* prisoners who were about to be released from prison. Prison wardens were assigned the task of fingerprinting and recording the full criminal record of every prisoner scheduled to be released.[25]   In addition, prisoners who were jailed more than three times were also tattooed on their wrist so that they could be easily identified. The tattoo marks consisted of the following: two letters of the alphabet which stood for "the Ministry of Interior," the identification numbers of each prisoner, and the year in which he or she was released. This mandatory marking of repeated offenders is quite notable considering that compulsory tattooing for *phrai luang* for general registration purposes was becoming extinct at this time. The marking of prisoners was mainly to ease the record check procedures, which were becoming cumbersome because of the overwhelming numbers of sets of fingerprints to be checked.

Besides criminal justice, the fingerprint records stored at the Fingerprints Division have also been used for non-criminal justice ends -- employment and licensing screening -- since as early as 1903. Beginning in 1903, the Metropolitan Police Department sent fingerprints of applicants for positions in the police force and for drivers' licenses to the fingerprints division for record checks. The Customs Department also followed suit in the screening of their prospective officials. The use of criminal fingerprint records as a screening tool resulted in a sharp increase in the workload of the Fingerprints Division, to the extent that it was elevated from division to department status in 1904. In 1905, the newly-established department for the first time opened its fingerprint record checking service to international organizations, beginning with the British Consulate, the US embassy, and the Singaporean embassy.[26]

The establishment of the Fingerprints Division was part of the modern state's effort to cope with the growth in crimes and criminal behavior. In the closing decade of the nineteenth century, the reformed government developed a centrally controlled police force and a new centralized judicial system. Both were organized as professional and bureaucratic

---

[24]The establishment of the Fingerprints Division coincided with the year in which Sir Edward Henry introduced a new fingerprints classification system at the British Scotland Yard.   This system, which was shortly after introduced to India, a British colony at the time, permitted the full ten-print classification of a person's fingerprints so that no two human beings would have the same classification numbers of patterns of minutiae.
[25]This practice became legalized in 1956. According to the Ministry of Interior Order No. 2/2499 B.E. dated 13 October 1956, the authorities in charge of the following institutions-- prisons, correctional facilities, and rehabilitation facilities -- were required to take fingerprints of prisoners, detainees, and trainees as well as a 2"*3" photo to the Fingerprints Division before any release.
[26]Department of Corrections, "History of ," 4-5.

organizations, aimed at keeping peace over the longer term and at bringing all citizens into a standard juridical relationship with the new state. The modern police force was a considerable improvement over the traditional force in which the state relied upon patronage arrangements for information on felons and contracted gangs for order enforcement.[27] In conjunction with the judiciary and correctional system, which housed criminal records and fingerprints records at the time, modern policing employed a mixture of informational and supervisory elements of surveillance in its crime control endeavor. These new and more impersonal means of surveillance, along with codified law and imprisonment, provided the new state with a much needed power to define what is "criminal" and a rational basis for the apprehension of offenders. It should be noted that the new Siam, with its newly-designated territory, was a very diverse society. The population within this new political entity was enormously varied in ethnic background and in historical experience. In this transitional period, there were rampant evasions and occasional outbreaks of active resistance against government control by rural communities and former tributary states. In many cases, offenders were protected from authorities by the local community. Even after the establishment of the new police and judicial system, both of which relied largely on recruits from Bangkok, the government still had difficulty arresting and prosecuting several bandits in the peripheral areas.

FROM MILITARY DICTATORSHIP AND BUREAUCRATIC POLITY TO PARLIAMENTARY DEMOCRACY (1932- 1982)

Despite the introduction of parliament and the enactment of a constitution, the leaders of the 1932 coup who toppled the absolute monarchy were never in real pursuit of a popular democratic government . Their mission was rather to place commoner officials in power and to organize a government that would rule on behalf of the bureaucracy.[28] This bureaucracy had two segments -- civilian and military. The elites from each group took turns dominating the government from 1932 until the late 1950s. The military's rise to political power was usually through a coup d'état, which had become a trademark of modern Thai politics.[29] With the

---

[27]According to one account, this traditional force was also reportedly manned by "crooks, slaves evading work, opium addicts, alcoholics and junkies." See Noel Alfred Battye, "The Military, Government and Society in Siam, 1868-1910: Politics and Military Reform During the Reign of King Chulalongkorn." Ph.D. diss., Cornell University, 1974.

[28]The core group of the khanaratsadorn or the People's Party which overthrew the absolute monarchy in 1932, were formed among civilian and military officials studying in Paris in the mid-1920s. It was composed of 34 army officers, 19 navy officers, and 45 civil servants.

[29]Between 1932 and 1992, there were nineteen attempted military coups. Most succeeded, while others failed to

exception of short periods of civilian government, the Thai political scene up until 1988 was dominated by the military. Throughout this period, the government bureaucracy remained an important political entity and the main power base of even the military-dominated state. It was largely through the bureaucracy that the state exercised its power over society. Much of this power was vested in laws, regulations, orders, and the constitution, all of which were created by the bureaucratic state elites.

In the year following the coup, the ruling People's Party also introduced a new administrative structure by abolishing the *monthon* and replacing it with the regional and provincial administration systems. The country was divided into four regions -- north, central, northeast and south. Provincial governors in each region now reported directly to the Minister of Interior who, together with the deputies, would divide their responsibility in overseeing the provinces on a regional basis. Meanwhile, a local government system was launched for the first time in 1933. This was not, however, a form of administrative decentralization, the Ministry of Interior still maintained networks of control over the newly established municipalities. In fact, local government in Thailand was seen as only "an extension of the political and administrative power of the central government in Bangkok."[30]

From 1939-1957, with the exception of a two-year interlude (1946-1948), Thailand was governed by a military dictatorship that attempted to put up a façade of democratic government. This period, which also coincided with the second world war, saw a rise in military nationalism as propagated by the leader Field Marshal Plaek Phibunsongkram or Phibun.[31] The most important indication of this state-bred nationalism was the change of the country's name in 1941 from Siam to Thailand to promote the domination of the ethnic Thai and their culture over "the others." Phibun also issued a series of decrees and *ratthaniyom* (cultural mandates or state conventions) designed to redefine Thaland as a modern nation. Some of these encouraged people to contribute to the strength of the nation by working hard, buying Thai goods, and respecting the national flag and anthem. Others laid down codes of social conduct deemed to be proper for the new "Thai" in the modern world. In addition, there were efforts by the state to undermine private businesses, which were usually stigmatized as

result in a change of government. Throughout this period, coups became the normal and expected way to change governments.

[30]Likit, "Thai politics," 429.

[31]In developing his version of military nationalism, Phibun and his chief ideologist Wichit Watakarn borrowed ideas from the Fascist movements in Europe and Japan, in which they saw parallel attempts to achieve national strength through the military.

being Chinese and alien, while supporting state-owned enterprises and ethnic Thai entrepreneurship.[32]

It was also during Field Marshal Phibun's period that the United States began to become involved in Thailand's security affairs. Indochina between 1945-1950 was one of the key arenas of the cold war. As the US decided in 1950 that it was necessary to fight in Vietnam to prevent the domino effect, Thailand became their front-line state in the region. Aside from using Thailand as a strategic base for US military operations in Indochina, the US also took an interest in the country's internal affairs. US policy-makers in this period believed that the best recipe for resistance to communism was strong government and economic growth based on private capital. To achieve the first aim, the US channelled enormous support to Thai military leaders and helped them consolidate their hold over the government. It gradually became clear to the Thai military leaders that the more they exhibited anti-communist sentiments, the more support they would receive from the US.[33] As for the second goal, the US strongly urged Thai military leaders to launch economic development programs that supported private capitalism.[34]

In the subsequent regime of Field Marshal Sarit Thanarat (1958-1963), who succeeded Phibun, both parts of this US recipe for anti-communism were realized, along with the harshest dictatorial rule in modern Thai history. Sarit successfully fused national security and national development, a success which earned him the dubious title of "the benevolent dictator." In a continuation of the expansion of domestic capitalism in the latter part of Phibun's rule,[35] Sarit established economic growth as one of the primary objectives of his government. The shaping of economic policy was largely put in the hands of a number of high-level technocrats who assumed leading positions in the bureaucracy. These technocrats were the products of Chulalongkorn's education reform and many state-funded scholarship programs for outstanding students to continue their studies overseas. The emergence of

---

[32]However, in the 1950s, the business leaders and the generals became new alliances and began to abandon state capitalism. The businessmen shared some of the profits of their private enterprises with the generals by having the generals sit on the boards of these enterprises and letting them make money from director's fees, patronage contracts, and various illicit techniques.

[33]From 1951 to 1975, the US channelled around US$2.5 billion in military support into Thailand, together with another US$625 million in non-military aid. These transfers had an enormous impact on the Thai economy. They eased Thailand's balance of payments position, stimulated local demand, and inflated government revenues. In addition, the US army, the CIA and the FBI also provided training for the Thai army and the Police to counter insurgency activities.

[34]Pasuk and Baker, "Thailand," 126.

[35]It should be noted that the expanding domestic capitalism in the mid-1950s was dominated by members of the military junta. These military elites sat on boards of various business concerns. This trend accelerated even further during Sarit's rule.

82

technocratic authority was effected through the establishment of several institutions to rationalize the government's development activities.   Among them were the National Economic Development Board (later renamed the National Economic and Social Development Board or the NESDB) and the Board of Investment (BoI).[36]   A close relationship was also forged between the technocrats and external organizations such as the World Bank and the US aid agency, who played an important role as policy advisers.[37]   This enabled the Thai government to draw on foreign financial and technical resources. apart from the military aid from the US. Japanese and Americans were the most important foreign direct investors.   During the 1960-1977 period, they held about half of the total foreign investment in Thailand.   This laid the groundwork for the massive expansion of industrialization in the subsequent decade.

As a surviving product of the 1932 coup, the bureaucracy, particularly the army, the Interior and Finance Ministries, and the Police, was very dominant in politics and policy-making under Sarit's rule.[38]   Thailand from 1932 to 1973 is often identified as a "bureaucratic polity" because of the heavy dominance of the political scene by bureaucratic elites and the virtual absence of extra-bureaucratic forces.[39]   Most premiers and cabinet members were either serving or retired military or civilian bureaucrats.[40]   Political parties, whenever allowed to operate, were often either the creation of or were under the patronage of leading politicians-cum-bureaucrats.   Organized interest groups such as labor unions or farmers organizations were few in number and weak in action.   Major policy decisions were thus made by bureaucratic elites who occupied both the key political and key administrative positions of the government, almost without input from any non-bureaucratic group.   Although the Thai

---

[36]The NESDB evolved from a public policy commission in the 1960s to a general economic watchdog in the 1980s. It is responsible for drafting national development plans. These plans, which are usually launched and enforced for a six-year period, set the theme and priorities for the country's development during that period. They also embody a commitment to laissez-faire policies whereby the role of the state is primarily to invest in infrastructure and support private sector growth. Presently, Thailand is implementing its eighth NESDB plan, which carries the theme of human resource development . As for the BoI, it has been. from its inception, playing a key role in promoting foreign investment by all sorts of incentives. This includes tax-holidays, tax-exemption for capital goods, the construction of economic infrastructure, among others.

[37]External agencies such as the World Bank and the US aid mission played a major role in influencing economic policy during the years of Sarit and his successors. The most important dimensions, perhaps, were, in encouraging domestic and foreign private investment and in reasserting the primacy of the laissez-faire market system.

[38]The expansion of the bureaucracy during this period was astounding. Take the civilian bureaucracy, for instance. In 1944, there were around 75,000 ordinary civilian officials. This rose to 250,000 in 1965. The number of government departments also increased from 49 in 1941 to 113 in 1969, and the number of divisions from 317 to 827 over the same period.

[39]The Thai "bureaucratic polity" was notably founded on the distinctive political apathy of the populace. This apathy was attributed largely to the fact that there had been no foreign colonial rule in Thailand to provoke a nationalist sentiment that would provide the ground for popular political participation after independence.

[40]After the 1932 coup. it was commonplace for top-level bureaucrats to assume dual positions -- as a government official in the bureaucracy and as a minister in the cabinet.

economy was organized along capitalist lines, the influence of organized indigenous business on government policy formulation was minimal. Businessmen could affect public policy only in a covert and particularistic manner through outright giving of bribes or creation of clientelistic ties with military-bureaucratic leaders. The effect was felt more in the implementation stage rather than in the formulation of policy.[41]

During Sarit's years, there was also another wave of government penetration into the countryside, one which was far more aggressive than that during the Chakkri Reformation. With new highways and electronic media, the central administration was able to penetrate more deeply and more extensively into rural society. This time, mass education, a project which was initiated by Chulalongkorn but was delayed until a generation later due to lack of resources, was also used as a means to incorporate the peasantry into the "modern" economic development.[42] Furthermore, Bangkok administrators were also more careful in assessing the social reality of each peripheral region as they channelled increased amounts of authority and patronage to village leaders -- village headsmen and commune chiefs -- in order to co-opt them into the central government pyramid as the lowest rungs of the provincial administration. These efforts coincided with intense psychological warfare against communism being waged countrywide. As the US became a prominent player in Thailand's internal affairs, many rural development projects were carried out with US support and a characteristically anti-communist bias.[43] Despite some resistance, a large number of village communities were pushed into retreat from state penetration during this period as many village heads became the central government's agents through whom the district office, the land department, and the police carried out a wide range of activities in the villages.

[41]The bourgeois or business class in Thailand were mostly ethnic Chinese who before the policy turnaround in the 1950s had to face nationalistic-minded governments. Therefore, they had to resort to covert methods in order to affect public policy. See more in Anek Laothamatas, *Business Associations and the New Political Economy of Thailand: from Bureaucratic Polity to Liberal Corporatism* (Oxford: Westview Press, 1992), 2.

[42]During the 1960s, thousands of primary schools were built in the rural areas and by the 1970s the majority of rural children were getting four years of compulsory schooling. Meanwhile, tertiary education, which used to be reserved for members of privileged and aristocratic classes, also expanded tremendously. Between 1961 and 1972, the number of universities expanded from five to seventeen, and the student enrollment from 15,000 to 100,000. See Pasuk and Baker, "Thailand," 301.

[43]For instance, during the late 1960s, the Department of Local Administration, which is the Ministry of Interior's core agency for provincial administration, recruited a number of village leaders to go on a field trip to the US . Under the sponsorship of the US government, these local leaders spent two months site-seeing around US cities and towns and learning about American culture and political system. According to a commentator, one of the recruited *kamnan* (commune chiefs) was selected because he successfully masterminded an assassination of an important activist and Communist sympathizer who was hiding in his village. See Khaen Sarika, *Vara sutthai haeng chiwit Jitr Phoumisak* (The last hours in the life of Jitr Phoumisak) (Bangkok: Sarika Press, 1988), 119-120.

Even after Sarit's death in 1963, the legacy of anti-communism, economic development, and the "bureaucratic polity" continued to dominate the Thai scene well into the mid-1970s. Nonetheless, by 1965 amidst strong anti-communist currents, the Communist Party of Thailand (CPT), which was involved in armed insurgency activities, managed to make inroads into some social circles, most notably college students and labor unions. With their leftist ideas and strong political motivation, these two groups formed a leading force against the dictatorial rule of the military cliques. In the early 1970s, college students, many of whom belonged to the first tertiary-educated youth from non-bureaucratic catchment, organized a number of demonstrations against the government. One massive protest that was organized in October 1973 led to a bloody clash with riot police and the armed forces resulting in more than one hundred student casualties.

Besides the students' movements, the early 1970s also saw outbreaks of protests by peasants in the rural areas of the country. The protest focused on two major problems: 1) indebtedness and land loss as a result of rapid swings in international crop pricing and cheating by moneylenders, and 2) a rising ecological crisis from massive deforestration. Students helped bring these local protests out of the villages and onto the national stage. In 1974, a protest was staged in a Northern province demanding higher paddy prices and government assistance with excessive interest rates and landgrabbing. Over the next few months, the protest, with the support of students and participation from peasants in other provinces, snowballed into a countrywide peasant movement. More than 7,000 of the protesters announced they were ready to burn their identity cards and set up liberated areas in the countryside. This campaign finally pressured the government into passing a rent control bill and taking steps to guarantee land rights. Meanwhile, the leaders of the movement founded the *Sahaphan Chaona Chaorai Haeng Prathet Thai*, or the Peasants Federation of Thailand (PFT), which was to become a major national platform for the peasantry to assert their importance in the future.[44]

Although the aftermath of the historic October 14, 1973 incident brought about a reintroduction of the constitution and a brief return to democratically-elected government in 1973-1976, it was short-lived. The remnants of the powerful military clique and the allied rightist paramilitary groups struck back a few years later against the reckless students, killing some 1,300 and wounding many more.[45] However, the repressive government that emerged

---

[44]Pasuk and Baker, "Thailand," 297-298.

[45]The October 6. 1976 massacre was probably the bloodiest crackdown on pro-democracy movements in Thai history. It featured atrocious violence in the forms of burning, hanging alive, and killing of unarmed and defenseless people. The right-wing allies were vehement to crush members of the student movements. One

following this bloody crackdown could not return Thailand to authoritarianism for long. With the widespread resistance from urban intellectuals, it was deposed by yet another coup in late 1976 after less than a year. The most enduring post-1976 regime was that of General Prem Tinsulanond which lasted from 1980 to 1988. Prem's period was regarded as a "semi-democracy" because it featured a compromise between full-blown liberal democracy and military dictatorship. The government would be a coalition government comprising popularly elected MPs from three to four parties headed by a respected retired general -- Prem himself -- as premier and with prominent military-civilian bureaucrats as ministers of key portfolios such as Defense, Interior, or Finance. Prem retired from politics in 1988 giving way for Chatichai Choonhavan, leader of the largest elected party in the 1988 election, to be the first civilian prime minister in more than a decade.

On the economic front, Sarit's emphasis on national economic development finally bore fruit. Economic growth was remarkable in the 1960s and continued to climb in the 1970s.[46] In a little more than a decade, the Thai economy was transformed from a small agrarian economy to a major agro-industrial economy that was on a path to full-fledged industrialization. The main driving force behind this transformation was an alliance between the bureaucracy and business. This alliance gave rise to massive expansion of import substituting industries -- principally agrarian and textile products -- which in turn pulled thousands of people out of the villages and into factories and service businesses in the city. The penetration of agri-business not only changed cropping patterns but also social relations and the distribution of wealth and power throughout agrarian society. This change continued and deepened into the 1980s when the government shifted to a more export-oriented industrialization that caused a dramatic economic growth.[47] The major shapers of this policy shift were the World Bank and local business leaders, who had by then formed into identifiable groups and negotiation organizations. The former put pressure on the Thai government through its loan contingency which prescribed a major institutional and policy reform to reorient the economy towards exports. The latter worked discreetly behind the scenes to influence the government to change their economic strategy to exports. The country's

---

Buddhist monk, Phra Kittivutho, was a spiritual leader in this right-wing group. He was notorious for his unorthodox preaching that killing communists is not a sin, but instead a merit, as it would help save the country.

[46]Between 1960-1970, Thailand's annual GDP grew at a rate of 9.7 per cent and escalated to an average of 17.5 per cent between 1970 and 1980.

[47]In the 1980s, Thailand enjoyed an average GDP growth of 11.2 percent. Over the 1965-1988 period, the share of agriculture in GDP declined from 32 to 17 percent while that of manufacture increased from 14 per cent to 24 per cent. Even more prominent was the increase in the share of manufacturing in total exports which jumped from 5.5 percent in 1970 to 30.1 percent in 1980. See World Bank, *World Development Report 1990* (Oxford: Oxford University Press, 1990), Table 2, 180-181; Table 1, 178-179; Table 3, 182-183.

economic ascendance from the mid-1980s onwards will be discussed in detail in the next chapter.

To sum up, following the 1932 coup, the modern government bureaucracy became the core of the polity and the most prominent social group after it was cut loose from the control and reward system headed by the monarch. Emerging security problems together with an extensive dictatorial regime intensified the bureaucracy's exceptional power and its centralized control on the populace. In the middle of the twentieth century, other new social groups such as businessmen, urban intellectuals or urban labor played a relatively minor role in politics and in influencing public policy formulation as they were still tied as clients to patrons among bureaucratic elites. Thus, for much of the period between 1932 and 1973, the state, represented mainly by the government bureaucracy, was dominant while extra-bureaucratic forces in society remained weak. The "administrative-centered state" began to decline in the mid-1970s because of the emergence of new social forces, first the students in the 1970s and later the businessmen in the 1980s. The decline of the "bureaucratic polity," particularly as a result of the penetration of business groups and other social interest groups, will be dealt with in the next chapter.

STATE SURVEILLANCE AND RESISTANCE FROM 1932 TO 1982

Aggregate Surveillance Of The Populace

In the post-1932 coup period before the 1980s, aggregate surveillance strategies in Thailand tended to highlight the security dimension, which was a primary concern of the state at the time. In 1942, the Phibun government conceived the idea of a national identity card during the Japanese occupation in World War II. In 1943, the National Identity Card Act B.E. 2486, the first of its kind in Thai history, was passed, but the law could not be implemented at once due to lack of resources. Ten years later, it began to be enforced on residents of the cities of Bangkok and Thon Buri. Officially, the objectives in launching the ID were: to furnish a legal proof of identity, to facilitate law enforcement officials' efforts to combat crime, to indicate eligibility for social services, and to be a means of verifying voting rights at elections.[48] With the benefit of hindsight, the faint democratic connotation in the last objective seems absurd. Phibun was notorious for his authoritarian rule and his lack of respect for

---

[48]Thiang Chalermchuang, "Control of Citizens," 37.

democratic procedure. In fact, Phibun himself was responsible for masterminding a major poll fraud during an open election, which later came to be known as the "dirty election" of 1957. Given his strong nationalist predisposition and his fervent effort to contain the Chinese in urban business, the conception of the new identity card was likely inspired more by his desire to reorient the country towards a new military nationalism in addition to war time necessity. Notably, from the late 1930s until the early 1950s, the Phibun government consistently argued for increasing government control over the urban economy, which was dominated by Chinese businessmen. By enforcing a national identity card on all urban residents -- Bangkok and Thon Buri, the government was equipped with an effective means to single out the Chinese, who were subsequently levied special taxes and subjected to all types of harassment.

The new ID card, which was first issued in 1953, featured a long piece of paper folded into quarters. It contained the following information about the cardholder: name, date of birth, current address, profession, complexion and build, mark, nationality, ethnicity, name of father, name of mother, address of place of birth, photograph, fingerprint of right thumb, signature of cardholder, place where the card was issued, date of issue, card number, and signature of official who issued the card.[49] All Thai citizens aged between sixteen and seventy in the Bangkok and Thon Buri area were legally required to apply for the card. Only the handicapped, mental patients, and prisoners were exempted. This ID card was valid for ten years.

Apart from introducing a national identity card for citizens, the nationalist Phibun government also for the first time put foreigners living in Thailand under the state's registration system by passing the Alien Registration Act B.E. 2479 in 1936. According to this law, which was revised and reenacted again in 1950, aliens or resident aliens referred to all people who currently resided in Thailand but were not of Thai nationality. The law required that all resident aliens who were twelve years of age and older acquire an alien document from the designated authority in the district and report to this authority any important changes in their activity -- birth, death, relocation. Only a few categories of aliens are excluded from the law -- diplomats, the United Nations employees, and the Royal Thai Government's employees. This law is still in effect today.

The Phibun-inspired ID card (for citizens) was short-lived and was replaced by a new card when Sarit took over. In the early 1960s, a border crisis in the Northeast was escalating

---

[49]Ibid., 38-40.

as a large influx of Laotian and Cambodian refugees migrated into Thai territory after civil war broke out in Laos. Meanwhile, the southern border was also increasingly threatened by Chinese Communist guerrillas from Malaya. After both Laos and Cambodia fell under the influence of Hanoi in 1964, the Thai government opened its door for the US to station troops. The next few decades would see a strong US military presence in Thailand both as a base for the fighting in South Vietnam as well as an effort to counter the spread of communist insurgency into Thailand. As people in Indochina had similar ethnic features and shared several cultural and linguistic traits, it was difficult to distinguish the Thais from "the others." As a result, the Sarit government decreed the requirement to carry a new national identity card and assigned the Ministry of Interior the task of issuing the card. The new card, as a classified document puts it, was primarily meant to be a means of prevention and control of illegal border crossings, one which would benefit both the state and the citizens (See Table 3.1).[50] In a bid to cope with the mounting border pressure, the despotic Sarit ordered that the issuing of the new card be completed nationwide as soon as possible. The Ministry of Interior responded with a three-year plan, starting in 1962 and ending in 1965. In the first year, twenty provinces would be covered with priority given to border provinces. Except for Bangkok and Thon Buri, the remaining eighteen provinces under the first-year plan were provinces bordering Malaysia and war-torn Laos and Cambodia. About fifteen million citizens were to be covered under this card-issuing plan.

The issuing of the new ID card was wholly centralized within the Department of Local Administration under the Ministry of Interior. All cards carried the signature of the minister in Bangkok. Unlike the Phibun-inspired ID, the new ID was much smaller in size and carried far less information. Its design was similar to any ID card today. The card was a six-by-nine centimeter rectangle. The front featured the garuda emblem of the royal Thai government together with the words, the Office of the National Identification and Registration, the Ministry of Interior. It also indicated the issuance and expiry date. The back of the card had a photo of the cardholder laminated into the card with a corresponding registration number underneath the photo. It also carried the following information: name, date of birth, address according to household registry, the signature of the official who issued the card, and the name of the district in which the cardholder resided. All Thai citizens were required to apply for the card with the exception of people in certain categories. For instance, immediate royal family members, members of the privy council, military-bureaucrat officials, members of parliament,

---

[50]Ibid.. 42.

officials of local governments. monks. priests. the handicapped. prisoners. and mental patients. This new ID card was valid for six years unless renewed.

Table 3.1
Comparative Summary of Benefits from
the new National Identity Card
for the Thai State and the Thai Citizens

The State	The Citizens
1. Civil registration work could be improved with the ability to identify the citizens by their appearance.	1. The new ID card would serve as a legal document for each citizen to identify himself/herself, and also as proof of innocence.
2. Verification of voters could be facilitated during elections, hence reducing the rate of fraud.	2. Each citizen could use the national ID as an identification document in place of household registry, conscription form, or marriage certificate when they needed to communicate with the bureaucracy.
3. Without a proper ID, aliens could be more easily distinguished from Thai citizens.	3. The new national ID would be a supplemental piece of identification evidence to cross check with other documents.
4. Illegal immigrants at the border could be better identified and suppressed.	4. The new national ID would be useful for other transactions which would require some form of identification.
5. The new national ID would be useful for prevention and control of terrorism, and of infiltration by Communist insurgents and subjects who would be threats to national security.	
6. The new national ID would aid in the accumulation of population statistics. With all the collated information from each ID application, the state could better arrive at a demographic profile of the population.	
7. The new national ID would be useful for the police in criminal investigation as the personal information of each citizen including his/her photo would be collected and stored at a central base of reference.	

Source: Thiang Chalermchuang, "Control of Citizens for National Security," (*karn kuabkum phonlamuang kiawkab khwam mankhong khong chart*), (Special degree thesis, National College of Defense, 1965), 50-51

In accordance with the overall structure of state administration at the time, the collection and storage of information under the new national identification plan was highly centralized. Card applicants had to fill out application forms at their respective district offices before the completed applications were sent, via an internal mailing system of the Ministry of Interior, to the Registration Administration Bureau in Bangkok for processing. There information from each application would be copied and the copy stored in a central dossier.[51] Approved applications would be issued new identity cards which would be sent, via the same means, back to the originating district offices. The entire process could take up to six months, depending largely on the proximity to Bangkok of the district office from which the application was sent.

As far as the public response to the new cards is concerned, there is no recorded evidence of objection or resistance of any kind. The compliant attitude towards this new state surveillance project can be attributed to three important factors. First, it is likely that Thai citizens had by this time grown accustomed to being "surveilled" by the state given the country's extensive history of tight control of manpower and the civil registration process already in place. In an environment where political choice was minimal and civil rights were unheard of, Thai citizens had no legal grounds for not cooperating with the authorities in such matters. It should also be noted that respect for authority had always been an important value in Thai society and one which was further stressed under the military dictatorship of Sarit.[52] Second, and related to the first factor, the new ID card was conceived during a time when Thailand was facing security problems from communist insurgency and illegal border crossings. The ruling government was thus able to justify the launching of the new card as a national security measure, by drawing upon the perceived need to combat communism. As a result of the intense psychological warfare against communism disseminated through radio and television, anti-communist sentiments were high in Thailand, except in certain radical university and union circles. The military government was opportunistic in capitalizing on these patriotic sentiments to enforce the national identity card law.

---

[51]During this period, the copying of information was done by hand, either handwritten or handprinted. Officials in Bangkok simply transferred the same information onto an identical standard form. No electric photocopiers were in use at the time.

[52]In Thailand, people in authority, particularly bureaucratic officials, have always been referred to by the term of *phu yai* (big people), while ordinary people are known as *phu noi* (little people). These terms do not necessarily contain negative connotation. They only indicate the social hierarchy in the Thai social order.

In addition, the introduction of the new national identity card in 1962 also worked in concert with the second attempt by the Bangkok government to penetrate peasant society. Apart from the co-optation of village leaders into the central bureaucratic structure, this second wave of government intrusion also saw the spread of mass education into the villages. Increasingly, the peasants saw education as a means to climb the social ladder, one which would enable their children to enter the privileged and prestigious bureaucracy. In order to enroll their children in schools, parents were required to have proper official documentation, which included a household registration document and, if available, national identity cards (for the parents). As a result, civil registration was gaining importance as a passport to modern education for the peasants. This, coupled with increasing enforcement by assimilated village heads and commune chiefs, paved the way for the introduction of the new national identity card, which was to become a crucial part of the Thai people's life in the next generation. On this note, it is worth mentioning that by the early 1980s, the catchment for higher education had significantly changed, and more students now "came from a small-town lower-middle class that, in their generation, for the first time in Thai history gained access to higher education."[53]

The impact of the introduction of the national identity card was gradual and initially incomplete. While in theory this new document could instantly supplement the existing civil registration system with an ability to identify all card-holding citizens by their photos, the situation was much more complex in practice. In the absence of advanced and high-quality imaging and data-processing technology, the newly-introduced card and the related information storage were relatively poor in quality. For instance, the photo, which was in black and white, was usually smudged, shadowed, out-of-focus, or unclear. In some cases, it was impossible to use the photo ID as a reliable identification. The lamination on the card was also not water-proof and often peeled off easily. Moreover, since this 1962 version of an ID card involved relatively simple technology in the card-making process, it gradually became susceptible to widespread fraud. According to a study by an interior official, it was the prevailing rate of fraud, particularly in the border provinces that led to the replacement of this card with a new and computerized version in 1983.[54]

Meanwhile, the storage and retrieval system of personal information of citizens at district offices countrywide relied exclusively on conventional filing cabinets and manual

[53]Benedict R. O'G.Anderson and Ruchira Mendiones, *In the Mirror: Literature and Politics in Siam in the American era* (Bangkok: Duangkamol, 1985), 41-42.

[54]Chodok Veeratham Poonsawat, "The Project to Issue Citizen Identification Number: National Security and the Right of the Citizen," (*Khrongkarn chatthani lekprachannua prachachon kab khwammankhong khong chart lae sitthi khong prachachon*). (Special degree thesis, National College of Defense, 1983), 14.

search. As the amount of information grew. so did the difficulty in storing and retrieving information. The same system was also used at the Registration Administration Bureau in Bangkok, where a massive and centralized pool of information on all card-holding and registered citizens was stored. This central storage has been held as the core of the country's civil registration system and one which was supposed to be updated constantly. For instance. if a person reported birth, death, marriage. or relocation to his or her affiliate district office. this change would be notified, via an internal mailing system of the Ministry of Interior, to the Registration Administration Bureau in Bangkok where the change would be made accordingly. This centralized system of collection and storage of population information, it should be noted, rested upon a notoriously slow and inefficient bureaucratic system.

Due to bureaucratic red tape and the highly centralized card-issuance system, nationwide coverage was significantly delayed. particularly in remote provinces. In addition, since the concept of the ID card was relatively new, certain groups of people who already held some form of official ID were not responsive to it. For instance, members of the state bureaucracy or the *kharatchakarn*, both civilian and military, were technically exempted from the requirement to apply for the new card since they were able to get by with their official bureaucratic ID in their daily activities. Ultimately, it was mostly ordinary citizens, or more precisely, those from the non-bureaucratic and non-aristocratic classes, who were subject to this new form of state surveillance when it was first introduced.

As time passed, the use of the national identity card grew by leaps and bounds, not only in official transactions but also in more ordinary activities. By law, all citizens who are eligible cardholders -- those who are 15 years of age or older -- are now required to carry a national identity card in public at all times. Failure to comply is considered a violation. Police officials also have the right to ask to see a person's ID card on public premises at any time. Gradually, Thai people also came to habituate themselves to presenting their ID card or submitting it as a security deposit when visiting official or company premises. This demand for submission of ID at offices is believed to have begun during the late 1960s in the midst of the Cold War and Communist insurgency when security concerns were high. Meanwhile, as new factories were being set up in Bangkok and the outlying provinces and workers pulled from the countryside, employers also required that prospective employees produce a copy of their national ID card and household registration document as a show of good faith. Prior to the arrival of photocopying machines, these migrant laborers had to obtain a hand-written copy of these documents from officials at district offices where they were registered. Often these officials, who were at low official salary levels. would extract unofficial fees for such

services.[55] In fact, district officials particularly in the civil registration section, have for a long time been notorious for being corrupt and intimidating to poor and underprivileged peasants. As use of national identity cards and household registration documents became more widespread, the window of opportunity expanded for registration officials to make an extra-extraction from their record-keeping and retrieval services. After the introduction of photocopiers to civil registration work in the early 1980s, the practice of commissioning hand-written copies of registration and identification documents became obsolete. Yet, registration officials still found new ways to "squeeze" those within their power -- the poor peasants as well as wealthy people who were willing to pay to expedite the services.

Police Surveillance Targetted on Dissidence

In line with aggregate administrative surveillance, which reflected the emphasis on national security, police surveillance during the dictatorial period also resonated a similar priority but with a political twist. During Phibun's rule, for instance, police surveillance functioned as a means to suppress dissidence or what Phibun considered to be threats to his system of rule. Although the police department was established in 1897 by King Chulalongkorn, it was more of an administrative unit to oversee provincial police forces and to suppress other illegal activities rather than a political force. Under Phibun, the police became a counterweight against other armed forces and a personal army of the dictatorial premier. In the early 1950s he founded the Special Branch Police, which specialized in surveillance, espionage, and suppression of terrorism and political dissidents. Although written records were difficult to come by and few survivors of Phibun's suppression lived to tell the tale, there are reasons to believe that target surveillance must have taken place as early as the 1940s.[56]

In this period, "communism" was a convenient label for any kind of dissent and continued to be so for the next three decades. In 1952, Phibun reenacted the anti-communist law.[57] This automatically empowered local law enforcement officials, the police, and all levels

[55]The revenues raised from this illicit practice were usually divided up into portions, some of which would go to the collectors themselves and others to superiors up the line of command.

[56]Incidents of arrests and disappearance of political dissidents became increasingly apparent in the 1940s. For instance, in 1947, the police, under Phibun's order, arrested several people from the Bangkok Chinese community on grounds of political connection with mainland China. In 1952, more than 100 writers, editors, labor organizers, Chinese community leaders, intellectuals, and other dissidents were arrested on grounds of suspected communism. Many were jailed for a number of years. See more in Pasuk and Baker, "Thailand," 271.

[57]The first Anti-Communist Act was enacted in 1933. Then, the Communist movement was still small and relatively inactive. This law immediately outlawed the Communist Party, which then went underground and did not emerge again until the 1960s.

of administrators of the Ministry of Interior to undertake surveillance of potential communists and to arrest them, if need be. Such vigorous suppression of "communism" continued into the Sarit period (1958-1962). This led the Communist Party of Thailand (CPT) to abandon the parliamentary route to power and to concentrate on the rural areas as part of their pursuit of the "countryside surrounding the city" strategy.[58] During the late 1950s and the early 1960s, left-leaning students, who were not necessarily communists, also began traveling to the countryside in an effort to reach out to the rural peasantry. According to one of these former political activists, the students were kept under close scrutiny by provincial authorities watching for any action that could be interpreted as "communist" or a "threat to national security."[59]

At first, information from hired informants and agents was key to surveillance in the countryside, according to a retired army general who played an important role in suppressing a communist stronghold in the Northeast.[60] Before the US involvement in countering communist insurgency in the mid-1960s, there was really no significant technology involved in surveillance work. Informants usually had a strong anti-communist bias and gave much information that was inaccurate and unreliable. In the 1970s, however, defectors from the communist movement were hired as informants along with village volunteers.[61] Use of surveillance technologies also increased and became very useful in monitoring and hindering insurgent activities.

In the urban area, plainclothes police from the Special Branch were always on the lookout for left-wing political deviants on university campuses where most political demonstrations took place. Many of these police officials mingled in the campus crowd passing as fellow students. By the early 1970s, when student movements were widespread and a high time for socialism in Thailand, many prominent student leaders were also closely watched by Special Branch Police. By this time, the Thai police had also been thoroughly-trained by the CIA.[62] Their information-gathering techniques became much more sophisticated. According to a senior Special Branch Police official and a veteran in police

[58]This strategy derived from Maoist "countryside surrounding the city" strategy.

[59]Mr. Dej Bhumikacha, president of the Thai Volunteers Association, interview by author, 25 April 1996, Bangkok.

[60]Gen. Phichit Kullavanit, member of the privy council, interview by author, 11 June 1996, Bangkok.

[61]As part of its assistance to the Thai government to counter insurgency, the US also provided funds for recruiting anti-communist village volunteer forces.

[62]The US military took over direct responsibility for training Thai police in counter-insurgency work. The CIA was brought in to organize the Thai police for specialized operations. Between 1965-1968, the Thai police force increased from 51,000 to 80,000 men. By one estimate, half of all US economic aid in the period of 1965-1969 was channeled to the police. See Pasuk and Baker, "Thailand," 277.

surveillance on dissidence, the Special Branch Police had constructed detailed files on student leaders and other political dissidents. Much of this information was inevitably obtained from the Civil Registration Office where these dissidents' household registries and personal records were kept.[63]

After the two bloody crackdowns in the early 1970s, surveillance and harassment of left-leaning students and social activists continued. In fact, this practice continued even after the policy turnaround from the extreme right in 1976 to a more moderate policy of trying to win over the students-turned-insurgents through a political campaign.[64] For example, a former student activist, who joined the insurgency movement after the 6th of October 1976 massacre said her mother, who resided in Bangkok during the turbulent time, was kept under surveillance by the Special Branch Police for at least five years. During this time, she herself was with the insurgency movement in the Northeast. The ordeal ended when the family moved to a new residence in a different city.[65]

Surveillance Of Criminals

In a separate but related development, the collection of criminal fingerprints continued at the Fingerprints Department. Between 1908 and 1931, the size of the criminal fingerprint record system grew significantly as different types of records were added to the storage. For instance, in 1908, the Metropolitan Police Department began to store at the Fingerprints Department fingerprint records of Thai citizens who were driven into exile and children who were sent to correctional schools. In 1914, the Army requested the Fingerprints Department to store fingerprints of soldiers who were convicted on criminal charges as well as fingerprints of those soldier-prisoners recently released from prison. During this time, the recording and storage systems were also upgraded. Thai numerals and symbols used to mark fingerprint cards were replaced with the more internationally recognized and more standardized Arabic numerals and symbols. New standardized drawer cabinets with more storage space were also imported from overseas to accommodate the rising number of fingerprint cards. Meanwhile, the use of these records also increased as more organizations sent in more fingerprints for record checks. By 1914, fingerprints of applicants for guns licenses and for all types of

---

[63]Major Police Gen. Yothin Matthayomnand, deputy-commander of the Special Branch Police, interview by author, 20 August 1996, Department of Police, Bangkok.
[64]This refers to the Prime Minister's Office Order, No. 66/2523 issued in 1980 and 65/2525 issued in 1982.
[65]Ms. Nidhinand Yawsaengrat, interview by author, October 7, 1996, Bangkok.

vehicle drivers' licenses as well as fingerprints in legal contract documents were sent to the Fingerprints Department for background checks.[66]

As a result of the expansion in size and use of the criminal record system, a new and more durable type of paper was introduced in 1932 to replace the deteriorating paper used for fingerprint cards. The record system was also revamped as only those prisoners with more than two jail terms were included in the department's fingerprint cards and criminal history files. In 1952, as the Fingerprints Department was inundated with incoming fingerprints records and record check requests from various organizations, it began adopting the British method of fingerprints verification, which was more systematic and scientific. Nevertheless, the new system still relied mainly on humanpower to manually and visually detect patterns of minutiae, with little help from any technology other than a magnifying glass, paper, and a pencil. In 1960, the Fingerprints Department was transferred to the Police Department and renamed the Criminal Records Division.

In the decade after its establishment, the Criminal Records Division benefitted significantly from the US presence in Indochina during the Cold War crisis. As mentioned earlier, a large portion of US aid to Thailand during 1965-1969 went to the police for financial support and training. The FBI was, at this time, involved in training the officials at the Criminal Records Division to use U.S. fingerprints classification technology. The FBI technology was based upon the coding of minute details in fingerprints using the right thumb as the main indicator. Records with the same pattern of minutiae for the right thumb were grouped together in the same category and further sub-divided within that particular category depending on the minutiae of other fingers. Although this method of classification provided an organizational edge over the British method, it remained a primarily manual technology highly prone to fraud, inaccuracy and inefficiency. As the number of incoming requests for criminal record checks increased over time, problems associated with the manual system became more apparent. Up until the early 1990s, the criminal records division coped with these problems by adding more staff to handle coding and record matching jobs and by expanding storage space, cabinet drawers, and other equipment. The division expanded from dozens of staff working in a small office in 1972 to 392 staff working full-time in a three-storey building in 1988. In the meantime, the number of records in their fingerprint and criminal history files also grew consistently to fourteen million by 1989.[67]

---

[66]Department of Corrections, "*History of Penal System,*" 13.
[67]Ibid., 16. This exceptionally high figure obviously reflected the inclusion of records submitted for employment and licensing screening aside from ordinary criminal records.

After the 1932 coup, the mainstay of civil registration work -- household registries -- was put to an additional use, that is, to construct voter lists for election of Members of Parliament (MPs). Prior to the country's first general election in 1937, the Ministry of Interior in 1936 ordered a nationwide population survey to update the existing registration records. Ever since, every election has relied upon the Ministry of Interior's civil registration records not only for the listing of voters but also for the calculation of the number of MPs for each constituency.

In addition, in 1956, the Ministry of Interior enacted Civil Registration Act B.E. 2499, which incorporated and revised all existing laws relating to civil registration. This law systematized the civil registration process by establishing five hierarchically-ordered civil registration offices -- central, provincial, district, sub-district, and municipal. What had been the census section within the registration division of the Local Administration Department now became the Registration Administration Bureau. It oversaw civil registration work in offices at the four lower levels and also at the Thai Consulates and Embassies abroad. Moreover, it coordinated with other agencies or government departments that dealt with or might benefit from civil registration. For example, the Police Department, the Ministry of Public Health, and the Ministry of Foreign Affairs. This administrative setup has remained largely unchanged to the present. The Civil Registration Act, however, was reenacted in 1991 due to the need to cope with computerization of the civil registration process.

According to the 1956 Civil Registration Law, civil registration work under the jurisdiction of the Local Administration of the Ministry of the Interior had the following objectives:

1) to facilitate government administration and to promote national security;

2) to serve as legal evidence and central means of verification of a person's identification and personal history;

3) to accumulate demographic information about citizens for the purpose of public policy and planning in the areas of national defense and national development; and

4) to protect the rights of Thai citizens and to facilitate the exercise of these rights and the rendering of public services for them.

CONCLUSION

During the period studied in this chapter, the rise of the Thai modern state, which began in the late nineteenth century, was the major force that shaped the nature of state surveillance. Initially under an absolutist rule, the royal leaders constructed a new centralized bureaucracy to bypass the old nobility in state administration. At the same time, they defined new borders, drafted new codes of law, and formed new armed forces, which together provided the new state with an ability to monopolize the use of force within a given territory and the newly-constructed bureaucracy with the means of subjecting its population to detailed surveillance. This semi-modernized bureaucracy, which replaced the traditional *sakdina* administration, opted for more rationalized and bureaucratic modes of surveillance through registration documents and population surveys. Unlike in the traditional period in which state surveillance was openly used to promote class oppression and exploitation, new modes of surveillance were gradually legitimized under the less arbitrary claims of law and public policy. In addition, this new face of surveillance became integrally linked with the extension of citizenship, a novel concept to the majority of the population (the former *phrai*) who were only recently freed from corvée obligations and indentured services. In the new surveillance scheme, each person was no longer identified by his or her affiliation to a certain *mun nai*. Instead, each person, regardless of his or her ethnicity, was for the first time identified as an individual, and as a citizen of the "mystic" nation of Siam .

Despite the centralization and systematization of information collection and storage by the state, surveillance under the absolutist rule had limited success, particularly in the rural villages where peasants were reluctant to cooperate with officials from the central government. Since one of the main purposes of data gathering in this period was taxation, the other being the keeping of population statistics, evasions of registration were rampant in the hinterland. In this light, the collusion between peasants and their local leaders -- village headsmen and commune chiefs -- worked to shelter rural autonomy from the encroaching central state. Since the bureaucracy was new and still limited in its administrative reach, it was unable to surmount this "dialectic of control" advanced by the local peasant community. Thus, the expansion of surveillance during the absolutist state only achieved a larger but far from complete information base on the subject population and an improved supervisory capacity over a primarily urban populace.

Over the years, however, the bureaucratic and rationalized surveillance systems, whose foundations were laid during the absolutist period, increasingly became a crucial administrative basis for a more effective operation of at least three institutional sectors of the modernizing Thai state -- the state bureaucracy, the police, and the armed forces. In the decades following the 1932 coup, surveillance activities carried out by these institutions became even more profound with the application of new technical inventions such as printing, photography, and new data-gathering and processing technologies including population surveys, document filing, identity cards, and fingerprints classification techniques. Some of the modern technologies were transferred from Western countries (primarily the US), which came to play a prominent role in Thailand's modernization program. At the core of the modernizing bureaucracy is the Ministry of Interior, which was chiefly responsible for the furtherance of state surveillance activities at an aggregate level through its countrywide civil registration system. By deploying the new technologies and by administering surveillance through its expanding networks of authority borne along by new highways and electronic media, the Ministry of Interior was able to penetrate more deeply and more broadly into the lives of the Thai people even in the rural areas.

In the 1950s-1960s, which saw consolidation of dictatorial rule, state surveillance also began to develop a new tendency -- an extreme focusing on certain social groups who were perceived as threats to the leaders and their system of rule. The use of target police surveillance as an element in totalitarian rule intensified as the threat of communism loomed large in Indochina and insurgency movements mushroomed in the Thai countryside in the mid-1960s. At an aggregate level, the Ministry of Interior, driven by the perceived need to combat communism, also introduced a new mode of "surveilling" the subject population -- national identity cards. This card increasingly became an important official paper, one which is now mandatory for a significant portion of the population, and which is used to follow even the most ordinary of activities.

Although the way Thai people have become habituated to the use of national identity cards and household registration documents over the years might have contributed to the state's social control measure, the actual surveillance capacity of the state was still marred by several factors. First, and foremost, was the internal weakness of the government bureaucracy -- red tape and inefficiency -- which became increasingly apparent with time. As this bureaucracy expanded, its highly centralized organizational structure, which was originally intended to create the utmost centralization of power during Chulalongkorn's reform, proved to be a major impediment for efficient operations. A good illustration is the case of the Ministry of Interior's national ID card system. While the Ministry might be able to amass a larger file of information

on the subject population and to centralize its control on that information base, it managed the flow of information between the central base in Bangkok and the district offices poorly. Aside from the extremely centralized chain of control, the slowness of this flow can also be attributed to limited technological capabilities in the means of transportation and communication as well as the ineffectiveness of clerical officials, who are usually underpaid and unmotivated.

Secondly, while the Chulalongkorn-created bureaucracy may have taken the form of a rationalized modern organization, it was, even after the 1932 coup, still held together internally by strong traditional bonds of clientele and exchange. Typically, corrupt activity by lower-ranking officials was systematically organized to raise unofficial revenues, portions of which were passed up the line to senior officials in exchange for career advancement opportunities. In many ways, this practice of nepotism is reminiscent of the patron-client relations inherent to the traditional *sakdina* system. This tendency to corruption, which became institutionalized in sections of the service-oriented civil registration system, gave rise to widespread fraud and swindling, particularly in remote provinces. Ironically, while one of the original intents of the state in issuing national identity cards was to ward off illegal immigrants, it so happened that in many cases registration officials in provincial posts were paid to issue fraudulent cards or to tamper with registration records precisely by immigrants wishing to obtain Thai citizenship.[68]

In any case, the inherent inefficiency and rampant corruption within the Thai bureaucratic civil registration system could be seen as a blessing in disguise from the standpoint of one wary of the power of an overpowering state. This is because, despite the expansion of the documentary activities of the state during this period, the systems of collection and collation of information were too poor and incomplete to amount to any significant control. Besides, members of the subject population could always resort to collusion with corrupt officials as another avenue to evade the state's control over their lives. Yet, these plausible channels for a "dialectic of control" should not lead one to underestimate the power of the state as administered through several surveillance schemes. As will be illustrated in the next chapter, the pervasive state surveillance system has over the years grown with increasing momentum, gradually enclosing more and more of the daily life of the general populace with a penetrating gaze.

---

[68]Although no exact number of ID fraud cases were detailed, evidence indicated that a significant number of them were inside jobs. In most cases of fraud, which usually involved illegal immigrants, the major motive was to obtain Thai citizenship. Nevertheless, there also existed other types of frauds -- of both ID card and household registration documents -- which were carried out by people outside of the bureaucracy. As mentioned, the technology involved in the making of the 1962 ID card was quite simple, therefore it was highly susceptible to frauds. See Chodok Veeratham Poonsawat, "The Project," 25, 29.

CHAPTER 4

CONTEMPORARY STATE SURVEILLANCE SYSTEM IN THAILAND: A CASE STUDY OF THE POPULATION INFORMATION NETWORK
(1983 - present)

This chapter traces the historical context, development, and social implications of an important government surveillance system in Thailand from 1983 until the present. The Registration Administration Bureau's population information network (PIN) is selected as a case study.[1] This system features a massive database containing personal information that have been collected over the years from Thai citizens. While the database represents continuity with past surveillance efforts, it has recently undergone significant changes with the introduction of computerization and later ICTs in the collection, storage, processing and retrieval of the data. Not only has this surveillance system been given a new "face lift," but its capacity has also considerably expanded in various dimensions.

Similar to the preceding chapter, this chapter will begin first with a historiography of the period studied to contextualize the analysis that follows. This historical narrative, which also includes a brief section on the development of an "information society" in Thailand, will also be relevant as a background for the next chapter which deals with another case study on the Police Department's computerized criminal records system. The case study on the PIN will discuss the development and major characteristics of the project, with a focus on a number of areas in which the automation of record-keeping practices and systems may raise public-policy issues. These include: growth in surveillance capacities and institutional capacities to affect people's lives, access to public records, third-party inter-organizational transfers of information; data protection, and legal and organizational changes. This list is not intended to be exhaustive as it is unlikely for this case study alone to be able to address the broad range of issues and questions that the use of ICTs in surveillance systems raise.

The historical segment in this chapter will rely upon reviews of existing literature and archives as a method to establish the historical background of contemporary state surveillance and to explore informatization currents that shape it. As for the empirical assessment of the nature, characteristics, and functioning of contemporary forms of state surveillance, I have decided to use

---

[1] The Registration Administration Bureau is a division within the Department of Local Administration, the largest and most important department within the Ministry of Interior.

a case study as a methodology. (For a detailed discussion on the methodology used in this chapter, see Appendix 1) The Registration Administration Bureau is chosen for the case study because it fits the desirable profile -- a governmental organization that specializes in record-keeping and has the financial, managerial, and technical resources to apply computer technology to their record-keeping practices. According to a review by Privacy International, a London-based NGO specializing in privacy protection, and a conversation I had with a specialist from a major local system integration company, the PIN project is by far the most organizationally and technologically innovative in personal record-keeping in Thailand.[2] In addition, it also holds the largest number of important personal records on local citizens.[3]

THE CHANGING POLITICAL ECONOMY, THE RISE OF NEW SOCIAL CLASSES AND THE EMERGING "CIVIL SOCIETY" (1980- PRESENT)

In the broadest sketch, the past two decades saw the decline of the "bureaucratic polity" and the emergence of a "civil society," which was born out of the rapid economic growth since the 1970s and the ensuing social differentiation.

To recap, the economic reform introduced by Sarit in the 1960s laid a stable groundwork for laissez-faire economic policies and later export-oriented industrialization, which came to dominate for the subsequent three decades. The development of manufacturing exports in Thailand began in the late 1970s and early 1980s with textiles, shoes, and toys before moving to more complex products such as computer components, auto parts, and electrical goods in the late 1980s and early 1990s.[4] Table 4.1 shows the changing structure of exports from 1981 to 1996. Agri-business and other resource-based industries also grew, while the traditional farming sector shrank since so much of the labor force was drawn into the industries. The growth in exports

---

[2]The review by Privacy International was obtained from its website on the internet at http://www.privacy/org./pi. As for the computer specialist I talked with, he was an executive at Control Data Group (CDG) Corporation, a major computer system integration company. He asked that his name not be mentioned in the study.

[3]It should be noted that in the beginning I had set out to conduct site-visits to six different public organizations that have had a major computerization program in their record-keeping operations. This includes, in addition to the mentioned two organizations above, the Department of Revenue, the Social Insurance Office, the Department of Land Transportation, and the Bangkok Metropolitan Administration. But after having conducted a few site visits to these organizations, and having examined their record-keeping practices, I came to conclude that their operations were still too incomplete and inadequate, by themselves, to be classified as "surveillance" as earlier defined. Therefore, I decided not to include the data gathered from these site visits in this study.

[4]Although medium technology products now account for one-third of all exports, Thailand is mainly an assembly base for most of these products since design, hi-tech manufacturing processes, and marketing are located elsewhere.

and the influx of foreign investment culminated in an economic boom. Between 1986 and 1990, per capita GNP at constant prices increased by 44 per cent. The economy recorded double-digit growth from 1989 to 1990, but most of the growth was clustered in Bangkok. The economic boom started to flatten out in 1991-2 because of the Persian Gulf Crisis and internal political instability. However, the economy was still expanding until it came to a halt in mid-1997 as a result of a meltdown in the financial sector. In the midst of the economic and financial crisis, the Thai government requested in August 1997 financial support from the International Monetary Fund (IMF). The IMF agreed to extend a US$17 billion rescue package, which also included a prescription of stringent fiscal and financial policies. Thailand's economy has been in decline ever since. At the time of writing (late 1998), there are only slight signs of recovery as certain economic indicators have shown improvement, but the overall economy is still in the doldrums.

The economic expansion of the late 1980s and early 1990s gave rise to a significant change in the Thai social structure. Most evident is the emergence of the urban, non-bureaucratic, while-collar labor force. This increasingly prominent social group comprises small business owners, salaried employees of new and modern businesses, and independent (self-employed) professionals. They grew from a few thousand to several million over a period of one generation.[5] Aside from the white-collar workforce, the blue- collar workforce most of whom were migrant labor from the rural farming sector, also grew substantially on the back of the economic growth of the last three decades. The latter group, however, have a more subservient political role when compared to the former.[6]

Meanwhile, democratic elections, which have taken place consistently since the October 14, 1976 incident, helped enhance the political power of the modern business sector. In fact, the parliamentary system has provided a major avenue for businessmen, first the Bangkok group in the 1970s and then provincial groups from the 1980s onwards, to penetrate into the once autonomous "bureaucratic polity." Over the past two decades, the number and proportion of business-based politicians gradually rose as opposed to those with bureaucratic backgrounds. After 1988, provincial businessmen came to dominate the Cabinet and often

---

[5]This group is a subgroup within the middle classes. The middle classes are a more heterogeneous group which include civil servants and military officers as well.

[6]Since labor unions were banned by the military junta in 1991, collective organization of this social group has been obscure. As voters, they also do not pull their full weight. Since many, if not most, of the laborers are from the rural provinces, they usually have not changed their household registration from their villages. So if they vote at all, their votes will be dispensed across the rural provinces of Thailand rather than concentrated in the industrial belt of the country.

Table 4.1

Structure of Exports, 1981 - 1993 (billion baht)

Types of exports	1981	1985	1988	1990	1993
Agriculture[a]					
Rice	26.4	22.5	34.7	27.8	32.9
Tapioca	16.4	16.6	21.8	23.1	21.7
Total	73.0	73.4	104.5	100.0	110.7
Labor-intensive manufactures[a]					
Textiles and garments	14.7	26.6	64.1	92.3	129.6
Jewellery	5.2	8.7	23.7	34.9	41.0
Footwear	0.6	2.4	9.7	20.2	27.9
Total	22.6	41.5	118.7	185.1	257.2
Medium-high technology manufactures					
Machinery and appliances[b]	0.3	2.5	16.5	45.4	90.8
Electrical Appliances	0.6	1.4	6.3	32.5	62.6
Electrical Circuitry[c]	6.2	8.2	29.9	32.8	75.6
Vehicles and parts	0.1	0.3	3.8	5.5	16.5
Total	7.9	13.7	61.7	130.3	281.4
Total manufactures	54.7	95.6	265.6	440.4	752.6
Total exports	153.0	193.4	403.6	589.8	935.9
Manufacture as percentage of total exports	35.8	49.4	65.8	74.7	80.4

Sources: Thailand Development Research Institute (1994); Bank of Thailand; Pasuk and Baker (1995), 160.

---

[a] All other categories (other agriculture, other labor intensive, etc.) have been omitted.

[b] Mainly computer and parts

[c] Mainly integrated circuits

used their ministerial appointment as a vehicle to redistribute resources from Bangkok back to the provincial and rural provinces. It is important to note that development strategies since Sarit's period have had adverse distributional consequences. Not only did these policies reinforce the general centralization trend of the government, they also assigned urban industrialists a privileged status in policymaking. Thus, most of the growth has been centered in and around Bangkok and served the political interests of the Bangkok bureaucratic elites and industrialists.

In trying to reverse the distribution game, provincial business politicians found it crucial to first undertake a cabinet portfolio so that they could assume command over the bureaucratic machinery of government. After all, administrative power still remained concentrated at the center in the Bangkok-based government bureaucracy. It merits emphasis that an elected minister participates in nearly all aspects of policy-making at the national level. Elected representatives at the provincial and local level have no effective authority over provincial administration, and there are very few electoral channels at the provincial level for the average citizen to influence policy formulation. Although local elections became regular affairs in the provincial capitals, districts, and sub-districts, local representative assemblies and councils were not permitted any legal authority over the administrative apparatus of the government. The true source of power in allocating resources for rural constituents still remains in the central bureaucracy in Bangkok. And the persons who are in command in this establishment are the elected ministers, their deputies and the permanent-secretary of the ministries.[7]

In this light, parliament, as an institution, has little authority or interest to scrutinize the activities of the bureaucracy. The parliament serves largely as a vehicle of the Cabinet. Its formal powers are weak and it has chosen to limit its exercise of power mainly to legislative functions. Even so, the legislature does not control the laws and regulations that govern state interventions into the economy or society. Usually, the parliament passes legislation which sets broad mandates for implementing a given policy, but that legislation does not specify precisely what the bureaucracy is to do. Laws passed under Thailand's administrative legal code simply assign discretion to the various bureaucratic agencies and authorize them to issue subordinate legislation that civil servants deem to be necessary for achieving the broad objectives laid down by

---

[7]Because Thai party policies are vague or non-existent, politicians usually appeal to voters not with ideology or platforms, which suggest ways in which ministerial authority will be exercised, but simply with promises that the party will assist in forming a coalition government and win lucrative Cabinet assignments. By being a Cabinet minister, politicians can exert influence, for example, by reshuffling ministerial personnel, authorizing measures that benefit a target constituency, or directing ministry projects to their electoral districts. See Scott R. Christensen, "Democracy without Equity?: Institutions and Political Consequences of Bangkok-based Development," in Who Gets What and How?: Challenges for the Future Proceedings of the 1993 TDRI (Thailand Development Research Institute) Year-End Conference Held in Chon Buri, Thailand 10-11 December 1993, (Bangkok: TDRI, 1993), 18.

the law.[8] In other words, the parliament does not have authority over the implementation process, though this is the most crucial process.

Aside from exercising their influence on the government through parties and electoral politics, businessmen also organized themselves formally into lobbying associations to voice both their collective and particularistic interests on the direction of national economic policies.[9] According to Anek Laothamatas's very important study of Thailand, the role of these organized business associations is monumental as they have opened up a new model for understanding the contemporary Thai political economy.[10] With the strong emergence of liberal corporatism as evidenced in the powerful business associations, the political regime at work in the realm of economic affairs in Thailand is no longer a bureaucratic polity. While the bureaucratic force may remain strong, it has ceased to monopolize the decision-making and public policy formulation. Business groups have succeeded in affecting these policy-making processes in significant ways.

In the social realm, however, the role of business associations has been minimal. It was mainly the non-governmental organizations (NGOs) and a group of academics who played a crucial role in mobilizing against the top-down policy approach of the domineering bureaucratic state. Known in Thai as *sangkom pracha* or an equivalent of the western concept of "civil society," these movements were originally scattered and diverse in nature.[11] They developed in

[8]Surakiat Sathirathai, "Law and Regulations concerning Natural Resources, Financial Institutions and Export: their Effects on Economic and Social Development," research report, (Bangkok: Thailand Development Research Institute, Management of Social and Economic Development Project, 1987).

[9]Business groups have organized channels of instrumental influence on public policy at three levels. At the highest level are the big four groupings -- the Board of Trade, the Thailand Chamber of Commerce, the Federation of Thai Industries, and the Thai Bankers Association. These organizations were created in the 1950s and 1960s to facilitate formal consultation over collective business interests with senior government officials. By the early 1970s, representatives from these associations were already invited by the NESDB to participate in the formulation of national development strategies. These four flagship associations gained an even higher profile in national policymaking after the creation of the Joint Public-Private Consultative Committee (JPPCC) in 1981. One of the JPPCC's most important achievements was the promotion of an export-oriented industrialization strategy. At the sectoral level, trade associations representing specific industries increased from 48 in 1967 to 233 in 1987. These groups are used as vehicles both for collective industry representation and for the particular interests of individual firms and business families. Lastly, at the provincial level, the key associations are the network of Provincial Chambers of Commerce and the various provincial branches of the Federation of Thai Industries.

[10]Anek Laothamatas, *Business Associations and the New Political Economy of Thailand: from Bureaucratic Polity to Liberal Corporatism* (Oxford: Westview Press, 1992), 70, 161.

[11]The concept of "civil society" in western social thought and political theory incorporates a variety of meanings and interpretations. Here, I follow the notion given by Jean Cohen and Andrew Arato, who conceptualize "civil society" as the domain of uncoerced interaction and association within daily life. This domain of social interaction is situated between market and state (and organized political society). The existence of this social association is also capable of affecting official policy. See Jean L. Cohen, and Andrew Arato, *Civil Society and Political Theory* (Cambridge, Mass: MIT Press, 1992), 18. The application of this concept to the Thai context tends to focus on the very notion of creating independent forms of social activity and power from below, free from state supervision.

different realms including religion, popular culture, mass media, and development work. It was in the late 1980s that these movements began to coalesce into a loose but identifiable set of interlocking networks. The common core seems to lie in the shared democratic vision of enhanced autonomy and emancipatory practices against the pressures of capital and government bureaucracy. NGOs and a number of academics have played a central role in spearheading and coordinating these movements, which have emerged to defend a number of basic citizenship rights and to guarantee political pluralism in the decision-making of the state. A large number of members of these movements were participants in the student movements of 1973-1976.

The most famous achievement of the *sangkom pracha* movement thus far has been in the area of environmental protection. Because of their constant and earnest struggles in many battles against mega-projects with adverse environmental implications, NGOs have now been given a permanent seat in the country's National Environmental Board. They also succeeded in pushing for monumental environmental preservation legislation, which requires a public hearing and open dissemination of information to the public about any projects that may affect the environment.

Aside from environment protection, NGOs have also been prominent in democratization movements. This was manifested most clearly during the political crisis in May of 1992 when pro-democracy demonstrators rallied against a non-elected military premier who took power after a coup in the preceding year. An NGO called the Confederation for Democracy was an active force in organizing peaceful protests and in keeping the public abreast of new developments during the crisis after the military censure of all channels of media.[12] They also played an active role in campaigning for the recent political reform.

Like the NGOs, the press has in the past decade or so become a major platform for communication within the emerging "civil society" and a site of conflict between the state and the people. Up until the late 1980s, the print media was more prominent in this regard than the electronic media, which developed under close state control.[13] In the late 1980s and the beginning of the 1990s, however, television news also became more aggressive and specialized in controversial social and political stories. Television's political influence fluctuated, however,

---

[12]During the May 1992 crisis, there were 44 casualties, 1,000 injuries and 39 missing persons.
[13]Unlike the electronic media which are owned by the state, the printed press is privately owned and thus is not subject to the same control. Before 1996 when the first privately-owned television channel began airing, Thailand had five television channels, which were owned by the army and the Department of Public Relations. As for radio stations, the majority were owned by the army and the Department of Public Relations, while a smaller number of stations were owned by the Air Force, the Navy, the Police and other government agencies in that respective order. Boonlert Suphadiloke, *The Right to Communicate in Thailand (sitthi karn seusarn nai prathetthai)* (Bangkok: Thammasart University Press, 1984), 39.

depending on the openness of the ruling political regime. Since the technical infrastructure of television is owned by the state, it is commonplace to see television being censored or used as mouthpieces of the agencies that control them.[14] The structure of ownership and control of television began a significant shift in 1996 when a new ultra-high-frequency (UHF) television channel commenced broadcast. This channel is the first privately-owned television station in the forty six-year history of Thai television broadcasting. Calling itself "Independent Television" or ITV, the new channel specialized in news reporting and controversial documentaries and became recognized by its audience as a more reliable source of political information than the state-owned channels.

As far as the military is concerned, their political role from 1988 until the present has ebbed and flowed. Following the 1992 crackdown on pro-democracy demonstrators, the public developed a strong hostile sentiment against the military, which resulted in a sharp demilitarization in the country's politics. Nevertheless, the military's role has not entirely faded into oblivion. Ruling civilian governments still have to appease the armed forces with sizeable defense budgets while cutting back on other more important areas in order to ensure a good and cordial relationship with them.

While the businesses, the NGOs, and the press are emerging in political influence, the bureaucracy is entering a state of decline.[15] The lack of major structural change and adjustment over more than one hundred years since the 1892 Chakkri Reformation has made it incapable of coping with the transpiring social and economic changes. The central bureaucracy's top-down approach not only makes it increasingly unable to produce coherent and effective policies for a more complex society but also makes government agencies resistant to input and feedback by citizens' groups in the formulation of many sectoral policies. There are also the age-old problems of centralization of power and the inflexibly long chains of command, which led to sluggish procedures and even gridlock in supplying public services. Moreover, the Thai bureaucracy has been plagued by a stunning decline in the income of civil servants as opposed to the sharp

[14]Such is exactly the case with the famous *Mong Tang Mum* (Different Perspectives) program, which began in 1991 featuring a round-table discussion with audience participation on current social and political issues. The program attracted a lot of audience because it brought public opinion into the medium. The program was shelved in 1996 by the authority in charge (the Minister of the PM's Office who oversees the Public Relations Department) after one of the participants in the program made disparaging comments about the premier and his business dealing. This program was organized by an NGO, the Creative Media Foundation, and hosted by a university professor and a staunch social critic, Dr. Chirmsak Pinthong.

[15]Beginning in the period of Premier Chatichai in the late 1980s, senior bureaucrat appointees at state enterprises were removed and replaced by business allies or friendly bureaucrats. The NESDB was pushed to one side and its role in overseeing public sector projects was terminated. Today, the role of the NESDB has become even more obscure as the business politicians tend to be more unilateral in executing public policy.

upsurge in salary and benefits in the private sector.[16] See Table 4.2 for the comparative salary scale of government and private sectors. This has contributed significantly to the pervasive "braindrain" problem and the (alleged) persistence of corruption among the bureaucratic officials.

As industrialization proceeds, many of the base-line services and regulatory functions the state needs to perform may not be expressed in the form of demand by voters and interest groups. This may be due to sheer indifference as well as what is perceived to be unnecessary organizational costs by ruling elites. Their provision thus depends upon the wisdom, foresight, and leadership of politicians and civil servants. Many sectoral policy areas, in particular, are heavily knowledge-intensive and require administrative and technological sophistication. Unfortunately, with the bureaucracy ailing and the politicians preoccupied with reaping benefits from a ministerial appointment, these new requirements, which might not have been crucial a decade ago, are left unanswered. The Thai state, it is argued, has been particularly lax at the sectoral level and tends to respond in an ad-hoc fashion with piecemeal policies.[17] The presence of several appointed ad-hoc committees to oversee various sectoral

problems has replaced public hearings and proper feasibility studies to assess long-term impacts of certain public policies and projects. While not anticipating long-term policy needs, the increasingly interest group-centered Thai state also responds primarily to the immediate patronage demand of those enterprising groups who can gain temporary access to the offices and policy instruments of the state.[18]

---

[16]In an economy where the average per capita real income has been increasing at about 4 per cent per annum in the postwar era, the income for the highest official (rank of permanent secretary of a ministry) in 1990 were worth about 15 per cent of their real value for the year 1909. See Pratya Vesaraj, *Bureaucratic Reform for the Future: Strategies for Development* : Proceeding of the annual seminar 1996 on Bureaucratic Reform for the Future of Thailand (Bangkok: Thailand Development Research Institute, 1996), 10.

[17]Scott R. Christensen and Ammar Siamwalla, "Muddling toward a miracle: Thailand and East Asian growth," *TDRI Quarterly Review* 12 (April 1994): 19.

[18]Christensen, "Democracy," 2, 20.

Table 4.2

Comparative salary scale of government and private sectors (monthly, in baht)

Level of education	Private	Government	Private more than Govt (%)
Secondary Education	4.725	4,100	15
Polytechnic certificate	5,778	4,700	23
Higher Polytechnic certificate	6,912	5,740	20
Bachelor's degree (Social Sciences)	9,617	6,360	51
Bachelor's degree (Accountancy)	10,587	6,360	66
Bachelor's degree (Engineering)	14,175	6,360	123
Master's degree	17,366	7,780	123

Source: Pratya Vesaraj, *Bureaucratic Reform for the Future: Strategies for Development* : Proceeding of the annual seminar 1996 on Bureaucratic Reform for the Future of Thailand (Bangkok: Thailand Development Research Institute, 1996), 8.

Prior to the economic downfall in 1997, which has since overshadowed all other issues, two contentious topics captured the national interest in Thailand -- political reform and bureaucratic reform. The former, which appeared as a far-fetched proposal by a group of democratic advocates only a couple of years ago, materialized in 1997 when a new constitution was enacted, setting the ground rules for new political procedures and practices. One of the new constitution's central objectives is to clean up the notoriously corrupt electoral process by making it more difficult for dirty politicians to maneuver illicit tactics or to even run for office in the first place. Unlike the other constitutional changes in the past, the new charter had a great amount of public participation in the drafting process to ensure that it is the people's own version.[19]

The issue of bureaucratic reform has been widely debated within academic and public policy circles. The problem was framed in terms of the need to improve the state bureaucracy's administrative and management efficiency to cope with changing conditions brought about by globalization and internal societal adjustment. These changes, it is argued, have created higher expectations of government services from the public and from the private sector, ones that the cumbersome, outdated, and inefficient bureaucracy has not been able to deliver.

Among the major targets of criticism in the government bureaucracy is the powerful Ministry of Interior. Over the years, it has grown to be an enormous empire with the largest number of departments -- fourteen departments and seven state-owned enterprises -- the largest number of officials, and a wide range of activities including provincial administration, involvement in local government, police, public prosecution and more. This Ministry's scope of responsibility, it should be noted, involves the most encounters with citizens through various public services including, among others, civil registration services. For the past ten years, the Ministry of Interior has been ranked among the top three ministries in terms of budget allocation.

---

[19]The proposal for the political reform was inspired by the recognition among a group of academics, activists, and some politicians that the current parliamentary democracy was not suitable for Thailand. Due to the large gap between the urban and the rural areas and the pervasive patron-client relationship in the local political culture, vote buying and vote soliciting have been rampant. As a result, politicians who are elected through such questionable means are inclined to be corrupt because of the need to recoup their investment during the campaigning. Therefore, the new charter is aimed mainly at filtering out potential electoral candidates with unacceptable background and at ensuring a fair and clean election process. The Constitution Drafting Assembly was set up to draft the new charter. The Assembly consisted of 99 members who were carefully selected through several screening processes and indirect elections nationwide. After the drafting was completed, the new charter was open to tremendous public participation including a nationwide public hearing process in which civic groups from each province registered to debate a wide range of charter-related ideas.

In 1996 and 1997, the Ministry received the highest budget allocation totalling Bt106.87 billion, and Bt152.64 billion respectively. Much of this allocated budget went to support the acceleration of the provision of information and communication infrastructure of the Ministry's administrative offices in Bangkok and its vicinity and in the provincial areas.

As the following case study unfolds, it will become increasingly clear that part of the expenditure designated above must have gone into the implementation of the Department of Local Administration's Population Information Network (PIN) project. Being the largest and possibly most powerful department in the Ministry of Interior, this department controls the crucial Registration Administration Bureau, which is in charge of collecting and keeping information on all citizens nationwide for administrative purposes. The extent of its surveillance of the population is most clearly evident in the widely used household registration documents and national identity cards, both of which have become almost impossible to live without in Thai society. Since 1983, the Registration Administration Bureau has been computerizing its massive databanks, which contain personal data from household registration documents and national identity cards. This computerization project, which is technically known as the Population Information Network (PIN), has grown by leaps and bounds since its inception. On several occasions, the efficiency achieved from the application of computers and later ICTs to civil registration tasks has been praised by many observers. For instance, a high-profile report which came out of a conference on the re-engineering of the government bureaucracy in Thailand cites the Department of Local Administration as an exemplary case in using ICTs to improve the efficiency of public services and organizational management.[20] In fact, ICTs are listed as one of the central issues that have to be addressed in the anticipated reform of the Thai bureaucracy.[21] The pervading technocratic obsession with efficiency has indeed obscured plausible adverse impacts of ICTs to the point of invisibility.

---

[20] Pratya Vesaraj. *Bureaucratic Reform for the Future: Strategies for Development* : Proceeding of the Thailand Development Research Institute (TDRI)'s annual seminar 1996 on Bureaucratic Reform for the Future of Thailand (Bangkok: Thailand Development Research Institute, 1996), 35.
[21] Ibid.. 10.

THE DEVELOPMENT OF
AN "INFORMATION SOCIETY" IN THAILAND

The dramatic economic expansion of the late 1980s and early 1990s aroused many hopes and dreams in Thailand. At first, aspirations focused on becoming a newly-industrialized country (NIC), or more precisely, throwing off the unflattering stigma of "developing country" status. Eventually, as talks about the post-industrial society" and "globalization" took center stage, another equally if not more important aspiration emerged, that is, development of an "information society." As in the rest of the world, Thai elites sought to jump on to "knowledge society/information economy" bandwagon. Inspired in part by catchy notions like "The Third Wave" and "Megatrends," which were popularized by the local media and computer and telecommunications industries, these elites were persuaded that information and ICTs are *the* major factors of production and wealth creation in the 21st century.[22] Riding on the same current, the local policy community also became caught up in this same euphoric campaign.

In 1992, the government established the National Information Technology Committee (NITC) to oversee the policy aspect of ICT development and deployment in Thailand.[23] The NITC comprises 22 members from public and private agencies, and it is chaired by the Deputy Prime Minister in charge of social and economic development. At present, it has 18 sub-committees overlooking ICT development in various areas, including three that directly affect electronic commerce development, the Electronic Data Interchange (EDI) subcommittee, six ICT-law subcommittees, and the Electronic Commerce Task Force. To complement the NITC, the government in the same year also set up the National Electronics and Computer Technology Center (NECTEC) to carry out research and development (R&D) in electronics and computer-related areas.[24] NECTEC operates fifteen laboratories specializing in various technologies such as microelectronics, telecommunications, networking, software, and computational linguistics. It was also assigned the role of NITC secretariat.[25]

---

[22]John Naisbitt, author of *Megatrends,* came to Bangkok in 1995 as a guest of the Association of Thai Computer Traders. He spoke at a downtown hotel to a high-profile audience about the future envisioned in his book. In the audience were business elites, government bureaucrats, academics, and journalists.

[23]It should be noted that in Thailand ICTs are referred to as IT (information technology). To be consistent with the rest of the study, this section will use mainly ICTs but may occasionally use IT to observe the original usage in some contexts.

[24]NECTEC is a statutory agency under the Ministry of Science, Technology and Environment.

[25]It merits emphasis that the development in the ICTs policy sector has been entirely separate from that in the telecommunications sector. Telecommunication regulation is under the care of three public entities within the Ministry of Transport and Telecommunications -- the Post and Telegraph Department, the Communications Authority of Thailand (CAT), and the Telephone Organization of Thailand (TOT). Since current Thai law does not allow private provision of telecommunications services, all telecommunications activities are under the

To date, the NITC and NECTEC have been involved in many ICT development activities, including R&D, human resources development, public awareness programs, legal infrastructure, software industry promotion, electronic commerce, development of technical guidelines and standards, and diffusion of ICTs in the public sector. In 1992, NECTEC initiated the Thai Social, Scientific, Academic, and Research Network (Thaisarn), the first non-profit information infrastructure for academic and research communities in Thailand using the internet as a backbone network technology. In 1995, the NITC organized Thailand IT Year campaign during which activities were organized to stimulate public interest in ICTs and to promote further diffusion of the technology. One of the by-products of the IT Year campaign was a school informatization program called the SchoolNet project. Using the existing Thaisarn infrastructure, the project features a joint effort between NECTEC and the Ministry of Education to connect local schools to the internet, in order to raise the quality of secondary education. In 1996, at least 50 secondary schools (19 in Bangkok and 31 in other provinces) were reportedly connected to the SchoolNet.[26] In 1998, another phase of the SchoolNet was open, allowing 1,500 secondary schools nationwide to access the network.[27]

Alongside, the government has also done its part in promoting ICT diffusion by passing several measures to stimulate computer utilization. Efforts include a 1991 reduction of import tariffs on computer hardware (finished products) from thirty-five to forty per cent down to five per cent, a similar reduction for computer software from twenty per cent to five per cent in 1994, an adoption of minimum requirements for IT in the public sector, as well as mandatory computer

monopoly of these organizations. The situation changed in the 1980s as rapid economic expansion drove up demand for telecommunications services to the extent that the public monopoly could not cope with. A new collaborative scheme called Build-Transfer-Operate (BTO) was thus devised, enabling state enterprises like TOT and CAT to contract out certain large-scale services that require capital-intensive investment and sophisiticated technological knowhow. Among the projects contracted out to private companies under the BTO scheme were: a three-million fiber-optic telephone line installation project, a domestic satellite project, and two mobile cellular phone projects. There were also signs of regulatory changes as two masterplans for telecommunications development were formulated and approved by the cabinet between 1995 and 1997. The main policy elements of the plan included aspects such as liberalization, increasing private participation, establishment of an independent regulatory body, and R&D industrial development. See Sethaporn Cusripituck, "The Liberalization of the Thai Telecom Sector," a paper presented at the Canada-Thailand Executive Information and Communication Technology workshop, 23-24 November 1998, Bangkok, Thailand. Mr. Cusripituck is presently director-general of the Post and Telegraph Department.

26Paisal Kiattananan, Pichet Durongkaveroj, Thaweesak Koanantakool, and Adshiriya Agsorn-intara, "National Information Infrastructure in Thailand," a paper presented at the International Forum for APII Test-bed, Seoul, South Korea, June 18-20 1996, 2-3.

27Thaweesak Koanantakool, The Internet in Thailand: Our Milestones. http://www.nectec.or.th/users/htk/milestones.html. Dr. Koanantakool is the current director of NECTEC.

literacy for civil servants.[28] Computer and other office automation equipment are now used widely in all government offices and private sectors across the country. Accordingly, the budget allocation for ICT projects in government organizations and state enterprises has grown significantly over the years from a mere Bt260 million to an estimate of more than Bt5 billion in 1999.[29]

In 1995, the NITC published a report entitled "Towards social equity and prosperity: Thailand Information Technology (IT) policy into the 21st century." The many pages of this ambitious report read like a flashback to the visions of Daniel Bell's "post-industrial society" or Yoneji Masuda's "computopia," which dominated the mainstream discourse of the "information society" thesis earlier. In the Thai report, ICTs (referred to as IT in the report) are seen as pervasive and enabling technologies that will offer not only new economic possibilities but also opportunities to equalize and better social conditions for the citizenry. Insofar as the government policy was concerned, ICTs were said to hold extreme potential, to wit:

> IT can play a pivotal role to support many of the government's policies for better distribution of wealth and opportunity to rural inhabitants; for equal opportunity to personal and corporate development, healthcare, and other public services; for solving the chronic traffic gridlock and worsening pollution; for conservation of the nation's natural resources and environment; in addition to that of making the country a regional hub for finance, manufacturing and trade, transportation and tourism.[30]

While maintaining a positive outlook on ICTs and on the harnessing of information throughout, the report does acknowledge possibilities of ill effects that may arise such as information disparity between the rich and the poor, violation of personal privacy, abuses of intellectual property rights, and cultural encroachment. But these are generally mentioned only in passing and accorded very little significance. The main emphasis of the report is on the urgency to develop an "information society" in Thailand, which is treated as an inevitable course of action for the state and the entire society. This is explained in the following terms:

> The transformation into a fully-grown Information Society will be an arduous journey. We must start on that journey sooner or later. The journey will be

[28]According to this mandatory measure, all government officials above the C-5 level have to pass a knowledge test on computer applications in order to be qualified for a promotion above that level. See Paisal Kiattananan et al. "National Information." 1.

[29]Jirapan Boonnoon, "Slight growth predicted for IT market in Thailand this year." *The Nation*, 2 March 1999, F 2.

[30]National Information Technology Committee Secretariat, *Towards social equity and prosperity: Thailand Information Technology (IT) policy into the 21st century* (Bangkok: National Electronics and Computer Technologies Center, 1995), 1.

smoother in reaching its intended destination if the whole society take active part. For that, the state has the mandate to show the way forward.[31]

Soon after, the main ideas in the above NITC report were recycled, with little modification, into a national ICT policy masterplan entitled "IT 2000: a National Policy on Information Technology." This policy masterplan rests on three pillars of ICT development -- investment in information infrastructure, investment and improvement of human resource in ICTs, and model diffusion of ICTs in the public sector through government computerization programs. The last agenda entrusts the state to become the prime moving force for the envisioned metamorphosis. Not only is the state charged with the planning, promotion, and coordination of all concerned sectors --- education, research, infrastructure, industry. and human resources -- in fostering the ICT-oriented change. but it is also expected to provide a role model to the rest of society in terms of IT diffusion as well as to remove obstacles that may stand in the way of realizing the central aspiration.

To enable the state to assume such role, the NITC provided the following recommendations: 1) a series of measures to equip government agencies with sufficient office automation and ICTs; 2) a study entitled "IT for Good Governance Handbook," to assess how ICTs should be applied to improve effectiveness and efficiency in administration and service delivery in the public sector; and 3) computerization projects in many departments and ministries. Besides the PIN project, other major government computerization programs include the Revenue Department's tax computerization program, a geographical information system of the Ministry of Agriculture, Ministry of Science, Technology and Environment, and the Bangkok Metropolitan Administration (BMA), and the Ministry of Labor and Welfare's social insurance database system.

The above computerization projects form a preliminary step towards the much envisioned Government Information Network (GiNet) project, which is the equivalent of a government information superhighway. The planned project, with an estimated investment of Bt2 billion. will provide a high-speed network for government services through provision of channels for delivering government electronic information within geographically dispersed ministries and for inter-ministry communications.[32] Such services, as a NECTEC publication argues, "would not only help each agency which generally lacks IT manpower to service the agency's networking

---

[31]Ibid., 9.
[32]According to the plan, the GiNet project will be running on high-speed optical fiber backbone capable of data transmission at 620 megabits per seconds across the country. See Thaweesak Koanantakool, *IT Projects into the Future*. http://wwwusa.nectec.or.th/it-projects/index.html.

needs. but will also enhance the utilization of each and every network to its fullest by sharing this common information pipeline."[33] Since approval by the cabinet in May 1997, the project has received strong support by politicians and bureaucrats. The ruling government in 1997 sees GiNet as "an important key towards government reengineering since agencies could be empowered to reform themselves towards the slimmer but smarter government."[34] The prime minister at the time, Gen. Chavalit Yongchaiyudh, once said on public television that he would stop building roads for a day or two to funnel the money for making this important network.[35] Be that as it may, the project was delayed from its original plan to begin implementation in 1998 by the economic slump which broke out in mid-1997. More recently (April 1999), however, the Department of Local Administration, which has been assigned the responsibility for network installation of the GiNet project, proposed that its network, which is the biggest information infrastructure amongst all ministries, be used as an alternative so that GiNet could achieve faster implementation.[36] No decision has been made by the cabinet at this stage.

In addition to intensive diffusion of ICTs in the public sector, NITC and NECTEC have also played a viable role in facilitating the emergence of electronic commerce in Thailand. This is in keeping with the general trend in Asia where electronic commerce is seen by the regional business circle as a competitive necessity for the region's economic revival.[37] The two organizations' role in electronic commerce development is manifest in three areas: policy framework, legal aspects, and technical guidelines and standards. The development of the framework brings together public and private sector representatives to jointly assemble policies suggesting the roles and responsibilities of government agencies while facilitating private sector involvement in electronic commerce. In parallel, six ICT laws are being drafted including a data protection law, computer crime law, electronic data interchange law, digital signature law, electronic funds transfer law, and universal access law. The six laws, as a NECTEC report puts it, "will serve as an infrastructure for doing electronic commerce and enhance confidence among members of the electronic transaction playground while providing rules and etiquette for fair

---

[33]Paisal et al. "Information Infrastructure." 3.
[34]Thaweesak Koanantakool. "IT Projects." 7.
[35]Ibid.
[36]Suchalee Pongprasert, "Alternative proposed to implement GiNet project," *The Nation* , 20 April 1999. F 4.
[37]According to a major new survey of CEOs in Asia, conducted by Price Waterhouse Coopers and the World Economic Forum, nearly 73 per cent of the CEOs surveyed believe that electronic commerce will either "completely reshape" or have a "significant impact" on competition in their industries. A fifth of the CEOs surveyed also see more than twenty per cent of their total revenues coming from electronic business in the next five years. Nearly 300 CEOs from major companies in nine Asian countries including Thailand took part in this survey. *The Nation* (Bangkok). 20 October 1998.

play."[38] In the last dimension -- technical guidelines and standards, NECTEC has called for voluntary participation of government agencies, the private sector, educational institutes, and independent research centers to draft IT technical recommendations and standards. Among the standards to be set up are those for smart cards and Public Key Infrastructure (PKI). In 1998, NECTEC formed a group of volunteers called the Thailand Smartcard Working Group to develop recommendations for these standards. The recommendations are expected to stimulate widespread use of smart cards and PKI technology, which are said to be key in building trust among international electronic commerce participants.[39] A more detailed discussion on the development of smart cards will be dealt with later in the chapter.

THE POPULATION INFORMATION NETWORK (PIN)

The PIN (Population Information Network) project was initiated in 1976 by the Department of Local Administration of the Ministry of the Interior in initial collaboration with the National Statistics Office. The project was approved by the Cabinet in 1982 and began operation in 1983. The first phase of the project or PIN I (1983-1988) primarily involved the issuing of personal identification numbers and the creation of a central population database (CPD), which hosts basic personal information on all citizens within one single computerized databank. These two activities were deemed essential in the face of rising population, cross-border illegal immigration, and the mounting problems in civil registration work during that period.[40] The second phase of the project or PIN II (1996-2001), which was partly inspired by the inefficient centralization of PIN I, features two efforts: to establish on-line linkage of the CPD with all civil registration offices nationwide and to issue new personal identity cards with magnetic stripes.

PIN I: ISSUANCE OF PERSONAL IDENTIFICATION NUMBERS
AND THE CENTRAL POPULATION DATABASE (CPD)

At the inception of the PIN I project in 1983, Thailand had a population of forty-eight million, which was continuing to grow by 1.3 million annually. The country was also facing a

[38]Thaweesak Koananthakool, "The Roles of the National Electronics and Computer Technology Center and the National Information Technology Committee on Electronic Commerce Development in Thailand." (Bangkok: Ministry of Science, Technology, and Environment, 1998), 1.

[39]Ibid., 2.

[40]Chodok Veeratham Poonsawat, "The Project to Issue Citizen Identification Numbers: National Security and the Right of the Citizen," (*Khrongkarn chattham lekprachamtua prachachon kab khwammankhong khong chart lae sitthi khong prachachon*), (Special degree thesis, National College of Defense, 1983), 39.

large influx of illegal immigrants from the neighboring war-torn countries in Indochina. This influx had led to widespread fraud and abuses in birth certificates and household registration documents. Meanwhile, the civil registration system, which had been revised in 1956 was ripe for another major overhauling for several reasons. First, while the hierarchical setup of the civil registration system, as discussed in chapter three, might appear centralized, the fact that there were 846 district and sub-district civil registration offices scattered nationwide made the envisioned centralized control impossible. This spatial limitation was intensified by a second problem -- technical obsolescence. At the time, all district offices maintained their household registration and citizen identification information in paper files and relied on typewriting and handwriting for record-keeping. This manual system was not only inefficient in retrieving records but was also highly prone to fraud. Communication between district offices was infrequent as telephones were scarcely in use, and few officials would bother to verify evidence of relocation or other changes with another district registration office because of the slow postal system.[41] Thirdly, the national identity card, which was born in 1963, turned out to be inadequate as a means of bureaucratic surveillance. The laminated photo was, as aforementioned, of such poor quality that most of the time it could not be used as a reliable identification. What the ID card really needed, according to a study completed by a Ministry of Interior 's administrator, was a built-in mechanism, such as fingerprints, that would help to quickly and effectively verify a person.[42]

In addition, as civil registration work grew quantitatively and became qualitatively more complicated, the existing number of registration personnel were insufficient and, in many ways deficient, to cope with the task at hand. Many district registration offices reportedly had a three-to five-year backlog in entering new civil registration information into their files. Because of poor transportation and communication, some lower-level registration offices also failed to submit their registration reports to the registration office at the next hierarchical level in time for a national update. All these factors combined resulted in out-of-date and inaccurate information, which, by any standard, would not be very useful as statistics for national planning, let alone, as means for bureaucratic surveillance.

---

[41]Since all a person had to do to get a national ID was to show that he or she had a name listed on a household registration card, many illegal immigrants found several illicit ways to get a card. Among the methods they used were: 1) faking a move-out application from one district office and registering a move-in at another district office where they obtained a new household registration document; 2) falsely adding a name to a real move-in application form following other names that were actually moving in; and 3) faking the entire household registration card. Considering that the forms used for moving, household registration and other civil registration work had remained unchanged since 1956, the falsifying of documents was rampant. See Chodok. "The Project." 76

[42]Ibid.

In response to the above problems, the PIN I project which featured an estimated budget of Bt2 billion (US$80 million) was introduced with the following objectives:

1) to be a measure to verify citizens and to more thoroughly control the population;
2) to set up a uniform system for issuing personal identification numbers for all citizens nationwide;
3) to set up a centralized database to store civil registration records of all citizens at the Bangkok-based Registration Administration Bureau, which will be readily expanded for storages of other forms of personal documentation in the future;
4) to increase the efficiency, extent, speed, and accuracy of civil registration work as well as to better prevent fraud and abuses;
5) to process population information with computers and to use the computerized information for public policy and planning, national defense, and national development.[43]

Not only was the Department of Local Administration clear and sincere in its motives to control, centralize, unify, and boost efficiency of the means of social control by using computers, it was also just as open in its intent to share this new resource of information with other government agencies and the private sector. The deputy director-general of the Local Administration at the time describes this as part of the project's rationale.

.....The central population database will be widely open for other government agencies and private enterprises that wish to make use of this central database for inquiry on personal history of the citizens. This will help save the government's budget and will eliminate the unnecessary duplicate collection of citizens' information.[44]

According to this senior official, the exploitation of the CPD could be in the form of file sharing, linking, or copying of files. It is also possible to make requests for collection of other additional fields of information.[45]

PIN I involved two important activities: the issuing of a 13-digit identification number to all citizens and the creation of a central population database (CPD). As far as the former was concerned, the Thai bureaucrats who proposed the PIN were inspired mainly by the systems at work in Scandinavian countries -- Denmark, Norway and Sweden. In Sweden, for instance, a

---

[43]Department of Local Administration, Ministry of the Interior. A Manual for the Operation of the Project to Issue Identification Numbers to Citizens, 2526 B.E. (khu meu patibat ngarn tamkrongkarn chat tham lekprachamtua prachachon pi 2526) (Bangkok: Agriculture Cooperatives Union of Thailand Press, 1983), 21
[44]Chodok, "The Project", 2.
[45]Ibid., 80.

system of national identification numbers was introduced as early as 1947. All Swedies are identified by unique ten-digit Personal Identification Numbers (PINs), which include full information on name, date of birth, address, gender, income, education and more. The numbers are routinely available and widely used as the standard identifier for individuals in all public and private information systems.[46] While the Thai bureaucrats adopted the technical idea from the Scandinavian bureaucracy, they were careful not to borrow the socialist idea of a cooperative commonwealth underlying the Swedish surveillance system. Scandinavian nations are welfare states and in order for the governments to render welfare for their respective citizens, they have to be able to identify each and every subject to determine eligibility and to minimize welfare fraud. In the context of Thailand in the 1980s, however, social welfare was not yet a priority on the Thai public policy agenda.[47] The Thai Ministry of Interior introduced these identification numbers primarily for social control not welfare purposes, although it foresaw the use of the numbers for other purposes, including social insurance in the future.

While Scandinavian countries use ten and eleven digits for their personal identification numbers, Thailand opted for a thirteen-digit numbering system because of the much larger population that had to be covered. Nevertheless, the basic principle of these identification systems is the same, as the number in each digit signifies different attributes about a particular citizen. The Thai personal identification numbers could be decoded as below.

| 5 | | 1 | 0 | 0 | 9 | | 9 | 9 | 0 | 2 | 4 | | 1 | 5 | | 9 |

The first digit signifies the type of a person's nationality status (citizen versus non-citizen) and the period in which the person was issued the identification numbers. For instance, 1 suggests that the person is of Thai nationality and receives the identification number at birth by having it assigned to the birth certificate while 3 indicates that the person is of Thai nationality, was born before 1983 (when the issuance of identification numbers began) and properly had their

---

[46]In Sweden, the 10-digit PINs are used to identify citizens for their eligibility and obligations in the following areas -- military service, civil defense, social insurance, education, public health service, passports, vehicle registration and driver's license, general insurance, banking, and employment. Karl - Johan Nilsson, "System of Identity Numbers in the Swedish Population Register. *Technical Paper*, No. 3, Sept. 1979., 3-4, as quoted in Chodok, "The Project," 155.

[47]Thailand's first social insurance law was not passed until 1991. At present in 1997, the system is still in its early stage of implementation and is limited to only a limited portion of the population.

names listed in a household registry during the time when the personal identification numbers were being issued.[48] There are altogether seven categories to describe this attribute.

The second to the fifth digit indicate the codes of civil registration offices in the provinces. district, and municipality where the person was issued identification numbers. The sixth to the twelfth digit indicate the ranking of that person in the registration roll of each particular registration office. The thirteenth digit is the check digit which is computer generated to ensure the accuracy of the preceding 12 digits.

In 1983, when these 13-digit numbers were first issued, the Ministry of Interior foresaw the use of these identification numbers as a universal system for various agencies and activities. The following were listed as potential users who would benefit from this ID system:

1) the Department of Local Administration's civil registration system;

2) the Department of Local Administration's national identity card system;

3) the Department of Revenue's revenue collection system;

4) the Ministry of the Interior's insurance system;

5) the government's social welfare system;

6) the Police Department's criminal suppression department;

7) the Ministry of Defense's conscription and administrative system;

8) the Ministry of Education and the Ministry of University Affairs' education system;

9) the Ministry of Public Health's health care system;

10) the Land Transport Department and the Police Department's motor vehicle and driver's license registration systems;

11) the Land Department's land registry system;

12) the Labor Department's labor system;

13) the Department of Public Waterworks' billing system;

14) the Electricity Generating Authority of Thailand's billing system;

15) the Telephone Organization of Thailand's billing system;

16) the National Statistics Office's population census system;

17) private banks and other financial institutions;

18) administrative divisions in both the public and private sectors.[49]

---

[48]The issuing of the 13-digit identification numbers began first in 1983 to those who had their names listed in the household registration documents. In the following year, the Local Administration Department started issuing these numbers to every newborn child by assigning the numbers to each child's birth certificate.
[49]Chodok, "The Project", 157.

Under the issuance of the identification numbers scheme, all persons residing in Thailand were entitled to personal identification numbers. They could be classified into two broad groups. The first group consisted of the permanent residents who were of Thai nationality and those resident aliens who lawfully held resident aliens documents. The second group was comprised of those illegal immigrants who did not have resident aliens documents. The identification numbers for both groups were computer generated by the Registration Administration Bureau. Aside from the issuance of personal identification numbers to all residents, every household was also assigned a new computer-generated household registration number. Two parallel processes -- 1) the entering of new identification numbers for citizens and households into the existing household registration documents and 2) the revision and correction of information held by civil registration offices nationwide -- took place between 1983 and 1984. Trained officials from the central government were dispatched to the provinces to help improve the quality of civil registration information in paper files to the standard acceptable for computer data entry in the next process.

Following the issuance of the personal identification numbers, the creation of the central population database (CPD) began in 1985. The most crucial thing about the CPD was its highly centralized and hierarchical design. In technical terms, this type of design would be commonly known as the databank approach.[50] The early proponents of government databanks, who definitely inspired the advocates of Thailand's CPD, think that much of the data collected in day-to-day operations could be shared on a government-wide basis, thereby reducing duplicate collection and storage of data while increasing the multiple use of data.[51] Although there have been a number of databank projects in the US, none were of the government-wide scope of the CPD. Government-wide databank projects did not materialize in the US mainly because they required data be collected by one department to be used by other departments or top management without specific use for the collecting department. In addition to the prohibitive costs of gathering and storing massive amounts of data that were not destined for a specific use, the public sentiment against intrusion of privacy was another important factor that prevented the creation of such a databank in the US. This is evidenced in the widespread American public anxiety over the proposal in the late 1960s to establish a National Data Center for statistical

---

[50]A databank is a centralized storehouse of data that can be applied to multiple information needs. The primary emphasis of this approach is on data organization which is highly hierarchical in structure. See Kenneth L Kraemer and John Leslie King, *Computers and Local Government, vol. 1, A Manager's Guide* (New York: Praeger Publishers, 1977), 14

[51]Ibid.

research. Because of the public concern and resentment, the proposal was finally dropped.[52]

The situation was clearly different in Thailand in the 1980s with the absence of visible privacy concerns or awareness by the public. Besides, the creation of the CPD was, like most Thai public policies, imposed by a powerful government bureaucracy in a top-down fashion on an uninformed and unquestioning populace. Whether or not the general Thai public would have perceived it to be in the public interest and not threatening their own interests is not known as a public hearing was never conducted. Assessing public opinion was still unheard of during the semi-democratic climate of the 1980's. In any case, the creation of the CPD took off without a hitch, and by 1988 it became one of Asia's largest databases of personal information.

From 1985 until 1988, the CPD was constructed by entering data from paper household registries and personal citizen records from 846 civil registration offices nationwide into the mainframe computer at the registration processing center of the Registration Administration Bureau in Bangkok. As the amount of data to be entered was immense -- covering some 50 million citizen records and some 10 million household records, 600 data entry staff worked in two shifts, day and night, to enter a daily average of 60,000 personal and household records. Before the data from each source document was entered into the computer, it was microfilmed to create an additional backup that would then be stored in the Bureau's microfilm library. Then, the data was entered into the mainframe through one of the 300 computer terminals at the Registration Administration Bureau. The entered data was temporarily stored in a 5 MB - 30 MB hard drive (capable of storing between five million to 30 million characters) before being transferred into magnetic tape as a final storage device. At present, the CPD's capacity has been significantly upgraded. During the site visit in August of 1996, the mainframe which stored all civil registration and national identity card information, had a capacity of storing 80,000 megabits of information.

In 1988 after data entry into the CPD was nearly completed, the Registration Administration Bureau began issuing new personal identity cards to citizens in many provinces. The procedure of card issuance was highly centralized as all cards had to be issued from the Registration Administration Bureau in Bangkok. This was done in order to prevent fraud which was rampant particularly in the outlying border provinces. The usual process of card issuance began with district and sub-district registration offices taking photos and thumbprints of the

---

[52]See Simon G. Davies, "Re-engineering the Right to Privacy: How Privacy Has been Transformed from a Right to a Commodity," in *Technology and Privacy: the New Landscape*, eds. Philip E. Agre and Mark Rotenberg (Cambridge, Mass: MIT Press, 1998), 145.

citizens applying for the card and sending the negatives together with corresponding card applications to Bangkok. Then, staff at the personal identity card section in Bangkok would develop the films, attach the developed photos to the application form, and make microfilms out of the completed applications before sending them to the adjacent registration processing center for data verification. If the data in the application matched with the one in the CPD, a new card would be issued. If not, it would be sent back to the original registration office.

The new card clearly differed from the 1962 card in utilizing computerized prints, color photos, and security-sealed lamination. The material used, however, was still paper-based. The layout of the 1988 personal identity card with corresponding translation are shown in Figure 4.1 and Figure 4.2.

Along with the new personal identity card, a new and computerized household registration document was also issued to all households nationwide. As far as the format was concerned, this new computerized version did not appear very different from the one before. The main difference was the computer characters instead of handwritten or typewritten characters. An example of the new version of the household registration document is provided in Figure 4.3.

What is in the CPD?

By 1988, data entry was completed for most of the provinces and the CPD then contained six major registration files, which were interrelated through a database management system (DMBS).[53] They are:

    1) Household registration file;

    2) Personal identity card file;

    3) Name and history file;[54]

    4) Marriage and divorce file;

    5) Guns and weapon file; and

    6) Voters' list file.

---

[53]A DBMS is a type of application software that has been developed to work with data stored in database files. DBMS allows users to construct a database environment for a set of related files and to quickly and easily access and manipulate the information located in several separate files.

[54]This file contains records about citizens' moving history and about citizens who have changed their names.

Figure 4.1a: 1988 National Identity Card (front) The card is 6 centimeters in width and 10 centimeters in length.
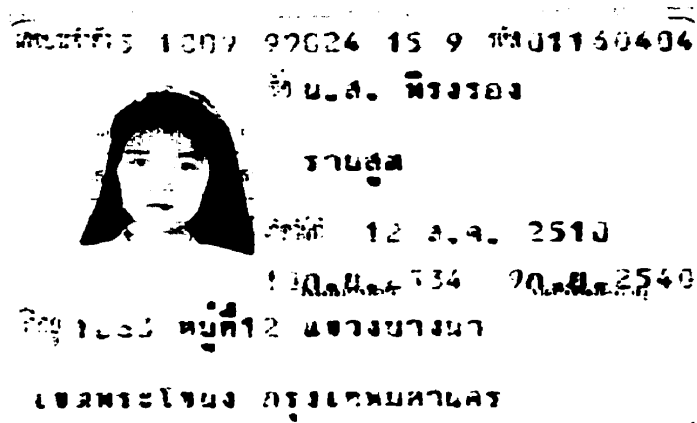
Figure 4.1b: 1988 National Identity Card (back)

Figure 4.2: Translation of the 1988 personal identification card (front)

Figure 4.2 Translation of the 1988 personal identification card (back)

129

Figure 4.3: 1988 Household registration card
Household Registration Number:
1000009108854
House No.: 1063   moo No.12
Type of property: house

Tanbon: Bangna

Name of Registration Office: Prakanong
District: Prakanong   Province: Bangkok

Rank	Personal ID numbers / Title First name / Last name	Sex	Status	Date of birth	Nationality / Microfilm #	List of father and mother: Personal ID # / Name	Nationality	Move in: from	signature	Move out: to	signature
1.	3100903491692 Dr Teera Ramasoota	M	X host head / dweller	25 Aug 1931	Thai / 0 02200 0421	Yeun / Khun Ramasoo Kosakorn	Thai / Thai	on 13 Dec. 82			
2.	3100903491706 Mrs. Pantyp Ramasoota	F	host head / X dweller	23 Nov 1936	Thai / 0 022004421	Buatong / Amorn	Thai / Thai	on 19 Nov. 74			
3.	3100903401714 Mr. Pongrama Ramasoota	M	host head / X dweller	28 Aug 1962	Thai / 0 022004421	Teera / Pantyp	Thai / Thai	on 19 Nov. 74			
4.	3100903491722 Mr. Pachara Ramasoota	M	host head / X dweller	3 Apr 1964	Thai / 0 022004421	Teera / Pantyp	Thai / Thai	on 19 Nov. 74			
5.	5100909024159 Miss Pirongrong Ramasoota	F	host head / X dweller	12 Aug 1967	Thai / 0 098011682	Teera / Pantyp	Thai / Thai	on 19 Nov. 74			

130

The two main files are the household registration file or the "house file" and the personal identity card file or the "pop file." Although the early advocates of the CPD had talked about collecting crucial personal information like income and profession prior to the creation of the CPD, this did not materialize largely due to legal limitation. The Civil Registration Act B.E. 2499 (1956), which was still in effect until 1991 only enabled registrars to collect basic information such as listing of names in a household, births, deaths, moves, and the like. This outdated law was mainly designed to accommodate traditional civil registration work, which did not foresee the massive storage of citizens' information for any other purposes but civil registration.

As a result, there has been no dramatic change in terms of the sensitivity of the information collected. The pop file, for instance, contains the following fields of information: personal identification numbers, name, gender, date of birth, nationality, person's status,[55] father's identification number, mother's identification number, father's name, mother's name, father's nationality, mother's nationality, house identification numbers, address, photo, and prints of right and left thumbs. Essentially, the major additional change in the new computerized file was the fingerprints.

In 1993, a new file was added to the CPD. This was the facial image and thumbprint file. Unlike the other files which were text-based, this file, using optical disk as a means of storage, contains compressed digital images of citizens' faces and thumbprints. The creation of the file began in 1993 following the replacement of an old ID card application form with a new and computer-readable form. This new form, which is still used in most of the registration offices, contains boxes for photo and thumb prints which are readily scannable into the computer memory. In the process of scanning the images from the application forms onto the optical disk, the thumb prints are also classified according to the patterns of minutiae and given a code accordingly. This classification and encoding are intended for future verification purposes. In fact, this file was invented as part of the effort to create an integrated system of personal verification by drawing not only upon computerized textual records but also computerized records of images.[56] Aside from enhancing the capability of verification, the new file is also intended to help reduce the incidence of fraud in the issuance of personal identity cards. Without the advent

---

[55] A person's status covers more than marital status. These are the statuses that a Thai resident can be classified as -- deceased, single, married, divorced, in exile, registered under a household registration document, registered by a birth certificate, registered by approved adding of name in a household registration document.
[56] An ordinary personal verification process would rely on three important fields of information as contained in the personal identification card files of the CPD. They are: 13-digit personal identification numbers, the number on the application form for a personal ID, and first and last name.

of the optical disk, the construction of this file would not have been possible.[57] Retrieval of information in this file now involves much less effort than searching manually in the microfilm library as was the case in the past.

Growth in surveillance capacities and institutional capacities to affect people's lives.

As far as bureaucratic surveillance is concerned, the PIN I project has increased the state's capacity to monitor its citizens in at least three aspects. First, the size of the files held by the central government on its citizens significantly expanded. By 1988, the CPD hosted approximately 52 million personal records and about 11 million household registration records. More people were incorporated into the system than ever before. Secondly, as the design of the CPD well attested, these files were highly centralized. All the information about the provincial populace which used to be scattered in district registration offices around the country, was now available within one centralized databank in Bangkok. With a few strokes on a keyboard, an official at the central government could access the personal record of any citizen in the country by searching under his or her name or using other key information. In addition, the speed with which the CPD rendered information was also remarkable as it would only take an average of three seconds to access any individual citizen's record from a terminal at the Registration Administration Bureau. Ironically, however, such speedy and easy access was limited to the Bangkok center, which maintained virtually no contact with most of the population whose records were stored in the CPD. Provincial or local officials who deal directly with this population were not blessed with such access. Provincial registration officials, in particular, still had to do everything manually and had to send all civil registration applications and new information to the center for updating of the CPD and for transactions such as the issuance of household registration documents and personal identity cards. Irksome as this centralized arrangement was, it had been the norm for the entire country until at least the launch of PIN II in 1996.

According to two senior officials who have been involved with the PIN project from the beginning, this highly centralized design of the CPD was not deliberate but was the most technologically feasible option at the time.[58] They argue that a distributed database setup would

---

[57] Optical disk storage uses laser beams to store a massive amount of data in digital form. It is particularly useful for storing images, which generally require much more memory. A single optical disk can store four billion characters, comparable to forty reels of magnetic tape.

[58] Mr. Vichian Chidchanognarth, head of the registration processing center, division 3 (Nakhon Ratchasima), interview by author, 3 January 1996, Bangkok, registration processing center, Registration Administration Bureau, Bangkok; and Mr. Surachai Srisaracam, director of the registration processing center, interview by author, 9 October 1996, Bangkok, registration processing center, Registration Administration Bureau, Bangkok.

compromise the data integrity and would require more expertise and maintenance skills, which the local and provincial registration offices did not have. A view from the actual designer of the CPD was contradictory. According to an employee at Control Data Group (CDG), which was the system designer and technical supporter for PIN I, the centralized design was entirely deliberate.[59] Having worked with many officials at the Department of Local Administration for a number of years, this CDG employee who asked not to be named, said that it was clear from the beginning that the CPD was to be an information resource to facilitate control from the center over the peripheral provinces. In initiating the PIN, the central authority of the Ministry of the Interior cited their concern about the rampant fraud and abuses at civil registration offices in the remote provinces. Thus, they would contemplate only the design that would most enable centralized control. According to their plan, the CPD was to be a standard database for verification of civil registration information for the whole country. If a filed civil registration application from a province carries contradictory information, it will not be processed unless it is corrected to accord with the information in the CPD.

Although the centralized arrangement of the CPD obviously hindered efficiency in many transactions, the overall PIN I project was still a "tremendous success," according to the people who implemented it. To many officials who have been involved with PIN I, the benefits accruing to the state, particularly the enhanced social control, far outweighed the costs.[60] Aside from enabling the state to better locate citizens and verify identities of non-citizens, the PIN I project also rendered important aggregate population data for national planning and policy-making. The CPD data, it is argued, is a more accurate indicator than statistics-based census data since it is constituted of actual registered persons and households and not mere estimates. Another contribution most often ascribed to the PIN I is its ability to purge false persons and multiple registrations from the system. Since the CPD was programmed to reject any names with common attributes -- address, date of birth, personal identification numbers -- that appear in more than one household registration, it was no longer possible for anyone to be registered in more

---

[59] An employee of Control Data Group Co., interview by author, 14 September 1996, Bangkok, Control Data Group Co. office, Bangkok. Control Data Group (CDG) began operation in Thailand over three decades ago as a subsidiary of the Minneapolis-based Control Data System Corporation (CDS) which technically supported the US military operation in the region. About ten years ago, the American partner withdrew and a group of Thai businessmen bought out the shares and turned it into a successful computer solution corporation. CDG's business comes mainly from government contracted computer projects. It maintains links with CDS for technical collaboration while also acting as the latter's local distributor for some information technology products. This account on CDG Corporation was given to me orally by the same employee.

[60] According to one official, the CPD costs about Bt100 (US$4) for every Thai citizen, but the payoffs from it are unmeasurable. Mr. Vichian Chidchanognarth, , head of the registration processing center, division 3 (Nakhon Ratchasima), interview by author, 3 January 1996, Bangkok, 131 registration processing center, Registration Administration Bureau, Bangkok.

than one household.[61] Prior to the advent of the CPD, people had exploited and abused this loophole in the civil registration system in various ways. One of the most widespread forms of abuse was the frequent incidence of "ghost voters," where a person would show up at an election to cast a vote by assuming the identity of another person who had multiple registrations. With the new automatic processing potential of the CPD, it was believed that such errors associated with the manual system of the past had been removed. "If you enter in the correct information, it will remain correct forever."[62]

Following this line of technophilic thinking, the Ministry of Interior seems to put much faith in the CPD's voters' listing file as a means to guarantee a fair and clean election. Accuracy of voters' information, it is argued, is very crucial to the many elections that take place at different levels of administration in Thailand. Given the rising democratic awareness among the Thai populace, it seems that the Ministry of Interior has been drawing particularly upon this electoral list file as a sales pitch for the PIN and a point to highlight their central role in promoting democracy. Nevertheless, their conception of democracy is rather myopic as it is restricted to voting in elections. A citizen's right to vote overshadows all other rights in their understanding of democracy. While the CPD's voters' listing file may substantially facilitate the election process with updated and comprehensive information on each voter, it does not in any way eliminate or help prevent fraud.[63] Poll fraud usually occurs because election officials turn a blind eye or, in some cases, conspire with the violators.

In the general election in November 1996, there were cases where Pollwatch volunteers found that the ID numbers of many voters who had cast ballots were not the same as those written in the voters' list.[64] Yet, polling officials, who were mainly from the Ministry of Interior, allowed these problematic voters to flee the scene when the volunteers tried to investigate the

---

[61] In cases where people have identical names, the computer could also distinguish them by the very same attributes.

[62] The official interviewed defined multiple identities as people who were registered in more than one household registration. Mr. Chakkri Cheun-ura, head of the technical registration section, interview by author, 23 August 1996, Bangkok, registration processing center, the Registration Administration Bureau, Bangkok.

[63] Voters' information changes every year due to changes such as moves, new 18-year-olds, new citizens and deaths. With the PIN's comprehensive civil registration system, these changes can be captured and updated more easily.

[64] In many people's views, the November 1996 election was seen as the dirtiest in three decades, comparable to the one in 1957. The Pollwatch Committee, which was authorized to oversee the election process, reported 4,260 cases of violations of the election law. The most prevalent form of violation was vote-buying and gift-giving to eligible voters. During the campaign period leading up to the election, the Bank of Thailand reported a cash flow of at least Bt20 billion (US$800 million), most of which was suspected to be money to buy votes. Supradit Kanwanich, "Vote-Buying in All Bangkok Constituencies," *The Bangkok Post*, 24 November 1996, 5.

matter.[65] There were also cases of pre-marked ballots and repeat balloters which could not have happened without the polling booth supervisors noticing.[66] Moreover, there were also reported cases of buying of personal identity cards and outright vote-buying, which was widespread in the rural provinces. Such frauds illustrate the existence of well-organized systems of vote soliciting in which local influence and patron-client relationships played major roles. In this light, the centralized control of Bangkok officials, which may have been enhanced by the PIN I project, did not seem to amount to much.

There is yet another irony in the Ministry of Interior's constant stress on the importance of the computerized voters' listing in the process of democratization. The fact that the election law allowed political parties to obtain the voters' list from district civil registration offices contributed directly to the efforts to rig the elections. With the help of the voters' listing, dirty politicians and their vote canvassers knew at least one month prior to the election day the names, addresses, and gender of the eligible voters in each constituency. Needless to say, this information could greatly assist in their vote-soliciting strategies. When questioned about this, a Ministry of Interior official responded that the voters' list would, in any case, be made public as it is customary to post it in the town hall or designated ballot site at least one month prior to the election date. One need not be a politician to have access to this publicized information.[67]

There is an even more distressing chapter in the election fraud story associated with the computerized voters' listing. According to the president of the Confederation of Thai Democracy,[68] there was an incident in 1995 in which civil registration officials in Khlong Toey district in Bangkok moved the registered names of more than 1,000 slum residents to a totally different household registry in another district in Samut Prakarn province in the outskirts of Bangkok. The slum residents were never notified. The maneuver was intended to construct an illegitimate and illusory basis of votes for a candidate vying for an upcoming electoral position in a municipal council in Samut Prakarn.[69] As to why these slum residents were picked as a means to achieve this fraud instead of others, it is most likely because of their poverty and powerlessness. As far as their legal standing is concerned, slum residents are also the most

---

[65] Ibid.

[66] This is a case in which one voter casts his ballot and repeats the process using names of other voters in the registry.

[67] Mr. Chakkri Cheun-ura, head of the technical registration section, interview by author, 23 August 1996, Bangkok, registration processing center, the Registration Administration Bureau, Bangkok.'

[68] This organization is the leading NGO in promoting democracy in Thailand.

[69] Editorial staff, "Lifiting the Curtain of the Confederation of Thai Democracy: Prof. Dr. San Hattheerat," (waek maan pit tuaton samaphan prachathipatai : Prof. Dr. San Hattherat) Hi-Class Magazine, December 1995, 50.

vulnerable. This is because they usually encroach upon pieces of public land or proprietary land and settle in by building shanties or some form of poorly-constructed shelters. The fact that the district office would allow them to be registered in a household registry at all is likely viewed as a big favor. Being registered in a household registry is a basic need for a person in Thailand today. For instance, a child of a slum resident could never attend school. even at the compulsory level, unless he or she had his or her name listed in a household registration document. As a result, district officials had a significant leverage over these slum dwellers, and it is probably this leverage that led to the exploitation of the slum residents' "digital self."[70] The action, however. drew outcries from some of the slum residents who found themselves listed in a totally different neighborhood, at least for the period leading up to the election in Samut Prakam.

As far as the Thai public was concerned, it may be fair to say that, unlike in the case of the state, there were no obvious benefits rendered to them from the PIN I project. For most citizens, PIN I probably just meant a new look for their personal identity card and their household registration document. Most Thais. as mentioned earlier, were not informed about the PIN project and its objectives when it was being conceived. Nevertheless, the gradual but significant impacts of the PIN I project have been felt by the populace nationwide.

While state surveillance has always been a part of Thai history, it has also been plagued with organizational behavior and technical limitations that would together undermine its efficiency in engendering control. With the development of the CPD and the increased capacities for surveillance it renders, the impacts have been two-fold. The state's already large public realm has been expanded and strengthened, while the citizens' private realm has been reduced and weakened even more. Although citizens may generate the information contained in civil registration files, they cannot legally claim ownership of it as long as this information is stored in the CPD. In effect, the legitimacy of the state's ownership over this information was reinforced with the creation of the CPD.

---

[70] The concept of "digital self" is adapted from Max Kilger 's concept of the "digital individual." Kilger conceptualizes it as a form of computerized identification. or a substitute representation of an actual individual human being in the sphere of computer and digital communication. Max Kilger. "The Digital Individual." *The Information Society* 10 (March 1994): 93-99. In the same vein. Mark Poster. as earlier discussed, also talks about the discourse of databases and argues that databases are not only an invasion of privacy but also a threat to a centered individual, since they led to the multiplication of the individual, and to the constitution of an additional self. Mark Poster, 1990. *The Mode of Information: Poststructuralism and Social Context.* (Chicago: University of Chicago Press, 1990). 97.

In the beginning of 1996 when PIN II, a continuation of PIN I was launched. Thailand had 57.7 million people and 12.7 million households registered within the CPD. While this was a remarkable figure, it was estimated by the authority in charge that close to five per cent of the population were still outside the system.[71] The unregistered consisted mainly of the older generation who were born long before the launch of PIN I;[72] those who belong to nomadic tribes or hill tribes; and illegal immigrants from neighboring countries in Southeast Asia and South Asia.[73] These unregistered individuals, it is argued, will be forced to enter the system one way or another. As more ID cards and household registration cards have been distributed and more people have been incorporated into the system, it has become commonplace for government organizations and private enterprises to require the presentation and/or supply of these two documents or photocopies in semi-formal to formal circumstances. For instance, they are required when visiting a government office or a corporate premise, applying for a telephone line, buying a cellular phone, enrolling in an academic institution, applying for a job, opening a bank account, applying for a credit card, enrolling for conscription, getting a driver's license, and voting in a political election. Usually, the requested photocopies of the two documents are only kept for reference or security purposes. Nevertheless, this customary practice has gradually produced important and profound disciplinary effects on individuals, in their capacities as citizen, employee, and consumer. It is almost fair to say that Thais have internalized the habit of presenting and supplying their IDs in most semi-formal to formal transactions.

Interestingly enough, however, while most citizens have increasingly found their national ID card to be indispensable, very few would connect the ID card to the existence of the CPD. Participants in one of the focus groups on information privacy, which is the subject of chapter seven, were asked if they recalled anything about the PIN project when it was launched in 1984. Everyone (except for the one participant who works at the Ministry of Interior) admitted they knew nothing about it. However, most participants recalled the change from a poor-quality ID card with a black and white photo to a new and better-quality ID card with a color picture, which

---

[71] Mr. Chakkri Cheun-ura, head of the technical registration section, interview by author, 23 August 1996, Bangkok, registration processing center, the Registration Administration Bureau, Bangkok.

[72] This category also includes individuals who, despite being registered in the CPD, did not actually bear personal ID cards containing the 13-digit identification number issued in 1983. One example is my own father who, when PIN I was launched, was working in the civil service and could get by with his civil servant ID. After he retired a few years ago, he was able to get a retiree card for civil servants, which could substitute for the Ministry of Interior's ID card. Nevertheless, he is registered in the CPD database and was assigned a personal identification number although he has never carried an actual ID card with that number.

[73] At the time of writing, it is estimated that there are about one million illegal immigrants residing in Thailand. Most are from the neighboring countries in Indochina -- Burma, Laos, Cambodia and Vietnam and also from certain South Asian countries such as Bangladesh. Mr. Chakkri Cheun-ura, head of the technical registration section, interview by author, 23 August 1996, Bangkok, registration processing center, the Registration Administration Bureau, Bangkok.

all of them found more appealing. As far as having their thumbs prints taken for this 1984-version ID, everyone seemed unperturbed by it. It should be briefly noted that having fingerprints taken is not uncommon in Thailand even when one is not a criminal suspect. As part of the screening for all public positions, one is required to have their fingerprints verified at the criminal records registration division of the Police department.[74]

Access to Records, Third Party Inter-Organizational Transfers of Information, and Data Protection at the CPD

The Civil Registration Act B.E. 2534 (1991) specifies that all civil registration information must be kept confidential and only permits access to individuals who want to review records on themselves, to authorized persons, and to stakeholders.[75] However, the law does not limit the use of the information to only the civil registration purpose for which it was gathered. National security and statistics are indicated as possible purposes for the data usage. Besides, Article 15 of the law also empowered any government agencies to access civil registration information by submitting document requests and through computer file sharing. In fact, the Ministry of Interior has been quite open to requests for data from the CPD as long as they remain the gatekeeper of access.

In 1985, the Ministry set up a special unit to specialize in providing civil registration information services to government agencies, private enterprises, and individuals. As outlined in its formal guideline, this section has the following functions:

1) to provide services in verifying and examining a person's personal history and household registration information according to the information in the CPD;
2) to provide population statistics;
3) to provide copies of civil registration documents, namely, birth certificates, death certificates, move notification forms, household registration documents,

---

[74] Before I was officially hired for a teaching position at Chulalongkorn University, I also had to have my fingerprints verified. The process involved going to the police station in the district where I was a registered resident, having the fingerprints verified by a police official, and awaiting reply from the university since the result of the verification was sent directly to the university.

[75] According to article 17 of the Civil Registration Act B.E. 2534 (1991), a stakeholder is defined as an individual or organization who has a legal relationship with the person whose record is to be examined. But according to guidelines for disclosure of citizens' information at the data provision section of the Registration Administration Bureau, stakeholder also covers the following: 1) an individual who has his or her name listed in the same household registration as the person whose record is to be examined; and 2) an individual or organizations who could furnish evidence of business contract or dealings with the person whose record is to be examined.

138

which are collected in the Registration Administration Bureau's microfilm library;
4) to provide services in amending information in the CPD and in civil registration documents; and
5) to provide services in verifying and identifying a person with the stored digital records of photo and fingerprint images.[76]

At a price of Bt10 (around 25 US cents) per one released copy of information, individual citizens and private organizations can request all the above services with the exception of 5) on the condition that they supply necessary supporting documentation. Government agencies and state enterprises are exempted from paying this fee. The services in 1) and 3) are provided only to individuals who request to examine information about themselves and to "stakeholders." Guidelines are clearly laid out regulating the release of such information to individual citizens, private organizations and banks.[77] Government institutions are exempted from this regulation, and so it seems they are entitled to disclosure of any types of information in the CPD. Supporting identification documents, which are required to accompany requests for access to the CPD data, are copies of household registration card, and copies of personal identity cards. As for private enterprises and banks, they are required to provide a document certifying business establishment and a copy of a relevant contract or document that demonstrates the relationship between the business and the party to be examined, for instance, loans contract, lease contract, or guarantor's contract. Requests of data for litigation purposes require that lawyers furnish a copy of their lawyer ID and a subpoena.

According to the head of the data provision unit, each request is thoroughly considered before any information is released.[78] Any request which lacks supporting documentation will not be processed. The official also said he and the staff in his unit adhere strongly to the confidentiality principle of the Civil Registration Act. He said there were cases in which direct mail and marketing companies requested lists of people's names and addresses in certain districts in Bangkok but were turned down because of their inability to furnish necessary supporting evidence. Citing article 17 of the Civil Registration Act 1991, which deals with confidentiality of the information, the official asserted that information can only be released as aggregate statistics. This means that it would contain only bald figures and not names and addresses of each individual.

---

[76] History and guideline of the Data Provision Service Section (unpublished material), no page number.
[77] It is important to note that banks stand out as a distinct category in this guideline.
[78] Mr. Chavalit Chitrman, head of the data provision service section, interview by author, 3 August 1996. Bangkok, the Registration Administration Bureau, Bangkok.

This Data Provision Service Section. which consists of fewer than ten staff members. handled about 400-500 requests daily and collected more than Bt3 million (US$120.000) in processing fees in 1995. These earnings came from fees collected from individuals and private enterprises who submitted a combined total of 79,847 requests to examine records on individual citizens during that period. The requests generated a release of 302,958 copies of records. Meanwhile. government agencies submitted a total of 29,915 requests for data in the same category and were delivered 120,887 copies of records. Requests for data on citizens' personal records accounted for the largest number of incoming requests while requests for statistical data were comparatively small. This is despite the consistent claim by many Ministry of Interior officials that most of the data released from the CPD are aggregate statistics for development and policy-making purposes. Table 4.3 provides a monthly breakdown in the number of requests and the number of released copies according to categories of data and types of requested parties during each month in 1995.

Of all the government institutions requesting data from the CPD, the Ministry of Interior made the most number of requests to examine personal records with a total of 19,718 requests.[79] The Police Department made the second largest number of such requests with 2,367 requests, followed by the Ministry of Agriculture and Cooperatives, the Ministry of Finance, the Ministry of Justice, the Land Department, and the Ministry of Education. each of which submitted 1,556, 971, 644, 547 and 61 requests, respectively. Table 4.4 provides details of this ranking and the number of requests made by different government agencies to examine registered personal records in 1995.

With regard to requests for statistical information. the Ministry of Justice seemed to be the most interested in statistics with 988 requests, followed by the Ministry of Public Health, Ministry of Education, Ministry of Communications and Transportation, and Ministry of Interior. with 102, 38, 37, and 11 requests, respectively. Of all 17 government agencies listed as clients of the Data Provision Service Section in 1995, only the above five made requests for statistical information.

---

[79] Most of these requests came from the Department of Local Administration, which directly oversees the Registration Administration Bureau.

Table 4.3: Number of requests for examination and verification of citizens' personal records and for statistics, and the number of released copies according to the types of requesters in 1995

Month	Examination and verification of personal records								Statistics	
	Public (government)		Private (organizations and individuals)		State enterprises		Sections within the Registration Administration Bureau		Public	Private
	No. of filed requests	No. of released copies	No. of filed requests	No. of released copies	No. of filed requests	No. of released copies	No. of filed requests	No. of released copies	No. of released copies	No. of released copies
January	2,565	6,950	5,942	22,569	96	1,507	34	51	40	41
February	2,644	8,697	5,622	21,574	85	1,289	38	50	51	3
March	2,769	9,325	6,542	27,321	138	1,543	50	57	34	59
April	1,927	5,628	4,710	19,046	226	1,284	24	29	19	28
May	2,598	10,899	6,780	25,009	74	1,043	40	72	53	55
June	3,548	15,399	6,805	26,581	95	2,035	40	78	35	66
July	2,546	15,399	6,732	24,623	81	1,136	28	31	28	31
August	2,591	13,003	7,565	30,512	73	1,346	28	48	33	54
September	2,254	10,047	6,987	28,964	104	1,772	44	82	61	40
October	2,120	8,194	6,933	28,245	84	2,061	31	47	44	28
November	2,409	8,987	9,514	29,908	110	2,501	25	39	56	13
December	1,944	8,353	5,715	18,606	69	1,311	21	29	54	50
Total	29,915	120,881	79,847	302,958	1,235	17,838	403	613	508	495

Source: Summary of the services provided by the data provision section, the Registration Administration Bureau in 1995.

141

Table 4.4

Number of requests filed by government organizations to examine citizens' records
in computerized files at the Registration Administration Bureau in 1995

Rank	Name of Agency	No. of requests
1.	Ministry of Interior (esp. Dept. of Local Administration)	19,718
2.	Department of Police	2,337
3.	Ministry of Agriculture and Cooperatives	1,556
4.	Ministry of Finance	971
5.	Ministry of Justice	644
6.	Land Department	547
7.	Ministry of Education	61
8.	Ministry of Labor and Social Insurance	49
9.	Ministry of Defence/ Ministry of Public Works	41
10.	Ministry of Prime Minister's Office	39
11.	Department of Social Service	33
12	Ministry of Public Health	28
13.	Ministry of University Affairs	25
14.	State enterprises	22
15.	Ministry of Transport and Communications	19
16.	Ministry of Foreign Affairs	9

Source: Summary of data provision services during January - December, 1995, civil
registration section, the Registration Administration Bureau

Besides access to copies of printed records, many government agencies have gained electronic access to the CPD via an on-line connection. This began some time in 1995 with the Police Department, the Revenue Department, and the Social Insurance Office. These three departments have their own databases, which employ different identification numbers from the CPD's 13-digit personal identification numbers. However, the 13-digit numbers were included as one of the fields in their record-keeping systems. These agencies' connection to the CPD is at present one-way and provides only a read-only access. In addition, some organizations and individuals can also access the CPD through more informal avenues. For instance, government agencies that deal with national security and intelligence can easily bypass the bureaucratic red tape to access the CPD. In the meantime, there are incidents where officials would do favors for friends or other associates in their patron-client networks by allowing access to the database. This is akin to what Arthur Miller describes as the "information buddy system" whereby a group of acquaintances in related professions develop "a subterranean information exchange network that functions on a mutual back-scratching basis or can be invoked for a fee."[80]

To date, banks have been the most privileged clients of the CPD. When the CPD first became operational, the authority at the Registration Administration Bureau was said to be very proud and had allowed employees of certain local banks to check out the database.[81] In other words, these bank employees could come in and look up from one of the terminals at the Registration Administration Bureau the record of any loan borrower with a delinquent account. Although they were only allowed access to the read-only inquiry screen, this was already very useful in tracing people with bad credit or other financial problems with the bank. This open access was later revoked after news about it was leaked to a foreign magazine, which later published the story and alleged intrusion of citizen privacy by the Ministry of Interior.[82] However, the practice did not seem to stop entirely. Recent anecdotal evidence came from a colleague at Chulalongkorn University who claimed that one of her graduate students, a full-time employee at a local bank, looked up her birth date from the CPD and gave her a surprise birthday wish. This incident happened in 1996.

---

[80] Arthur Miller, "Computers, Data Banks, and Individual Privacy: an Overview," *Columbia Human Rights Law Review* 4, no. 1 (1972): 10.

[81] This information is obtained from an interview from a person who has been actively involved in the development of the PIN and also wishes to be anonymous.

[82] This account was relayed to me by an employee at the Control Data Group (CDG) Corporation. It was later confirmed by Mr. Prakit Kanyabal, director of the Registration Administration Bureau, at the time. However, I was never able to find out the name or issue of the magazine that published the article in question.

While the "birthday wish" incident above may be benign enough. there are other detrimental uses that such open access to the database could lead to. Although there have never been cases of abuses publicized. this does not mean they do not exist. Since each citizen basically loses control of his or her information once it enters into the database, there is simply no sure way of detecting abuses. Besides. in the absence of a data protection law. a privacy or information controller organization. and most importantly. a public awareness about the rights of privacy, what is considered abuse by liberal western standards may not be so understood in the Thai context. On this note, I have conducted an interview with a senior executive at Telecom Asia Corporation, which is a major telecommunications concern in Thailand. This executive said his company had contacted the Registration Administration Bureau to request copies of citizen's records in certain areas of Bangkok as part of the effort to compile a database of potential consumers. He was presented with an offer to purchase the record at the price of Bt5 each (two US cents). This executive declined to name the section or official he spoke to.[83]

In addition to relatively loose restriction on access, the lack of effective enforcement on security measures and technical safeguards also undermines data protection measures at the CPD. To begin with, physical security was minimal particularly in the main data entry room, which housed about 450 data entry operators and at least 500 client terminals. Located on the second floor of the Registration Administration Bureau building. this room did not have a security guard and the security door, which would have required a key card, had been broken for a number of years. Entry screen terminals and query terminals were always left on even during lunch hours when the room was deserted. Workers' awareness of security issues was low, and no one was serious in keeping their login and password a secret. Even supervisors with higher hierarchy of access would make their password known to their subordinates for reasons of convenience.

As most of the workers in that room were female aged between 25-40, I could easily blend in as one of them. On one occasion during the site visit, I conducted a small experiment by pretending to be one of the data entry operators. Since it was during lunch time, most of the computer terminals were freed up, and the room was half empty. Just as expected, no one paid any attention as I spent more than twenty minutes looking up personal information of local celebrities and friends.

---

[83] Dr. Jen Sriwatthanathamma, director, Computer System and Services, Telecom Asia Corporation (Public Company), interview by author. May 9 1996, Bangkok. Telecom Asia Corporation, Bangkok.

According to interviews with several data operators, supervisors, and high-ranking officials who oversee the PIN project, there have not been any major cases of abuses -- unauthorized access, illegal disclosures, and use -- of data in the CPD. There were some "minor" incidents in which data entry operators were looking up some records for friends as favors. Normally, in this situation, supervisors would give a warning and supposedly keep an eye on the person. So far, no one has been permanently removed from the job for such practices. To date, the heaviest reprimand was a demotion and a relocation to a different type of responsibility.

Despite this apparent lack of concern about data protection, the PIN I project won in 1990 an award from a contest held in the United States for computer applications in record-keeping. The award entitled the Smithsonian Computerworld Award was bestowed on the CPD initiator for "heroic use of information." According to the official who formally received the award on behalf of the Ministry of Interior, it was the first time this award was given to an institution from outside of the US. The Ministry of Interior and its PIN project was chosen from among 250 organizations, government and non-government, worldwide. The award was offered to the Thai project for "its implementation of information technology for public interest and with vision in development."[84] Winning this award seemed to heighten the Ministry of Interior's belief in the PIN's merits as it was proudly recorded in underlined scripts in one of the Ministry's official documents that,

> This award which began in 1989 was initiated to illustrate the benefits of innovation in information technology. It is an international award for computer application, almost an equivalent of the Nobel Prize. The recipient of the award will have their project permanently exhibited at the Historical Museum of the Smithsonian Institution, in Washington DC, U.S.A. (original emphasis)[85]

---

[84] Mr. Surachai Srisarakham, director of the registration processing center, interview by author, 9 October 1996, Bangkok, the Registration Administration Bureau, Bangkok.

[85] Ministry of Interior, Summary Report of the Project for the New Registration System to Service the Public by Using Computer and the Project to Establish a Management Information System for Administrative Purposes (khrongkarn jantham rabob karn hai borikarn prachachon thang darn karn thabian lae bat duay computer phram karn jad tham rabob khormun khaosarn pheu karn boriharn ngarn) (Bangkok: Ministry of Interior, 1995), 2.

145

In 1991, three years after the CPD was established, a new civil registration law was passed to replace the outdated law which had been enacted in 1956. One of the main reasons for passing the Civil Registration Act BE. 2534 (1991) was to accommodate computerized record-keeping. Interestingly, the law provided retroactive legal grounding for several activities accomplished during the PIN I. For instance, article 16 of the law reads:

> in the collection of civil registration information, the director of the Registration Administration Bureau is responsible for assigning unique sets of personal identification numbers to each and every individual residing in the Thai kingdom.[86]

Besides, unlike the old law which was vague and ambiguous in the treatment of the term "information," this law specifies clearly what civil registration information would and would not cover. According to article 4 of the law, civil registration information is defined as:

> "Identifiable and personal information of individuals which includes first name, last name, gender, date of birth, date of death, nationality, religion, area of origin, marital status, educational achievement, name of father and mother or adopted parents, name of spouse, name of offsprings, and other information which is necessary for the operation of registration work according to this legislation."[87]

Correspondingly, article 13 of the law indicates that the collection of civil registration information does *not* include the following personal information:

> 1) income; 2) criminal records; 3) tax filing records; 4) information which is determined by the Cabinet; and 5) information which an individual is not legally required to report.[88]

According to a law professor who was involved in the drafting and revision of this law, this particular article was a result of his input and came from extreme privacy concerns. This legal scholar claims that he was one of the very few who realized the privacy implications of such a large database of personal information and has been trying to raise public awareness on the issue since the inception of the PIN project. The incorporation of the provision in the

---

[86] Registration Administration Bureau, *Manual for the Operation of Civil Registration* (*khu meu karn patibat ngan thabian rasadorn*) (Bangkok: Department of Local Administration, 1996), 6.
[87] Ibid., 1.
[88] Ibid., 5.

above article is to construct some form of a legal safeguard against further erosion of privacy through the use of personal files held by the government.[89']

Apart from accommodating computerized surveillance by the government, the new civil registration legislation also further consolidates the power of the Ministry of Interior in overseeing the country's civil registration system. Article 8 of the law provides that the Registration Administration Bureau has a responsibility in controlling the operation of civil registration nationwide. According to this article, the director-general of the Department of Local Administration is the Central Registrar whose jurisdiction spans over the entire kingdom. The same article also empowers the permanent-secretary of the Bangkok Metropolitan Administration (BMA) as the registrar for Bangkok and the Metropolis area. The jurisdiction of the BMA registrar, however, falls under that of the Ministry of Interior.[90]

In addition to the passing of the new civil registration law, a major restructuring also took place within the Ministry of Interior during the period between PIN I and PIN II. Prior to the restructuring, civil registration and personal identity card tasks were under the collaborative care of three agencies -- the personal identity card division, the registration division, and the Registration Administration Bureau. In 1993, a law was passed to decree the establishment of the Registration Administration Bureau, which grouped the three agencies above under one single entity. However, this newly-established Registration Administration Bureau, which would normally be an equivalent of a *krom* (department), is still under the administrative umbrella of the huge Department of Local Administration. The new agency has 1331 civil servants and 51 full-time and part-time employees.

PIN II (1996 - 2001) -- DISTRIBUTION OF DATA PROCESSING AND ISSUANCE OF PERSONAL IDENTITY CARDS WITH MAGNETIC STRIPE

Although the proposal for PIN II was raised in 1992, it was only in 1995 that the project was approved by the Cabinet. The significant delay was owing to the discontinuity in government and budgetary problems.[91] With a combined investment of Bt5.74 billion

---

[89'] Dr. Borvornsak Uwanno, professor of law, Chulalongkorn University, telephone interview by author, 17 September 1996, Bangkok, Chulalongkorn University, Bangkok.

[90] Ibid., 3-4.

[91] From 1991 to 1996 when the new civil registration law was passed until the implementation of PIN II, Thailand had five different governments. One of these lasted only for a month as it was led by a non-elected military general premier, Gen. Suchinda Kraprayoon, who finally stepped down after the bloody crackdown in May 1992.

(US$229.6 million). PIN II involves three important activities: 1) distribution of certain data-processing transactions to provincial and district registration offices nationwide; 2) issuance of a new form of personal identity card at civil registration offices nationwide: and 3) establishing a hierarchical on-line information network between the Bangkok-based CPD and civil registration offices in all parts of the countries.

PIN II was conceived to meet two main needs. First and foremost was the need for increased efficiency. The centralized arrangement whereby all types of civil registration applications from all parts of the country had to be processed at the Registration Administration Bureau in Bangkok resulted in a major bottleneck, particularly in the issuance of personal identity cards.[92] The slow mailing system also made a timely updating of the CPD impossible, resulting in its containing inaccurate and obsolete information. Consequently, the provincial and district registration offices,which still used paper filing for their reference registration records, were very slow and inefficient in servicing the public.

Along with the need to increase efficiency, there was also a need to better prevent fraud and corruption, which were still rampant especially in the rural civil registration offices. After so many years of enforcement, the 1988-version personal ID card, which was laminated with special seals, was also subject to the falsification problem. Because of the bottleneck in PIN I, many rural registration offices, even at the time of writing (1997), are still using the 1962 version of the household registration card. Since change could be made with handwriting, this document was highly prone to fraud. Nevertheless, the new 1988 version, which was a computer printout document, was not fraud-free either. Theoretically, any change in the 1988 household registration card ought to have been made at the Registration Administration Bureau, which was the location of the CPD and the only place with the proper equipment. Before 1996, most district civil registration offices were not equipped with computers or any associated peripherals that would enable them to make computerized changes. As a result, registrars or assistant registrars would sometimes resort to handwriting in making changes to the household registration document and would sign their names to authorize the change(s) made. This opened ways for dishonest officials and citizens to follow suit and led to the same fraud problem.

---

[92] During a site visit in August of 1996, I noticed that one of the data entry operators was processing an ID card application from a remote province, which was dated May 1996. This means that there was at least a three-month backlog in data entry. In addition, a report by the Ministry of Interior also indicated that about 5-10 per cent of the photos taken for the personal identification card were unusable. This resulted in even more lengthy delay since the applications would have to be returned to the original district office and the same process repeated again.

Therefore, in launching PIN II, the Ministry of Interior declared the following as its objectives:

1) to improve the efficiency of civil registration services for the public. The improved service will be fast, accurate, attractive and more effective in preventing fraud and corruption;

2) to provide a one-stop service for the issuance of the new personal identity card and the new household registration passbook at district and local registration offices;

3) to further extend the use of the CPD to support other applications such as the voters' listing and revenue collection.

4) to improve the efficiency in the administration, policy implementation, and communication of all levels of civil registration offices nationwide.[93]

The overall PIN II project is divided into two phases each of which involves these activities:

Phase I of the project (1996-1997), a Bt1.53 billion (US$61.28 million) investment spans over two years of operation. The first year (1996) involved the installation of computer systems and communication systems in all thirty-eight district offices in the Bangkok Metropolitan Area. This has established an on-line database system which linked the thirty-eight district offices with the CPD.[94] Under this plan, each district office is equipped with a client/server system, which consists of a UNIX server and personal computers (PC) as client workstations. The initial number of PCs was determined by the size of the population in each district. In this system, which is presently used, the UNIX server serves as a distributed database that will host the information on all registered citizens and all registered households within that particular district while being electronically connected, as a branch in a hierarchical network tree, to the trunk at the CPD. Communication between the CPD and these district offices is sent through high-speed leased telephone lines.

This new on-line database system has enabled the district offices to retrieve citizen records in real-time for faster and more efficient services. It is now possible for a person who wants to register a move-in to a residence in the Bangkok Metropolis area to do so without

[93] Registration Administration Bureau, *Information on the Registration Administration Bureau, Department of Local Administration (Origin, Structure, Authority, Responsibility and Important Projects) (khormun samnak boriharn karn thabian krom karn pok krong khwampenma khrongsarng amnart nathce khwamrabphidchob lae khrongkarn samkan)* (Bangkok: Department of Local Administration, 1996), 9.
[94] All satellite communication between government offices in Thailand employs the transponders of the domestic Thaicom satellite, which was launched and operated by a local telecommunication company, Shinawatra Telecommunication Group.

having to obtain an authorized move-out document from the district office at the old residence.[95] Moreover, according to the PIN II plan, the new ID card is to be issued on the spot at district offices instead of being issued from the Registration Administration Bureau as was the case in the past. With the deployment of several advanced ICTs coupled with the on-line database, each properly equipped district office is expected to complete the card-issuance service within 15 minutes, indeed a quantum leap from the three to six months wait of the past. Among the devices which will be used to enable this speedy process are card-coding machines, digital camera, thumb print scanners, and magnetic stripe reading equipment. The speedy issuance process is expected to encourage people to be more enthusiastic in getting their new ID and in using it. It is also expected to eliminate the widespread and illegal exploitation of the temporary ID substitute commonly known in Thai as "the yellow form."[96]

In addition to wiring and equipping the district registration offices in Bangkok, plans in 1996 also included the construction of similar computer systems in eight major provinces in different parts of the country. These provinces were designated as regional centers for the envisioned nationwide civil registration information network to be completed at the end of PIN II. Therefore, their systems will serve as hubs for information traffic between the CPD and the distributed databases in smaller district registration offices in the smaller surrounding provinces.

Phase II (1998-2001), a Bt4.2 billion investment (US$168 million), will see the installation of similar computer and satellite communication systems as the above in district registration offices and local government registration offices in the remaining sixty-seven provinces. This will cover a total of 869 district and sub-district registration offices and 136 local government (municipality) registration offices. By the end of the second phase, all these registration offices are expected to be connected under the network envisioned in Figure 4.4 and to be able to issue on the spot the new personal identity cards and the new household registration passbook. In other words, by the end of the project in 2001, a total of 1,045

---

[95] According to article 30 of the Civil Registration Act B.E. 2534 (1991), a person is required to report to the district registrar after having moved into a new residence within fifteen days after the move. He or she is also required to supply an official move-out document signed by the district registrar or deputy of the old residence.
[96] Normally, district offices will issue to expectants of a new ID or a replaced ID (in case of loss) a temporary ID substitute which is a piece of yellow paper containing the expected bearer's name, signature, address and identification numbers. The "yellow form," as it is commonly known, does not have a photo attached therein, however. Since the process of issuing a personal ID is usually very lengthy, particularly for residents in rural provinces, it is legally allowed to use the "yellow form" as a substitute for the actual ID in certain official transactions which require ID. The "yellow form" is even allowed at elections. Since there is no way of verifying against a person carrying a yellow form, many people have gotten around to exploit this loophole. Selling their "yellow forms" for money is one of the common forms of abuses.

registration offices nationwide will be interconnected in a hierarchical network structure with the CPD at the central core.

Although PIN II has only begun operation for a little more than two years, its impact can already be felt, most noticeably in the newly-introduced magnetic ID card. The new card is distinct from the 1988-ID card in two aspects -- the material used and the addition of the information-containing magnetic stripe.[97] The old card was made of paper and was laminated with special security-proof seal. The new card resembles a credit card as it is made of plastic and contains a magnetic stripe on the back. An example of the new card and corresponding translation is provided in Figure 4.5 and 4.6. Like the old card, the new card shows its bearer's photo and name, birthdate, address, issuance date and expiry date. The magnetic stripe contains the following information in machine-readable form: name, birthdate, and corresponding number of the cardholder's record as listed in the facial and fingerprint file in the CPD. With magnetic stripes, it is no longer necessary to transcribe information manually. When run through a proper card reader machine, the above information will be revealed and can be verified accordingly. The cost for this new card is estimated at Bt25 each (about US$1). This card expires after six years.

National Identity Card ATM -- Encoding a Market -Instrumental Rationale in Surveillance

Since it was launched, the new magnetic ID card has attracted much attention from the urban public to whom the card was first issued. The card's appeal is likely to lie in its trendy design as well as the functional value which it embodies. According to a senior official at the Department of Local Administration, the selection of the card design, with magnetic stripe that makes it capable of storing and transferring data, was intended specifically for data-sharing purposes. Other public and private organizations may share in the use of the card in rendering their services. This official cites the following organizational areas as plausible purposes that the card may be used for, aside from civil registration purposes -- tax, conscription, education, land transportation, policing, health, and finance. In the conversation I had with this official in late 1996, he also mentioned the possibility of the ID card being used as an ATM card to withdraw money from automatic teller machines at

---

[97] The nine provinces which will begin issuing this new ID include Bangkok, Nakhon Pathom, Chon Buri, Chiang Mai, Phitsanoloke, Nakhon Ratchasima, Udon Thani, Surat Thani, and Songkhla.

banks.[98] At the time. I did not think such a scheme was really possible and dismissed it as some sort of a technocratic daydream.

Unfortunately, I was later proven wrong. In October 1997, this "technocratic daydream" came true as the Siam Commercial Bank (SCB), a major local bank, joined with the Department of Local Administration to combine ATM banking services with national identity cards. Under this collaborative scheme, called the "National Identity Card ATM," SCB customers can sign up to have their identity cards serve as ATM cards as well. Typical ATM services such as depositing and withdrawing funds, and paying for utility services, can be conducted through the ATM/ID card. The service carries an annual service fee of Bt100, and interested customers can request personal identification numbers from any Siam Commercial Bank branch nationwide.[99] See an advertisement of this new service in a local magazine in Figure 4.7.

On a functional level, this new development may represent a collaborative effort between the public and private sectors to utilize ICTs in maximizing customer convenience. On a more ideological level, however, the ATM/ID card encodes a market-instrumental rationality in its true form. Through this new means of bureaucratic surveillance -- the magnetic-strip ID card, all aspects of Weberian modern "means-end rationality" -- scientific and instrumental calculation, rational capitalist enterprise, and rational bureaucratic state are fulfilled. By adopting the card and the idea of "convenience" that it embodies, the targeted citizens are simultaneously being inscribed with the penetrative power of both the state and the consumer market. This significant interaction between public and private sector surveillance, made possible by the new card innovation, demonstrates that the state-economy divide in Thailand is not so wide.

---

[98] Mr. Bhairoj Brohmsarn, deputy director-general of the Department of Local Administration, Ministry of Interior, interview by author. 12 November 1996, Bangkok, Department of Local Administration, Ministry of Interior, Bangkok.

[99] Editorial staff, "New Identity Cards Offers ATM Service Exclusive to Siam Commercial Bank." *The Bangkok Post.* 29 October 1997, B 2.

Figure 4.4: Centralization and Decentralization in the Population Information Network II (PIN II)
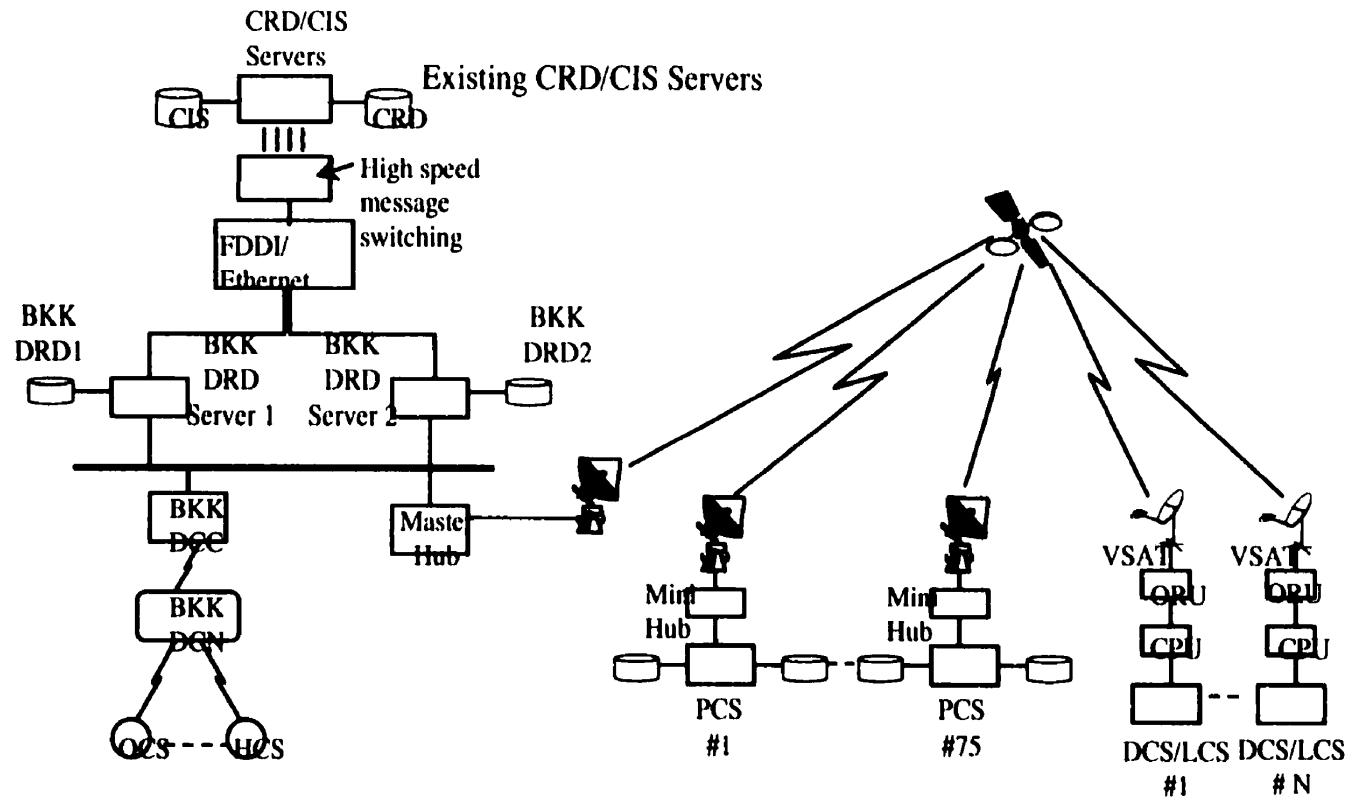
DRD – District Registration Data Base
CRD – Central Population Data Base
CIS   – Central Information System
LCS – Local Government Computer System
PCS – Provincial Computer System
DCS – District Computer System

DCC – Data Communication Controller
DCN – Data Communication Network
ORU – Outdoor RF Unit
VSAT – Very Small Aperture Terminal

Figure 4.5a: the 1996 personal identiity card (front)
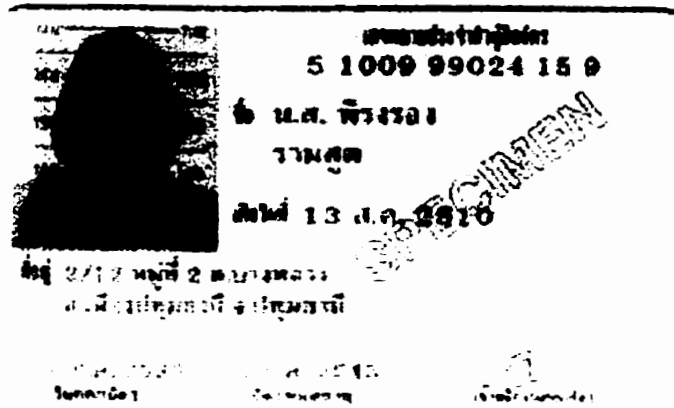
Figure 4.5b: the 1996 personal identiity card (back)

Figure 4.6a: Translation of 1996 National Identification Card (front)

Cardholder's identification number
....
Photo

First Name....................

Last name......................

Date of birth......................

Address...

....

.... (signature)
Issuance date   Expiry date   Issuance Officer

Figure 4.6b: Translation of 1996 National Identification Card (back)

magnetic strip

Personal identification Card

Department of
Local Administration

garuda emblem

Ministry of Interior

Figure 4.7

An advertisement for the national ID card/ATM service in a local magazine

Clad in modern attire and standing before a height scale (as they would for a national ID photo), the four presenters in the ad are showing off the new national ID card with a smile. The ad says: "new look in service from Siam Commercial Bank: a national ID card/ATM. Add value to your ID card by making it an ATM card too." The bottom of the ad shows logos of the bank and the Department of Local Adminitration, Ministry of Interior, side by side.

156

It should be noted that the new magnetic-strip ID card is intended to pave the way for a next-generation ID card, which is based on a smart card concept. The smart card, which is planned to be introduced in Thailand in the next five years, will have an embedded microchip and will be able to store a great deal more information than the magnetic-strip ID card. While a magnetic strip card can be used for many purposes, it can only store up to 240 characters. Smart cards, on the other hand, can hold at least eight kilobytes, or 8,000 characters. According to a senior official at the Registration Administration Bureau who is also a strong advocate of smart ID cards, the registration processing center, a division within the bureau, is developing the new smart ID card based on Java computer language.[100] It expects to integrate all necessary cards with the ID. In his words,

> "We hope that in the future, Thai people will have only one card. As well as being their ID, they will be able to use it for various financial and social services, from any organization."[101]

The basic applications embedded on the card will be concerned with government agencies, electronic commerce, and banking. Among the government agencies that will use the information on the card, apart from the Department of Local Administration, are the Revenue Department, the Social Insurance Office, the Ministry of Public Health, and the Ministry of Defence. The Department of Local Administration, which will be the central agency in managing this next generation ID card, will open to both electronic purse service providers and banks to register to provide services through the cards. According to this same senior official, the department will deploy "a first come, first served" strategy in registering those services.[102]

As mentioned, NECTEC has also been involved in the development of the new smart card through their R&D and technical standard efforts. Apart from forming the Thailand Smartcard Working Group in 1998 to develop recommendations for these standards, NECTEC also held in December of the same year its first public hearing to gain public feedback on its efforts to set up smart card standards for Thailand. According to the NECTEC director, the public hearings are intended to "allow the private and public sectors to get involved by putting forward their opinions and recommendations, in order to help establish a smart card standard that is acceptable to all parties" and "to help the smart card

---

[100] Java is a computer language for distributed applications created by Sun Microsystems Corp. in 1995. It allows users to add multimedia content and the code necessary to interact with that content. It is platform independent; it can run on several application programs including Windows' 95, Windows NT, Mac OS, etc.
[101] Mr. Surachai Srisaracam, director of the registration processing center, the Registration Adminstration Bureau, as quoted in Pongpen Sutharoj, "New ID cards likely to boast hi-tech features," *The Nation*, 8 December 1998, F. 4.
[102] Suchalee Pongprasert, "Multi-function chip ID cards in five years," *The Nation*, 20 April 1999, F 11.

working group in the design and create a suitable standard for use in Thailand."[103] Once the standard has been decided upon, NECTEC, with the cooperation from the Bank of Thailand, will go ahead with the pilot program, which is expected to cost about Bt100 million. A total of three public hearings are planned to formulate the smart card standard.

As things turned out, however, participants in the first hearing came from only government organizations and private corporations that are interested in joining in the use of smart cards. There was no representation from civic or democratic associations, nor from critical members of academia. As a result, the types of concerns voiced by these participants had to do mainly with the technical side of things -- card capacity, security technology, and utmost exploitation of the card for multi-purposes. Fear of privacy intrusion per se was not mentioned but was framed in terms of data security. To this matter, NECTEC technical experts proposed adoption of public key technology as a security standard for the smart cards. The public key technology, it is argued, is an encryption technology that can protect electronic data while allowing authorized people to access sensitive electronic information.[104]

Although the authority at the Registration Administration Bureau has said that the new smart card will not replace the existing magnetic-ID card and will only be available for those people who want to use their ID card for several purposes,[105] the fact that so many different functions will be integrated into a single card warrants concern. At this stage, the Registration Administration Bureau plans to talk with the Ministry of Foreign Affairs about integrating a passport into this next generation of ID card. Furthermore, several private organizations have already expressed interest in joining the smart card pilot project, including Siam Commercial Bank, Bank of Asia, 7-Eleven, Loxley Information Co., and Internet Thailand Co. As more and more organizations participate in this emerging surveillance scheme, a significant number of Thai people will find that several aspects of their lives, as citizens as well as consumers, will become growingly contingent upon possession of the new card. As a result, they will be compelled to adopt the card and to accept the types of control -- through the networks of data collection and supervision of behavior -- that the card embodies should the card arise in the future.

---

[103] Thaweesak Koanantakool, NECTEC director, as quoted in Jirapan Boonnoon, "NECTEC plans public hearings on smart card standard," *The Nation*, 10 November 1998, F 3.
[104] Ibid.
[105] According to this plan, the magnetic card will be the basic ID card, while smart ID cards will be available to those who make special requests at their district office. Mr. Surachai Srisaracam, director of the registration processing center, Registration Administration Bureau, as quoted in Pongpen Sutharoj, "New ID Cards," F 4.

On a more ideological plane, however, the new microchip card may also emerge as a new social stratifier for a primarily dualistic society like Thailand. Its functional values aside, the card also mobilizes an ideological semblance of "modernity." For the Thai context, the idea of "modernity" usually denotes a general category of desirable values, techniques, and socio-economic conditions -- rationalization, market capitalism, industrialization, and urbanization -- that are characteristic of the West or the westernized segment of the local populace. But in an age of high informatization like the present, "modernity" also has much to do with ICTs and practices that are related to promoting the existence of a local "information society." Evidently, the new smart card will in practice be more useful to the more urbanized and modernized segments of the population, who have greater need or desire to participate in a greater range of transactions and services that the card renders possible. Meanwhile, the less urbanized and modernized segments, who generally belong to the lower socio-economic strata, will have less need for it and will possibly settle with the magnetic-ID card that would be sufficient for more basic types of transactions. In this scenario, the smart card may become a status marker, dividing the population into "the more modern/informatized" and the "less modern/informatized."

RESISTANCE FROM THE EMERGING CIVIL SOCIETY

While other civil movements to protect the rights of individuals from state tutelage are on the rise, little attention and awareness exist in the sphere of personal privacy. At the time of writing (early 1999), there is no established action group in Thailand that specializes in promoting personal privacy. Interest in the issue does exist, however, in scattered circles of academia, NGO, mass media, and legislators. At least two prominent law professors at Chulalongkorn University expressed concerns to me about the Ministry of Interior's manipulation and exploitation of citizen data, which has gone unnoticed by the public. One of them, Dr. Borvornsak Uwanno, who is also the current dean of the Faculty of Law at the university, encouraged me to complete my dissertation as soon as possible so that "we could use your case studies as hard evidence to show how people's rights have been encroached upon and to raise public awareness."[106] Similarly, Dr. Sutham Yoonaitham, who has served as legal expert on NECTEC's IT-law subcommittee and is presently involved in the drafting of the Electronic Data Interchange law, also raised the point about the need to boost public awareness of the issue. He was also very critical of the Ministry of Interior's bureaucratic

---

[106] Dr. Borvornsak Uwanno, Dean of Faculty of Law, Chulalongkorn University, Thailand, interview by author, 11 October 1998, Vancouver, Plazcek Residence, Vancouver.

impulses to gather more information on citizens now that computerized storage and processing is available. In his words,

> So long as they (Ministry of Interior) gather and use data for administrative purposes -- the kind of data they actually use in their civil registration operation like name, marital status, birthdate. I have no problem with it at all. But if they want to add something like revenue, criminal records, credit history, and tax records to their files. I think it is way too much and there is clear bias in their motivation. In those cases, I think we really need to draw a line somewhere.[107]

While the two law professors are very clear about setting limits to the state's bureaucratic surveillance, particularly in the present electronic mode, other groups were less certain and seemed to be distracted by the promise of increased efficiency that the new mode of surveillance can render. For instance, when the Ministry of Interior unveiled the plan to launch the new ID card in 1996, a handful of representatives of local human rights groups did express concern about intrusion of privacy but also said they believe the benefits of improved services will outweigh the privacy costs.[108] It merits mentioning that most Thais are fed up with the inefficiency of the government bureaucracy, particularly with regard to public services that directly affect their daily lives like civil registration. Since the application of ICTs in the Ministry of Interior's project is rationalized on grounds of efficiency, it is understandable that it would be welcomed by the general public who are not very perceptive of the intangible implication of privacy loss. Even for those with a human rights orientation, "privacy" may still seem like a far-fetched consequence when compared with the more immediate promise of increased efficiency.

According to a member of a local NGO, "privacy" may be a desirable thing. But Thais have lived under authoritarian control for such a long time that people just learn to get by with less of it. To demonstrate her point, this NGO member pointed out how most, if not all, phone lines at major NGO offices are tapped. Although this is common knowledge among NGO staff, they did not feel they have sufficient cause to protest it. This is because, she said, it would be extremely difficult to Graham, Peter. since the organization responsible for the technical side of the wiretapping -- the Telephone Organization of Thailand (TOT) -- is a part of the government bureaucratic network. Similarly, it would be equally difficult to politicize the issue since the state would most likely rationalize it on the arbitrary grounds of

---

[107] Dr. Sutham Yoonaitham. assistant professor of law. Chulalongkorn University, Bangkok, interview by author, 3 September 1996. Faculty of Law, Chulaongkorn University, Bangkok.

[108] Phochana Hayeesalah and Thaneeya Peerapong. "Computerized ID Cards: Critics Fret Over Loss of Privacy and Human Rights Issues." *The Nation*, 13 February 1996, C 2.

national security. To "make do" under this surveillance, members of NGOs that are more prone to state interference -- those specializing in the promotion of democratic rights and environmental protection -- reportedly refrain from conversation that could be construed as "threats to national security" on the phone.[109]

From another angle, a local journalist views that an average Thai does not see privacy as an issue when it comes to civil registration and national identity card. To him, it is rather the citizenship dimension that these documents represent that really matter to them. In his words,

> Most Thais believe that identity card and household registration document open the door to citizen rights. Very few would think or care about privacy. And fewer, I believe, would regard these registrations systems as tools for state control.[110]

This journalist also recounted the experience in the late 1980s when he learned about a foreign news agency's report that the Thai Ministry of Interior's computerized system and its data collection method were a serious threat to personal privacy. He said his beat at the newspaper picked up the story and tried some follow-up, but to no avail, because "the issue just didn't ring the bell with the public."[111]

In this light, the practice of burning (or threatening to burn) identity cards in protests against the state confirms the journalist's above assumption that Thais regard the civil registration and national identification system as their "link" with the state rather than as a form of control. Burning identity cards thus symbolizes severing that link. However, incidents of card-burning or threats to do so have become more rare in recent years since protesters usually resorted to other measures that create "bigger noises" to attract attention.[112] The growing rarity of the practice may be due in part to the increasing indispensability of the two documents. In a recent incident of confrontation between farmers and the government in Nakhon Ratchasima province, villagers returned their identity cards to the authority because there was no electricity in their community. This was done in a relatively peaceful manner but it did spur the government into action after.

---

[109] Valakkamol Iamwiwatkit, interview by author, 21 August 1996, Bangkok, Chulalongkorn University, Bangkok.

[110] Tulsathit Tabtim, editor of the political desk, The Nation newspaper, correspondence with author via electronic mail, 13 July 1999.

[111] Ibid.

[112] For instance, they block highways, or march to Bangkok, or have some volunteers slash their arms.

Despite the usual fears about computers and their adverse impacts on privacy, the widespread application of ICTs in record-keeping may help sensitize public awareness about privacy in some social groups in Thailand. There are signs that such a trend may be emerging. In a parliamentary scrutiny of the Budget Bill in 1996, the House committee cited privacy concerns as a ground to oppose a Bt5.7 billion proposal by the Ministry of Interior for installment of provincial computer networks in the PIN II project. A Democrat MP, who chairs the subcommittee scrutinizing the computer budget, questioned the security of data in an on-line computer system and raised questions about possible violations of personal privacy.[113] Since the Registration Administration Bureau, which was responsible for the budget proposal, failed to clearly explain how their security system would prevent illegal access to information, the proposal was rejected.

CONCLUSION

The withering "dialectic of control"

Although the Department of Local Administration, the Ministry of Interior's most powerful bureaucratized base, has by this time expanded its administrative coverage over all provinces, districts, and villages nationwide, there are still limitations that shortens the radii of effective administration from the center. These include the rudimentary systems of transportation and communication in remote provinces and the demographic and cultural considerations of certain segments of the population that are dispersed into small and relatively self-sufficient communities, for instance, the hill tribes in the North, and the Malay-Muslims in the southern border provinces. On top of these technical problems, there are also remnants of the traditional patronage system that may occasionally provide some autonomy from penetrative administrative control. All these limitations, individually or combined, constitute degrees of a "dialectic of control" that subordinate populations can draw upon to develop their own countervailing power.

---

[113] Boonmark Sirivanakul, Democrat MP, as quoted in editorial staff, "Committee rejects database access plan," *The Nation*, 13 July 1996, F 4.

However. with the sweeping and unquestioned popularity of the "information society" that gave rise to many large-scale informatization programs including the PIN. the autonomy and spontaneity of individuals' behavior that were possible in a less-informatized social world may be withering. The widespread application of computers in bureaucratic organizations have considerably improved state surveillance capacities in all outlined dimensions -- size of files, centralization of files, speed of information flow, the number of points of contact between the system and subject population, and extended purposes of information use, thereby extending and deepening the network of state control into people's lives.

Take the case of the national identity card, for instance. Prior to the addition of the magnetic stripes which make possible data storage and data transfer capacities, the Thai national ID cards merely served as unique personal identifiers (UPI). A UPI is a link between its holder and the issuing organization that helps identify or locate the information/authority/responsibility/rights of the holder in terms of the holder's relationship with the particular organization. However, with the magnetic stripes, the cards have been transformed into standard universal identifiers (SUI). Unlike UPIs. SUIs have the prime objective of linking together separate collections of information relating to the holder, or alternatively, of having to access each separate file of information.[114] Put simply, one set of identification numbers can be used to access multiple files on the holder. Because of this ability, the networks of surveillance by different organizations will become more established and sophisticated.

It is also important to remember that by this time civil registration and personal identification systems have become firmly institutionalized in Thai society. After more than half a century of implementation, these schemes of bureaucratic surveillance are part of the Thai way of life and are inextricably intertwined with *all* types of public services, many of which engender citizenship rights. The mandatory nature of the card combined with its SUI character will make it extremely difficult for individuals to evade its use and the control that it embodies.

As the adoption of the card becomes more widespread in society both by individuals and organizations, even the age-old patronage system may no longer be a viable axis around which subordinate populations could seek to reclaim control over their lives. On the one

---

[114] See more about SUI and UPI in Peter Graham. "The Australia Card: a Burden rather than a Relief?," *The Australian Quarterly* 58 (1993): 4-14.

hand, patronage systems may provide a terrain in which personalized ties help free up some space from state surveillance, thereby undermining that domination. On the other hand, they can also constitute a means of surveillance through which technology, bureaucracy and patronage relations work together to consolidate a structure of domination by the state and elites over subordinate populations. Unfortunately, the contemporary trend has been tilting towards the latter scenario rather than the former. Unlike the case of the traditional past where clients (the *phrai*) were mobilized as strategic resources in the patrons' (*mun nai*) competition for power in society through the exercise of personalized supervision and surveillance, the recent explosive growth of industrialization and capitalism in Thailand have created new integrative and distributional effects, which have considerably marginalized the social significance of subordinate populations and their capacities as clients in the present patronage system. In the contemporary realm of bureaucratic surveillance by the state, the poor and powerless are by far the most unfortunate. Segments of this underprivileged population have been reduced to mere numbers of votes in the widespread vote-canvassing schemes, or to figures of "digital electorates" to be exploited by the new patronage factions in society -- bureaucratic officials and business politicians.

Besides, as inter-organizational linkages between both public and private databases expanded further with the advent of the GiNet and the smart ID card, the expanding "net" of bureaucratic surveillance will likely affect the relationship between state officials and subject population. As this relationship becomes increasingly mediated by the use of such technological innovation, not only will the space of individual citizens' invisibility and autonomy decrease, the salience of personalized ties and clientship that have shaped a social relation between bureaucratic officials and people in the past will likely subside as the bureaucracy becomes more and more reliant on this highly rationalized and impersonal mode of administration.

Beyond a compliant population -- state surveillance in the "information age"

The application of new ICTs in surveillance by the Registration Administration Bureau are as much expressions of technical rationality as they are instruments of power. These expressions can be analyzed at two broad levels -- instrumental and ideological.

On an instrumental level, it is apparent that the bureaucrats who are involved in the development of the PIN are fascinated by the potential of ICTs. They initiated the

164

development of the PIN under a standard assumption that more technology and more data will solve problems. But as the case study on the PIN shows, while the deployment of ICTs may help improve efficiency in rendering public services -- the receiving and more positive end of surveillance, it is not going to eliminate other major organizational problems that plague the Thai bureaucracy -- corruption, abuses of bureaucratic authority, and lack of bureaucratic accountability.

Worse yet, the increased knowledge that results from the exercise of this high-tech form of surveillance can serve the interests of corrupt politicians and bureaucrats who collude to buy or solicit votes during elections. Moreover, the database can even compound problems of social fairness as evidenced in the extreme case of "digital individuals" from poor neighborhood being exploited for illicit political gains. In such cases, the Ministry of Interior's legitimation of the PIN as facilitating democratization turns out to be delusionary at best.

In the present period where the urgency of the "security state" declined and the salience of private capital superseded the "bureaucratic polity," the purposes to which state surveillance is put have also changed significantly. As a form of technical rationality, a major system of state surveillance like the PIN not only serves as a means to advance administrative control by the state but also functions to promote the structuration of capital. This is evidenced in the following instances: 1) the indiscriminate access to the CPD by employees of banks and financial institutions, a sector which represents the bloodline of the capitalist economy; 2) the commodification of the now automated civil registration data as a result of growing demands from corporations wishing to compile a direct marketing consumer listing; and 3) the linking of public and private sector surveillance through the new ID card with magnetic stripe such as in the National Identity Card/ATM project.

By bridging surveillance in the state administrative realm and consumer market realm, the Thai state has evidently gone beyond its conventional objective in administering surveillance, that is, to create a compliant subject population for a security state. Through the National Identity Card/ATM project, the modern Thai state has not only provided a crucial service to the private economy but has also normalized citizens' behavior in a direction that is conducive to capitalist growth. Therefore, it can be said that on an ideological level, Thai people are being disciplined to become simultaneously "good" citizens and consumers through this new mode of state/corporate surveillance.

165

Meanwhile, it can also be seen that these aspiring civil servants who play a central role in the new hi-tech surveillance of the populace do not plan the database necessarily to serve egotistical self-interest or to serve the interests of the capitalist or the ruling class. They are simply and genuinely endeavoring for the general interest in the context of what they believe are technological imperatives of industrialism. Like many technocratic elites who have sought to influence the country's development policies, these bureaucrats have bought into the forceful rhetoric of the "information society" thesis or what I consider "the modernization paradigm with an information turn." Encouraging this impetus, of course, is the idea that the use of ICTs will augment their prestige and power, will enable them to use the latest hardware and software programs, and will lead their organizations and the entire society on a path to modernity. The common enthusiasm shared by technocrats at NECTEC and bureaucrats at Ministry of Interior to develop smart cards as the ID card for the next generation is a good testament to this ideological predisposition.

CHAPTER 5

CONTEMPORARY STATE SURVEILLANCE SYSTEM IN THAILAND:
A CASE STUDY OF
THE COMPUTERIZED CRIMINAL RECORDS DATABASE

This chapter deals with the computerization of the Police Department's criminal records database and its social implications. After a brief historical context, the case study discusses the development and major characteristics of the new computerized database project, focusing in particular on the Automated Fingerprints Identification System (AFIS), which has become exploited as a major employment screening tool in both public and private sectors. Aspects such as data quality, file inclusion, and data use are analyzed and brought to bear as impacts on the lives of people whose records are maintained in the criminal record files.

HISTORICAL CONTEXT AND MOTIVES FOR COMPUTERIZATION

In a continued practice of criminal record-keeping and background checking, the criminal records division, by the mid-1980s, found itself inundated with incoming fingerprints and criminal records with which its manual system could no longer cope. Besides standard arrest records, which were sent in by police stations nationwide, the number of records submitted for background checks for non-criminal justice purposes also grew considerably, particularly during the economic boom of the late 1980s and early 1990s. A significant portion of the latter type of records were submitted by budding private businesses that wished to screen out unwanted ex-convicts from their production lines and company premises. In 1991, a total of 140 private enterprises submitted requests and fingerprint sets of their prospective employees for record checks at the criminal records division.[1] During the peak hiring season in the same year, the usual daily statistics of 1,500 records received by the division was pushed up to 5,000 because of the influx of employment screening records. It merits emphasis that the rise in background-checking requests from the private sector was a relatively new phenomenon. Prior to the economic boom, requests for criminal record checks came mostly from government agencies and state enterprises.

---

[1]Banks, financial institutions, security companies, manufacturing companies, and department stores were among the major types of enterprises that requested record checks of their prospective employees.

167

In the big picture, the criminal records division's operation was in a state of disarray.

It experienced major backlogs and rising inaccuracy in both the initial coding of fingerprints

and record checking processes.[2] The manual method has also made the operation prone to

fraud. [3] Moreover, while the size of the fingerprint and criminal record files increased, the

ability of police officials to tap into those files for criminal investigation purposes did not.

Before 1994 when the new computerized fingerprint identification system began operation, the

Forensic division of the Police Department was unable to match a "cold print" found at the

scene of a crime with those in the criminal records files. The lengthy manual search procedure

was a major obstacle for such use of the files.

It was in this context that the projects to computerize criminal records -- history files

and fingerprint files -- were conceived. Like the advocates of the PIN project, proponents of

these projects also emphasized the need to increase efficiency -- by maximizing accuracy and

speed in the operation -- as the major reason, with crime control being the ultimate objective.

Interestingly, the need to accommodate employment screening was also cited as an impetus in

launching the automated records project. Part of the rationale in 1991 for a proposal for a

feasibility study of the new Automated Fingerprint Identification System (AFIS) project reads:

> It is believed that the incoming requests for criminal record (fingerprints) checks
> will continue to rise well into the future. This is because at present many
> private companies have become very interested in getting their employees'
> record checked at the criminal records division. Besides, most agencies in the
> criminal justice system need to verify the identity of repeat offenders by using
> their fingerprints, for prosecution purposes. If the existing problems of the
> criminal records system are not attended to immediately, we will reach a state of
> crisis in less than five years...[4]

This proposal for a feasibility study was reviewed by representatives from the criminal

justice system and other sectors, both public and private. In the absence of participation from

---

[2]An official at the division recounted to me some anecdotal evidence about the extent of inaccuracy experienced
in the manual coding of fingerprints. There was a felon who had been arrested on 13 occasions on charges of
prostitution and thefts. After each arrest, he was fingerprinted and the fingerprints were forwarded to the criminal
records division for background checks. Luckily, for this felon, each set of his fingerprints was coded
differently for all the 13 arrests. As a result, he was able to evade harsher sentences and was treated as a first
time offender in every trial.

[3] Generally, officials responsible for record checks were low-ranking clerical officials whose salary scale was
quite low. While receiving bribes from outsiders may not have been a common practice, it was cited in a
proposal for a feasibility study of an automated criminal record system as one of the major problems of the
manual system. Criminal Records Division, *Proposal for a Feasibility study of the Automatic Fingerprints
Identification System Project* (*Karn suksa khwam pen paidai khong krongkarn pramuan phon lai new meu doi
attanomat*) (Bangkok: Department of Police, 1991), 12.

[4]Ibid., 3.

the local civil liberties circle, the project was unanimously approved in principle as all the reviewers appeared to have confidence in its promised potential for crime control. As a result, issues or questions about the social implications of the new automated system were sidestepped in the grand pursuit of efficiency.

THE CRIMINAL DATABASE OPERATING SYSTEM (CDOS)

The introduction of computers to criminal record-keeping began in 1989, and slowly the information filed away on forms and kept in cabinet files was becoming automated. However, systematic changes were not made until the early 1990s after the Criminals Database Operating System (CDOS) was formally conceived and implemented. During the site-visit in 1996, the CDOS consisted of six main data files: criminal records files, crime re-enactment files, arrest warrants files; personal history and marks files, stolen wealth files, and stolen vehicles files. The six files are interrelated under a DBMS that allows retrieval of data from more than thirty terminals in a Local Area Network (LAN) system. The retrieval of any criminal data can be done directly through a terminal search by using names of convicted criminals, marks and physical characteristics, and methods of committing a crime. Meanwhile, police and criminal justice officials outside Bangkok can also radio in and make inquiries with staff at the criminal records division. CDOS is linked to the more extensive Automated Fingerprints Identification System (AFIS) through a barcode number for any corresponding criminal record. Although no on-line linkage is presently operational with any other divisions in the Police Department, an electronic connection is being completed to connect the CDOS files with the police information center that will act as the gatekeeper for all police records in the future.

The data contained in the CDOS derives from individual fingerprint/arrest cards, which arrive at the criminal records division from police stations nationwide. Whenever there is an arrest and a suspect is fingerprinted, even for minor crimes, the fingerprint/arrest record will be sent to the criminal records division for updating of its two criminal databases -- the CDOS and AFIS. As a result, the information contained in both computerized criminal databases include data of non-convicted persons, as well as those with pending charges.[5] This information is

---

[5]According to an official at the criminal records division, data of non-convicted persons will be specially marked so that it will not affect future legal decisions on the persons. The keeping of records of non-convicted persons is said to be necessary for investigative reasons. Lieutenant Colonel Kriengdej Chantaravongse, deputy director of the Automatic Fingerprint Identification System center, interview by author, 17 July 1996, Bangkok, criminal records division, the Police Department, Bangkok.

entered into the computer on a daily basis. At present, there are about three million personal records in the CDOS and the AFIS. This marked a sharp drop from the fourteen million figure prior to the beginning of the automated systems.[6]

The personal information below appears on the fingerprint/arrest cards and is the main input for the criminal record and personal history files:

-- personal identification numbers;

-- other types of ID numbers (civil servant, state enterprises, others), and affiliation;

-- resident alien ID numbers;

-- passport numbers, country of origin;

-- gender;

-- first name and last name;

-- date of birth;

-- ethnicity; nationality;

-- height; weight; build; skin color;

-- marks, deformity and tattoo;

-- visible personality;

-- area of origin;

-- profession;

-- place of work;

-- name of father; name of mother;

-- name of spouse.

Aside from the above information, a photo of an arrested suspect is also taken when there is a camera available at an arrest site. The photo files are stored in a different filing system and located in a different place from the criminal history files. The photo filing cabinets are labeled in accordance with the types of crime the suspect is charged with.

---

[6]The drop was owing to two important factors. First, non-criminal records, which used to be stored in paper files, and outdated records were not included in the computerization plan. The elimination of these records is to save computer storage space and to maximize the cost-effectiveness of project investment. Second, in 1995 in honor of the passing away of the King's mother, a special amnesty and early parole were granted to tens of thousands of prisoners, together with a special deletion of criminal history for prisoners whose records dated ten years before 1995. The inspiration for this deletion of criminal history came from authorities at the Police Department.

THE AUTOMATED FINGERPRINTS IDENTIFICATION SYSTEM (AFIS)

Along with the introduction of CDOS. the Police Department also initiated a feasibility study of the so-called Automated Fingerprint Identification System (AFIS). In 1990, the Department received a grant from the Japan International Cooperation Agency (JICA) to fund a project entitled "Grant Aid and Technical Assistance Project for the Improvement of Police Crime Laboratories in Thailand."[7] The first item approved by JICA was an assemblage of equipment for a pilot AFIS, with an estimated cost of Bt110 million (US$4.4 million). The proposed pilot system was expected to eliminate problems associated with manual record-keeping operations and to improve the ability to verify fingerprints, particularly in terms of accuracy and speed. From 1990 to 1991, the bidding for the pilot AFIS was open. NEC, a major Japanese electronics concern, won the bid to design and install the project. In the meantime. a few Thai police officials were sent to be trained at the National Police Agency in Tokyo. The pilot AFIS was set up at the forensic division in the beginning of 1991.

After one year of running the pilot project, the criminal records division proposed the actual AFIS project, with an estimated required investment of Bt448 million (US$17.92 million). for Cabinet approval. The project was approved in 1993 and the bidding was opened to interested companies later in the same year. Control Data Group (CDG), the same company that designed and operated the Ministry of Interior's PIN project, won the bidding. The installation of AFIS and the duplication of information from fingerprint cards into the system's mainframe computer commenced in 1995. The data conversion process, which involved about 2.5 million fingerprint cards, took more than a year to complete, during which time the automated system was running in parallel with the manual system. The AFIS began full operation in May of 1996. It is at present fully automated and hosts close to three million criminal fingerprint records.

---

[7]The Police Department's proposal for the grant was submitted to JICA in 1988. In 1989, the manager of a Japanese company, Mitsui Co. Ltd, in Laos was kidnapped and held for ransom at a hideout place along the Thai-Laotian border. The Thai police were able to rescue the Japanese businessman and bring him to a safe return. Following the incident, the Japanese government publicly complimented the Thai police for their successful rescue effort and in the subsequent year JICA agreed to extend the grant aid as requested by the Thai Police Department. Lieutenant Colonel Kriengdej Chantaravongse, deputy director of the Automatic Fingerprint Identification System center, interview by author, 17 July 1996, Bangkok, criminal records division, the Police Department, Bangkok.

Technically, the AFIS essentially features a combination of computer technology with the science of fingerprints identification. Its operation involves several stages (see Figure 5.1.). First, fingerprint cards submitted to the criminal records division by police stations nationwide and by organizations requesting record checks are sorted out into categories -- arrests, employment and licensing -- and stamped accordingly. On average, the division receives daily about 3,000 fingerprint cards, all categories combined.[8] Following the sorting, the fingerprint images on these cards are scanned into the computer and each record encoded with sets of computer-generated numbers that are entirely different from the numbers on the fingerprint cards. These new identification numbers, which will remain with the scanned records until the end of the processing procedure, are intended to prevent fraud resulting from collusion between workers in different sections of the system. During the scanning, the fingerprint images are edited to improve image quality for machine reading.[9] Then, the scanned and edited records are automatically forwarded for the matching process downstream.

In the matching section, the specially-designed software of the AFIS system will read and classify the fingerprints into classes -- arch, loop, whorl, and composite. The software will also mark the center point of the minutiae and other clusters of points on the minutiae which exhibit an identifiable pattern. The relationship between these points on the minutiae will be automatically computed into numerical values that will be used to search and match against pre-existing criminal fingerprint records in the AFIS database. Utilizing an automated pattern-recognition design, the computer will generate a number of candidates of fingerprints that have minutiae patterns similar to the queried record. Each candidate will be given a matching score indicating the degree of probability that the candidate record and the queried record are identical. In the end, it is up to the officials in the next section -- verification -- to determine whether the queried record matches with any of the candidate records generated by the computer.

---

[8]These figures are based on the actual statistics during my site visit to the criminal records division in June and July of 1996. According to an official at the criminal records division, most of the incoming fingerprint records are arrest records. Those in the other categories account for only a small portion.
[9]The editing is said to be necessary because sometimes the quality of the fingerprints from police stations, particular those in the remote provinces, are very poor. The editing process could help improve the images of the minutiae which are essential for the computerized search and matching.

Figure 5.1: Flow of operational stages in the Automatic Fingerprint Identification

2. Scanning, editing,encoding

Fingerprint images
scanned into computer
and edited for quality.
New ID numbers
generated and encoded
for each image record.

1. Sorting

Fingerprint cards are
sorted into categories
and stamped
accordingly.

3. Matching

AFIS software matches
queried record with
candidate records from
AFIS database.

5. Reporting result & decoding

4. Verifying match

Officials verify the
match by comparing
minutiae of queried
record to computer-
drawn candidate records
and determine a match or
a non-match.

173

The officials in the verification section will compare the minutiae patterns of each set of candidate fingerprints next to those of the queried fingerprints. and make the final decision whether to rule them a "match" or a "non-match."[1] After the verification process, a report of the search will be printed out. Those with matched records in the AFIS files will be identified. Up until this point, the computer-generated numbers are still used to identify each queried fingerprint record and all that the operators know of each fingerprint record is the category to which it is assigned. Then, the search report will be forwarded to the sorting desk where the fingerprint record will be decoded and labeled according to the search result. The fingerprint cards in the employment and licensing categories will merely be stamped "record found" or "record not found" and returned to the original senders. Meanwhile, those in the arrest category with matched records will be further scrutinized. The AFIS files are linked to the Criminal Database Operating System (CDOS), which compiles records on past criminals. As soon as the queried fingerprint record is identified as a match with an existing record, the system will give a corresponding number on the CDOS files for further background check.

Another important built-in technical feature of the AFIS is its restriction of delete access. This is basically a security feature to prevent any mismanagement and abuses by terminal operators. Delete access is limited to only a few high-ranking officials in the division and can be carried out only if it is proven that the persons listed on the records are deceased. The criminal records division is legally instructed to remove the criminal record of any person when he or she reaches sixty or when the charge against the person is dropped. However, these principles are not strictly observed in the handling of AFIS data. The standard practice is to keep the information on the CDOS and AFIS files until a date one hundred years after the birthdate listed on the record. This overinclusiveness of the files is said to be necessary for investigative reasons.

Although the Police Department had anticipated a nationwide on-line connection between police stations nationwide with the AFIS office in Bangkok, nothing has materialized thus far. Police stations in the provinces are not as technologically advanced as those in Bangkok, and very few stations are equipped with a computer, let alone an

---

[1] According to the international fingerprint identification standard, any pair of "match" records should have at least 12 points of similar minutiae patterns. It is also important to note that the candidate with the highest matching score (the highest computed probability) does not necessarily get picked as a match. Based on my observation during the site visits, those records with lower matching scores were often finally picked as the match. In other words, the human factor still plays a visibly important role, particularly at the verification stage, while the computer was more important during the screening and matching stage.

electronic connection. It will take some time to upgrade their technological infrastructure and expertise before any electronic linkage can be seriously discussed. While an electronic linkage is being completed between the CDOS and the police information center which is also located on the same premises of the Police Department in Bangkok, such connection is more difficult to establish with AFIS. CDOS files are text-based and are thus retrievable by even low-end computers with a modem. AFIS files, on the other hand are image-based and require client terminals to have more processing power, speed and memory storage in order to retrieve and display the images of the fingerprints. A future plan to establish a linkage with the Ministry of Justice is also being contemplated.

Since the AFIS became fully operational at the beginning of 1996, the criminal records division's capacity for data processing is said to have been significantly improved in all aspects -- speed, storage capacity, accuracy, and fraud prevention.[11] With the new automated searching of fingerprint files, tasks which would have taken days in the past are now reduced to minutes or seconds. For instance, the matching of a "cold print" found at the crime scene with existing records which was impossible only a few years ago can now be done in a reasonable amount of time. Meanwhile, the use of optical disk to store fingerprint images enabled an expansive and relatively more secure storage, while allowing for easy record retrieval. Furthermore, since the pattern-recognition design of the AFIS software relies upon mathematical values derived from scientific technique, degrees of error are supposed to be substantially reduced when compared to the manual system.

As far as fraud and security issues are concerned, the flow of the system was also designed with certain precautions. Workers who have first-hand contact with fingerprint cards work in a separate room from those who operate the workstations. In addition to built-in technical safeguards in the computer system, every room in which an AFIS section is located is also equipped with 24-hour surveillance cameras. All doors are security doors that require magnetic key cards. Certain doors that open to the control room and disk storage room allow limited access to only high-ranking officials and technical staff from the CDG corporation.

In addition, the launching of AFIS is also said to contribute to steadily higher rates of matching fingerprint records. According to an official who oversees the AFIS, the rate of

---

[11] Lieutenant Colonel Kriengdej Chantaravongse, deputy director of the Automatic Fingerprint Identification System center, interview by author, 17 July 1996, Bangkok, criminal records division, the Police Department, Bangkok.

record matching rose from 7-10 percent during the manual phase to around 14-15 percent after the AFIS began running in parallel with the manual system in 1994.[12]   After the entire system was fully automated, the rate went up to 25-30 percent.[13]   These rates apply to all categories of fingerprint records.

Insofar as record checks for employment screening is concerned, this area of use was fast growing when the AFIS first went into operation. As mentioned earlier, it has always been a common practice among government agencies and state enterprises to require background checks for employment purposes. It does not matter if a sensitive position is involved. As for the private sector, certain segments -- banking, security, and some manufacturing concerns -- also apply the same requirement. While no statistical records were kept as to the types of company that are likely to screen their prospective employees through fingerprint record checks, the director of the criminal records division recounted a few examples -- a Thai-Japanese manufacturing plant recruiting new factory workers, a financial institution in the process of hiring new brokerage staff and clerical workers, and a security and building maintenance company screening applicants for security guard positions.[14]

This director of the criminal records division admits that he is personally against the idea of criminal records being accessible to private employers. Such provision of record checking service, he says, may help make large organizations feel more secure about their employees, but it may also carry consequences that contradict the entire purpose of criminal correction and rehabilitation. In his words,

> If an ex-convict could not land a job as a construction worker or a janitor, I really don't know what they are worthy to do but to become a thief and to go back to prison again.   It is like the entire system is not willing to give them another chance. ...   It is clear that if criminal records checking

---

[12] Lieutenant Kantha Thangsupanich, AFIS staff, interview by author, 19 July 1996, Bangkok, criminal records division, the Police Department, Bangkok.

[13] A casual look at these rates alone can be quite misleading. A consideration of contextual and situational factors is crucial here. In 1996, Thailand celebrated the 50th year coronation of King Bhumibhol's ascendance to the throne. Several activities were staged to mark the celebration of this auspicious occasion including the granting of amnesty and early paroles to prisoners nationwide. Thousands of prisoners were granted early parole in 1996. As a result of this royal amnesty, several ex-criminals returned to the street and committed crimes. The crime rates went up significantly and many of the arrested criminals were those recently released from the royal amnesty program.

[14] Police Major General Chatri Sunthonsorn, director of the criminal records division, interview by author, 23 July 1996, Bangkok, the criminal records division, the Police Department, Bangkok.

continues to be used as an employment-screening tool. the ones who benefit the most are the capitalists.[15]

Not only does he disapprove of this employment-screening approach. this official also feels that the incoming requests from the private sector unnecessarily overloaded the work of the officials who should have been focusing entirely on record checks and data updating for criminal justice purposes. Moreover, he thinks it also opens the way for corruption among officials who deal directly with criminal records, in both print and computerized forms.

From early 1996 onwards this director was trying to put a stop to record checks from the private sector by making it a general internal policy to decline such requests. Nonetheless, a number of these types of requests still found their way to the AFIS. According to this official, many private companies who were turned down on their requests the first time bypassed his order by using their influential connections with higher-ranking officials in the Police Department. He also reported cases of friendly favors done by officials within the AFIS section that were beyond his scrutiny. While the division claims that record checks for employment screening accounts for only a small portion of the total requests received, it could not give precise figures. What this means is that each year an unknown number of the labor force has unknowingly been exposed to a data surveillance process that may critically affect their lives and those of friends and families. Even in a society that does not openly value personal privacy like Thailand, such information practice still poses important legal and moral questions. These concerns will be discussed in more details in the next section.

File Inclusion, Data Quality and Data Use

In his 1986 book *The Dossier Society*. Kenneth Laudon examines the social impacts of the national criminal history system in the US. He focuses primarily on the system's civil liberties consequences for individuals. In his conclusion, Laudon visualizes circumstances in which a computerized criminal records system would be efficient, effective and broadly accountable. This, he proposes, would involve a national database, with linkage to major law enforcement agencies, containing complete and accurate criminal history records on a

---

[15] Ibid.

relatively small number of serious multistate offenders.[15]   Adding to Laudon's vision, Diana
Gordon later suggests that this file be subject to continuous public oversight, available only
for criminal justice use and for limited high-security job checks, and subject to stringent
dissemination restrictions. The national criminal history system would be supplemented by
separate state systems covering a wider range of offenders and tightly regulated as to file
content, data quality, and access to records. Both systems, she argues, would have to be
regularly audited for timeliness and accuracy. There would also have to be penalties
enforced on violations of system regulatory standards.[16]

    While the situation in Thailand is vastly different from that of the US, with its unitary
state system being the most visible distinction, the criteria set forth by Laudon and Gordon
still have relevance to evaluate the Thai criminal records system.   Apparently, the emerging
computerized criminal records system in Thailand does not remotely resemble the picture
above.   To begin with, it manifests a defect Gordon calls "overinclusiveness of files."
CDOS and AFIS files include data from arrests without dispositions. The content of the
criminal history file contains no timely account of how the case was disposed of -- by
acquittal, dismissal, or conviction. The supposedly universal criminal justice principle of
"innocent until proven guilty" appears to be reversed in the Thai case. Data which may be
about acquitted or dismissed cases are included in files that are labeled as "criminal" for
"investigative reasons" and will likely remain there for decades.[17] Not only are these
practices affecting the integrity of the data and, more importantly, people's lives, but they
also contradict the regulations of the Police Department.   According to these regulations,
criminal records are volatile data and are to be removed under the following circumstances:

1) tne record subject is deceased;
2) the record subject is over 60 years of age;
3) the plaintiff dropped the charge against the record subject;
4) the district attorney did not file charge against the record subject;
5) the judge turned down the request for a trial;
6) the judge declared an acquittal after the trial;
7) the district attorney dismissed the charge during the trial;

---

[15] Kenneth C. Laudon, *The Dossier Society: Value Choices in the Design of National Information Systems* (New York: Columbia University Press, 1986), 309-313.
[16] Diana R. Gordon, "The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System," *Politics & Society* 15 (1987): 484-485.
[17] As mentioned before, the practice at the criminal records division is to remove the record once the person in the record is 100 years old.

8) a new law is passed after the person commits the wrongdoing and overrules that wrongdoing as a non-crime: and

9) when an amnesty law is passed which grants a pardon to the convicted record subject.[18]

However, since there is no oversight mechanism to keep the criminal records division in check, these regulations are practically moot. Furthermore, the criminal records system is technically exempted from regulation in the existing freedom of government information law or other legal statutes (see more details in chapter 8) and is relatively free of national control, for that matter. The enforcement and maintenance of a regulatory standard thus depends entirely upon internal rules or policy within the Police Department.

The effects of inadequate regulation are felt not only in terms of the inclusiveness of data subjects but also in the data quality. Although there are probably fewer errors in computerized records than there were in manual files, mistakes have more impact now because they travel further and can be readily utilized for multiple purposes. It ought to be remembered that criminal records at CDOS and AFIS are only as accurate as the local law enforcement records -- arrest forms and fingerprint cards -- that constitute them in the first place. As far as CDOS is concerned, data entry officials often complained about incomplete or inaccurate data due to the lack of cooperation from the arrested person and the illegibility of the handwriting in the filed arrest forms. In the AFIS case, the police stations that filed the arrest forms and fingerprint cards are usually blamed for doing a poor job in fingerprinting.[19] Sometimes the prints are too thick or too faded which makes it extremely difficult to classify them, even after undergoing computerized editing in the AFIS.

In addition to the problems with collected data, the binary feature of computerization also compounds the problem of accuracy. The process of record matching in the AFIS may be long and complex, but in the end the final report will only indicate either "record found" or "record not found." In non-criminal justice use of the files -- employment or licensing purposes, exactly this much data will appear as the end result since there is no perceived need to cross-check further with criminal history files in CDOS. In other words, it is the search

---

[18] Department of Corrections, "History of Penal," 48.
[19] The criminal records division organizes on a regular basis a training workshop to teach police officials from police stations countrywide the technique of fingerprinting. However, fingerprinting is not really a job description in any police station. Officials who actually do the fingerprinting at each station are usually low-rank officials who will over time get promoted to a higher rank and to a different duty. As a result, officials with less experience and expertise always end up handling the fingerprinting, resulting in poor quality and sometimes even unusable prints for verification purposes.

result that will be stamped on a job applicant's record and will determine his or her job situation, or future, for that matter.

Data quality is not the only operational problem in these databases: abuse of record access and use is another. Even after the director of the criminal records division had made it an internal policy to decline private employers for record checks, the practice still continued. It seems that this policy turn is not taken very seriously by staff. This is quite understandable since the use of records for employment screening has been practised for decades, and indiscriminate access to records for this purpose has been given to both the public and private sectors in the past. As long as these law enforcement officials do not realize the importance of the privacy of information contained in criminal record files, things are unlikely to change. Employers needing an unauthorized record check can always obtain it through personal contacts with people who have access to the record, or those with commanding authority in the bureaucracy. After all, a law enforcement agency like the criminal records division is also a part of the government bureaucracy and is thus not immune to the deeply-entrenched patron-client system.

Although no systematic review has been done of how many or what kinds of people have lost or been denied jobs as a result of these record check practices, anecdotal evidence suggests that the impact is felt mainly by the lower rung of the social strata. Presumably, those who lack education qualification and those people who have had the misfortune of being arrested would not apply for jobs where fingerprints are required for record checks. Those who do apply will just have to suffer the consequences. Considering the deficiencies of data quality in criminal records files, it is grossly unfair for many of these people, particularly if they were released after arrest or acquitted at trial, to have to live with this vulnerability for the rest of their lives. Criminal record checks may assist employers in screening their labor force, but this is far from an adequate rationale. With the type of check result derived from AFIS, a person's entire background is reduced to a binary "record-found" or "record not found," which translates as "criminal" versus "non-criminal" respectively. Notwithstanding the actual and more complex reality, this digital reality containing "digital individuals" is more powerful and more trusted as an accurate measure of people's character. In such a context, the computerized system really victimizes as it operates by decontextualizing. As an unintended result of this crime prevention measure, the decontextualized use of the AFIS for employment screening may inadvertently increase the incidence of crime since a potentially large number of people may be denied employment and left to fend for themselves by whatever other means available.

In many ways, the AFIS may have become the Thailand's largest "black list" and one that is readily available with its automated system of storage, search and retrieval, and relatively unregulated access. While it may constitute a law enforcement data surveillance on an unprecedented scale, its fishing expeditions for employment screening have gone on unnoticed by the critical segment of society. Press attention about the system was largely positive, even promotional, in supporting the use of ICTs for crime control. As for the scholarly and civil libertarian community, there has been, to my knowledge, no analytic discussion about the system and its far-reaching implications, at least not until this case study.

CONCLUSION

The creation of the CDOS and AFIS reflect a shift towards what Dandeker calls a "pre-emptive pattern of policing," a rationalized mode of policing that relies primarily upon "the police's own autonomous investigative skills based on an infrastructure of administrative penetration of society and linked mechanisms for the collection, storage, and processing of criminal records and intelligence data."[20] The dominant emphasis of this mode of policing, also called "techno-policing," is therefore in the use of information to detect crime through the application of technology and through the surveillance of populations likely to commit crime. In the Thai case, however, the effects of this "techno-policing" has expanded beyond the boundary of the police forces since the breadth of access to criminal records is extended to non-police organizations -- public and private employers.

From a surveillance perspective, the extension of AFIS data for such non-criminal justice use, particularly record checks for employment in the private sector, may be viewed in two different aspects. First, it can be seen as a service provided by the criminal records division, which is a part of the "modernizing" state administration, to the expanding private economy through its surveillance operation. By helping screen out supposedly "potential criminals" from employment premises, the state is in effect facilitating a relatively predictable investment climate for the private sector. Second, and contrary to the first, it can also be considered as a rationalized form of state domination and perpetuation of social injustice, that serves the interests of capitalists at the expense of certain socially disenfranchised groups.

---

[20] Christopher Dandeker, *Surveillance, Power and Modernity*, 131.

It is difficult to say which of the two positions actually prevails in the perception of the Thai public. This is because the knowledge about AFIS and its exploitation is limited to only small social circles -- the police, the system designers, the bureaucrats, the capitalist entrepreneurs who are clients of the system, and small numbers of the press. As a crime suppression division, the development of the CDOS and the AFIS has been shielded from regulation and public scrutiny. Although the criminal records division has not been entirely secretive about the existence of these database systems, they are not altogether open about them.[21] A quick read through an article in a local magazine about the AFIS shows that the writer does not have in-depth knowledge about the system and is likely to have based his piece on published materials or oral accounts rather than direct observation. The emphasis, as mentioned, is on the technical capacity of the system and related positive benefits. In the same vein, the silence from local academia on the social implications of the system may be attributed to pure ignorance. While the ideological prevalence of the "information society" may play a role in bracketing the problems of social control in these police databases, this is not the only factor. Compared to the PIN project, the case of the AFIS is more complicated for several reasons.

Besides being exempted from regulatory control, the AFIS also concerns only a small segment of the population, who are extremely politically and socially alienated -- the ex-convicts or arrestees. According to a critical review of past Thai constitutions and laws, there had not been adequate constitutional protection for the rights of criminal suspects in Thailand until 1984.[22] Although subsequent constitutional amendments have stipulations that improve upon the status of these rights, they are still poorly enforced in practice. Under such circumstances, the opportunities for the AFIS data subjects to maneuver against the risk of unfair victimizing by the status quo appear very slim. The veracity of the AFIS data notwithstanding, these data subjects have no right whatsoever to examine this data or to shield themselves from the consequences of being classified as a "population likely to commit crime." If such uncontested situation continues as technocratic plans to link up different computer databases materialize, the AFIS data subjects may find themselves eventually drifting towards something akin to a totalitarian regime.

---

[21] I must emphasize that I have been particularly fortunate to have been allowed extensive access to, and to have witnessed first-hand data-handling practices at both database sites.

[22] Thanes Apornsuwan, "The Rights of Thais in the Thai States," (sitthi khon thai nai ratthai) in *New Paradigms in Thai Studies in the Year 2000 (Jintanakarn su pi songphan navakam cheung krabuanthat darn thaisuksa)*, ed. Chaiwat Satha-anand (Bangkok: Thailand Research Fund, 1996), 188.

PART II: PRIVACY

CHAPTER 6

INTRODUCTION TO PRIVACY:
A THEORETICAL AND POLICY SKETCH

This chapter introduces readers to the concept of privacy in two major discourses --
philosophical/historical and public policy. The first section of the chapter discusses the
philosophical and historical roots of the concept, its importance in various dimensions, and an
evolving debate on whether privacy is a universal moral value. The second section gives an
overview of public policy and legislation relating to information privacy or data protection at
the national and international levels, as well as the theoretical basis on which such policy-
making rests. Following a critical review of the literature, the chapter concludes by
presenting an analytical framework that is suitable for an analysis of information privacy in a
setting like Thailand.

PHILOSOPHICAL AND HISTORICAL ROOTS OF "PRIVACY"

The dominant discourse on privacy is situated within the framework of western cultural
traditions. The many conceptual presuppositions associated with privacy today reflect deep-
rooted and evolutionary products of a social development, in particular, western liberal
traditions. In wrestling with the highly volatile, vague and controversial concept of privacy,
many writers from diverse backgrounds have attempted to define it with some verbal precision.
Table 6.1 provides a listing of some of the more prominent definitions and concerns
encompassing "privacy" as given by many authors over the years. This listing is intended
mainly to give some insights into the way privacy has been conceived by Western thinkers. It
bears no intent to supply an all-embracing definition or an exhaustive set of definitions for the
concept.

183

Table 6.1

List of some of the important definitions for "privacy"

Writers/ Year of Publication	Definition(s) of "privacy" given
Samuel Warren and Louis Brandeis / 1890	the right of an individual to be let alone.
Alan Westin / 1967	the claim of individuals. groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others
Charles Fried / 1968	that aspect of social order by which persons control access to information about themselves
Arthur Miller / 1971	the ability (of individuals) to control the circulation of information relating to them
Judith Jarvis Thompson/ 1975	a right that was derived from clusters of other (individual) rights. especially "rights over our own persons" and "rights over our own property"
Ferdinand D. Schoeman/ 1984	1) claim, entitlement. or right of individual to determine what information about himself (or herself) may be communicated to others; 2) measure of individual control over information about himself/ herself, intimacies of personal identity, or who has sensory access to him/her; and 3) a state or condition of limited access to a person

Source: Samuel D. Warren and Louis D. Brandeis, "The Rights to Privacy," *Harvard Law review* 4 (December 1890): 195; Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967). 7; Charles Fried, "Privacy," *Yale Law Journal* 77, no. 3 (January, 1968): 475-93; Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (Ann Arbor: University of Michigan Press, 1971), 211-16; Judith Darvis Thompson, "The Right to Privacy," *Philosophy and Public Affairs* 4, no. 4 (Summer 1975): 303; and Ferdinand David Schoeman, ed. *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984), 2-3.

With the exception of the definitions given by Warren and Brandeis, and Judith Jarvis Thompson, all the other definitions of "privacy" listed above exhibit a concern with information privacy that has emerged as a major area of privacy debate in industrialized western countries since the 1960s, and which is also a focus in this study. The Warren and Brandeis' classic definition was more oriented towards physical privacy, one that, they feel, was increasingly eroded by the operation of the news media. Meanwhile, Thompson's definition featured an effort to undermine the view that privacy is a separate category of right, in and of itself. This exception aside, all the above definitions are rooted in classical liberal doctrine with its emphasis on an individual's possession of certain natural rights. In this western legacy of privacy, the natural rights in question are framed in terms of private rights of individuals against intrusive or unjust acts by others particularly public authorities.

While several contemporary writers on privacy have drawn upon the philosophical insights of classical advocates of liberalism and liberal democracy such as John Locke and John Stuart Mill,[1] the historical precedents which have shaped the individualistic theory and practice of privacy date back to even earlier social and cultural trends in Western society. In his seminal anthropological study on privacy, Barrington Moore notes that all civilized societies, even as early as classical Athens and ancient Hebrews, are likely to display some form of awareness of the conflict between private and public interests. While fourth-century Athens is cited as an exemplary case of strong awareness of this public-private conflict, Roman society is viewed as the opposite model of such legacy. The Athenian tradition, with its emphasis on libertarian and egalitarian ideals, also provides a favorable background for the development of private rights against the arbitrary abuse of authority by the state. Without such a democratic line of development, Moore argues, private rights could not survive because

> only where the people have power are they in a position to erect effective barriers against the misuse of power, the capricious intrusion into what they conceive as their own affairs.[2]

---

[1]See, for instance, Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995), 25, and Colin J. Bennett, "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s," *Science, Technology & Human Values* 16, no. 1 (Winter 1991): 51-69. Regan attributes the root of contemporary theory of privacy to Lockean liberalism, while Bennett alludes to the liberal democratic theory of John Stuart Mill as the basic premise for the same theory.
[2]Barrington Moore, *Privacy: Studies in Social and Cultural History* (Armonk, NY: M.E. Sharpe, 1984), 271.

The Athenian legacy lived on through the Middle Ages and evolved further with the development of the notion of the peoples' right of resistance to an unjust king[3] and the practice of immunity in feudalism[4] in the areas outside of Roman influence. Although this divisive tendency separating the public and private realms subsided during the period of royal absolutism in Europe, which reached its height in the seventeenth century, it became visible again during the subsequent periods of the Enlightenment, the industrial revolution and the birth of liberal capitalism in the eighteenth and nineteenth century.

The Enlightenment, which featured a gradual spread and popularization of philosophies stressing the preeminence of reason and the individual, bolstered further ideas associated with private rights. Prominent philosophers in this period, namely Immanuel Kant and John Locke, have fostered the notion of a social contract between the individual and the state, with the latter having inherent limits in its power over the former.[5] This liberal concept of state-individual (public-private) relations, it is worth emphasizing, antedates the introduction of democratic principles and institutions, which did not amount to anything before the nineteenth century.[6] As many writers on privacy argue, this liberal political philosophy has contributed much to the creation of a body of laws that explicitly recognize the individual's right to privacy.

The emergence of the bourgeoisie and free wage labor, which replaced feudalism and traditional craftsmanship guilds, gave rise to economic individualism under which private property came to mean "the right to do as one wanted with one's own."[7] With the continued expansion of commerce and industry, this individualist trend became widespread in society at large, while fundamental social changes associated with urbanization and industrialization propelled the evolution of individual privacy further. This process of modernization which took place in the West in the late eighteenth century contains mixed implications for individual

[3]In practice, the right of resistance to an unjust king meant that the people rejected the king, refused further obedience, and elected another. The practice of this right appeared first among the Germanic and Nordic peoples during the period of migrations that followed the collapse of Rome. See Barrington Moore, *Privacy*, 280-1.
[4]The concept of immunity, which derived directly from feudalism, had two major forms. One was the transfer of public authority to persons or groups with the consequence of creating a distinct area of local self-government, as in a fief or a manor.   Under an immunity, the household and possessions of an individual or a group became exempt from the fiscal, military and judicial powers normally exercised by the holder of a public office that had authority over the territory. The other major form of immunity took the form of a granting of special powers to the towns, which became a special legal and administrative area separated from the remaining territorial jurisdiction of the exterior authority.   Both forms of immunity reflect decentralization and even social fragmentation., Ibid., 282.
[5]John Keane, "Remembering the dead: civil society and the state from Hobbes to Marx and beyond," in *Democracy and Civil Society: on the Predicaments of European Socialism, the Prospects for Democracy, and the Problem of Controlling Social and Political Power* (London: Verso, 1988), 34.
[6]C.B. Macpherson, *Democratic Theory: Essays in Retrieval* (Oxford: Clarendon Press, 1973), 24-25.
[7]Ibid., 284.

privacy. On the one hand, the changing social structural trends increased both the physical and psychological opportunities for privacy as evidenced in such phenomena as the nuclear family living in individual households, the anonymity of urban life, mobility in work and residence, and the weakening of religious authority over individuals. On the other hand, modern societies also create large bureaucratic organizations with their insatiable appetite for information on people, new and more pervasive surveillance technologies, and most importantly, the modern state with its technological and military capacity to create the utmost forms of social control.[8]

From the nineteenth century onwards, the consolidation of liberal democracy, as a political system and ideology, gradually became a viable force in shaping the importance of privacy in many modern western societies. When the first philosophical and legal writing about "privacy" appeared in the US in 1890, the authors' understanding of privacy was notably founded upon a strong liberal premise, with its emphasis on individualism and liberty. In this article, Samuel Warren and Louis Brandeis see privacy as an individual's means of withdrawal from society so that they can be "let alone." After a long interval of three-quarters of a century, privacy, provoked by technological changes and the growing demand of formal organizations for information on people, emerged as a major topic of philosophical interest in the 1960s. Writings that emerged during this period were also dominated by the liberal view of privacy. Although there are several works that tried to broaden the relevance of the concept of privacy from an individual basis to a larger social concern, they failed to develop this aspect as fully as they examined the importance of privacy to the individual. Among these, Edward Bloustein argues that privacy can be seen as a social value and a community concern, but he still bases his acknowledgment of this social importance of privacy on the "preservation of the individual's dignity."[9] Meanwhile, Carl Friedrich, evidently inspired by democratic ideas, expresses concern about the political implications of privacy, which he conceptualizes as "the boundary between public and private." According to Friedrich, while privacy has a distinctive function in maintaining a particular political order -- democracy, this functionality operates through the individuals by ensuring them of basic dignity "which is so crucial a constituent element of a democratic belief system."[10] Friedrich is not alone in recognizing the importance of privacy to a democratic system and in arguing that the destruction of a private sphere is

[8]Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 21.
[9]Edward J. Bloustein, "Privacy as an Aspect of Human Dignity -- An Answer to Dean Prosser," in *Philosophical Dimensions of Privacy: An Anthology* , ed. Ferdinand David Schoeman (Cambridge, Cambridge University Press, 1984), 158 (first printed in 1964).
[10]Carl J. Friedrich, "Secrecy versus Privacy: The Democratic Dilemma," in *Privacy*. Nomose Series 13 Yearbook of the American Society for Political and Legal Philosophy, eds. J. Roland Pennock and John W. Chapman (New York: Atherton Press, 1971), vii.

tantamount to totalitarianism. Alan Westin articulately contrasts the functioning of privacy and its converse, surveillance, in democratic and totalitarian systems:

> Just as a social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life.[11]

In addition, as a social value, privacy does not appear to be equitably distributed across different social groups. Certain social groups are bound to be more vulnerable than others in terms of privacy risks and protections. As Colin Bennett argues, privacy is not only culturally relative but also varies in accordance with a person's position in the socio-economic stratum and his or her social surrounding.[12] This argument is supported by results from several cross-sectional surveys on privacy, particularly computers and privacy, most of which were undertaken in the US. The results confirm that attitudes and opinions about privacy vary from context to context and that it is not possible to predict from one context to another.[13]

In all, it is quite clear that the philosophical arguments about privacy up until the 1970s tend to bolster liberal democracy as they are, implicitly or explicitly, associated with the concepts of individual rights, limited government, the rule of law, and a separation between the realm of state and civil society. In this light, the importance of privacy can be seen in different dimensions which are not necessarily mutually exclusive of each other. After all, individuals are a part of a society and obtain the concept of self from society and through social interaction. Insofar as western liberal democratic societies are concerned, privacy is important because it enables the development of a certain type of individual who forms the basis of a liberal democratic society.

---

[11]Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 24.

[12]Colin J. Bennett, *Regulating Privacy* (Ithaca, N.Y.: Cornell University Press, 1992), 13.

[13]See for example Louis Harris & Associates, Inc. and Alan F. Westin, *The Dimensions of Privacy: a National Opinion Research Survey of Attitudes Toward Privacy* (New York: Garland Publishing, 1981); James Katz and Annette Tassone, "Public Opinion Trends: Privacy and Information Technology," *Public Opinion Quarterly* 4 (1990): 125-143; and Oscar Gandy, *The Panoptic Sort*.

With the prominent exception of Barrington Moore's work, earlier writings on privacy seem to base the claim that privacy is an important value on empirical and philosophical evidence that is mainly limited to the West. Although Alan Westin may have tried to escape this Western bias by alluding to animal instincts as the origin of human claims to privacy, he was referring more to privacy in a physiological sense rather than privacy in the political sense of rights protecting individuals against intrusive or unjust acts by others, particularly public authorities. Physiological privacy covers human needs or desires to be secluded from others in such physiological activities as excretion, secretion, and copulation, to name but a few.[14]

Evidently, there is an important distinction to be drawn between "privacy" in these two senses, and it is doubtful if a connection can always be established between them. Although Westin recognizes the difficulties in making cross-cultural comparisons regarding norms of privacy in different societies, he still insists that privacy (see Westin's definition of privacy in Table 6.1) appears to be a cultural value in all known human societies although the form it takes, or the name it is known by, may vary enormously. In arriving at this conclusion, Westin, who relies heavily on secondary evidence compiled from cultural anthropological research in many "primitive" societies, has in effect conflated two aspects of privacy -- physiological and political -- into one. Meanwhile, he also elevates privacy and the private realms of behavior to a universal and indispensable role in the functioning of all human societies. In the same vein, another anthropologist, Robert Murphy, argues that privacy, as a means of social distance, is operative in and significant to all societies and not only western individualistic societies.[15]

By contrast, Moore is vehement about distinguishing the two aspects of privacy in his conception of privacy. He argues that while it may be safe to presume that the desire for physiological privacy is a panhuman trait,[16] such is not the case for privacy in the political

---

[14]Barrington Moore. "Privacy," 59.

[15]Robert F. Murphy. "Social Distance and the Veil," in *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand David Schoeman. 49. (first published in *American Anthropologist* 66. no. 6 (1964): 1257-1274) In this article, Murphy studies the use of a veil among a Mediterranean tribe called the Tuareg . He argues that the veil functions as a marker of symbolic distance enabling a Tuareg person to maintain a diffuse and generalized kind of distance between himself and those who surround him socially and physically. He also argues that social distance pervades all social relationships though it may be found in varying degrees in different relationships in different societies.

[16]In his extensive anthropological study of privacy. Moore asserts that there indeed exists a human society without privacy. in the physiological sense. He points to the case of the Siriono Indians in Bolivia, among whom all physiological activities can and do occur in the presence of other people. However, he also notes that a closer examination reveals that a desire for privacy does exist in the Siriono society. While noting that a

189

sense. The latter, he argues, is more culturally relative and specific since it depends more on a process of socialization and acculturation. In very simple societies -- defined as societies without chiefs or any political organization, Moore argues that privacy in the sense of rights protecting the individuals is completely missing although awareness of and desire for physiological privacy may be present. This is because there is no organized public authority against which it would be necessary to create such rights. However, there may exist rights against other individuals, which may take the form of tacitly accepted social circuit breakers or rules governing the etiquette of access to other persons.

In any case, Moore appears to be more interested in private rights against public authority rather than private rights against other individuals. While he has never made the linkage between the liberal roots of privacy and the conception of privacy explicit, Moore, as earlier mentioned, is vocal about associating the political aspect of privacy with democracy. Without democratic development, Moore is skeptical whether privacy and privacy rights can manage to grow at all. Powerful rulers, he argues, are bound to avoid granting rights against the misuse of their authority because such rights are both a limitation on, and a threat to, their dominance. Even in societies where there is a recognition of the distinction between public and private realms of behavior, this awareness does not necessarily translate into the protection of individuals against the abuses of public authority. Citing the case of ancient Chinese society, Moore points out how early Chinese thinkers were very much aware of the public-private distinction and yet the authoritarian rule of the ancient Chinese society provided practically no formal basis for protection of ordinary individuals against the intrusive abuses of public authority.[17] Similar to the Chinese, ancient Indian or Japanese political traditions also lacked the formal protective shield that resembles the right of resistance in the West. This tradition of rights against authority, argues Moore, has developed much further in, and is possibly unique to, the West.

While Moore's insight may shed some light on the cultural dispensability of privacy in some societies, his study is generally limited to social and cultural trends in societies remote in time and space from the modern West where privacy initially emerged as a basic right or legal

---

desire for (physiological) privacy may be a panhuman trait, Moore also observes that such a desire can be easily controlled or extinguished.

[17]Moore was emphatic about distinguishing "formal" versus "informal" means for individuals to protect themselves against arbitrary interference by authorities. In addition to the workings of the family patronage system, there were at least two other informal defenses of the individual against the government in ancient China. One was bribery and the other was distance from the arms of authority. Before the advent of new communication and transportation technologies, it took an enormous amount of time for information to reach the central government and for it to react. In this way, the mass of the population was able to achieve some level of autonomy from the state.

entitlement. Several contemporary Western writers indeed consider privacy a modern value, which has been expanding along with many other basic rights and social values since modernity began to evolve in Western Europe in the eighteenth century.[18] Some of these writers tend to highlight another aspect of privacy -- that of morality -- which Moore fails to discuss. In so doing, they have also accorded privacy the status of a universal norm.

Writings that emphasize the centrality of privacy to morality generally follow three related strategies. One is to demonstrate that respect for privacy is a key component in the more general regard for human dignity. The appeal here is to such conditions as moral integrity, individuality, consciousness of oneself as a being with moral character and worth. Control of one's private sphere is, seen in this light, as essential to a person's "dignity as a human being." Violating privacy is thus regarded as immoral.[19] Another strategy is to illustrate that respect for privacy is integral to one's understanding of oneself as a social being with varying kinds of relationships, each in its way important to a meaningful life.[20] The third strategy is to stress how respect for privacy is conducive to democracy, which is defined not only as a kind of polity or society but also as a set of moral ends. In other words, these approaches attempt to demonstrate a connection between respect for privacy and certain individual, social, and political ideals.

In many ways, the above ideals reflect a normative orientation that is clearly liberal. The fundamental premise of this moral bearing is that individuals qua individuals have moral rights that serve as constraints on government and others -- constraints that are under the control of the right holder. Since these rights are predicated upon an assumption that every human being is endowed with powers of reason, they are seen by liberal advocates as universal rights or norms, which are applicable to all people in all places at all times. At one extreme, the preservation of privacy can be seen as a universal value or right in itself. More frequently, however, it is seen as a value to be balanced with others or occasionally as a means to realize other related values and norms which are regarded as universal human properties.[21]

---

[18]See for example, James E. Katz, "Telecommunications and Computers: Whiter Privacy Policy?," *Social Science and Public Policy* 25, no. 1 (November/December 1987): 81-86.

[19]Robert S. Fortner, "Physics and metaphysics in an information age: Privacy, dignity and identity," *Communication* 9 (1986): 151-172.

[20]Ferdinand D. Schoeman, "Privacy: Philosophical Dimensions of the Literature," in *Philosophical Dimensions of Privacy: An Anthology* (Cambridge, Cambridge University Press, 1984), 158 (first printed in 1964), 8.

[21]David Lyon, " Privacy, Power, Persons," in *The Electronic Eye: the Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994), 185.

It is clear, from the discussion above, that what liberals see as universal norms grounded in the universal character of humanity are in fact particular norms embedded in shared understanding of a specific culture and tradition, that of liberal western civilization.[22] In essence, the liberal defenders of privacy, with their universalist claims and individualist presuppositions, have succumbed to the same flaws that their rights-oriented liberal peers have come under criticism for. First, they committed an epistemological error by articulating a universalist claim to a certain rights-based concept of morals while presupposing a substantive -- historically and culturally specific -- concept of the good. Here, universality is ironically reasoned with an Occidental understanding of the world and the belief in the moral superiority of the West.

Secondly, in their conception of privacy, the liberal champions tend to emphasize the notion of liberty and freedom primarily from the standpoint of individual rights and with little regard for social or community-based concerns. The liberal ideals of moral autonomy and individual self-development are fundamentally based on an atomistic and abstract concept of the self as the subject of rights. Even when merged with democratic principles and practices, these ideals could amount to only one version of democracy, in both a normative and empirical sense, that is, the liberal-pluralistic type. With this predominantly liberal grounding, (information) privacy can be "a pre-condition, not of democracy per se, but of a particular type of democracy -- one that is individualistic, possessive, and non-communitarian, rather than participatory and communitarian."[23] Closely linked to these two types of democracies are two types of individualism as outlined by C.B. Macpherson -- possessive individualism and emancipatory individualism. The former views an individual human being as essentially a consumer of utilities, with unlimited right of property holding and with very limited social responsibility to society.[24] The latter, on the contrary, sees a human being as a doer and an exerter who is capable of developing most fully his uniquely human capacity and of contributing to a development of a free and equal society.[25]

---

[22]This can be concretely illustrated by the evolution of western political and social institutions in the tradition of ancient Greece, English Protestantism and common law traditions, and American constitutionalism and property concepts.

[23]Colin J. Bennett, "Computers, Personal Data, and Theories of Technology," 60.

[24]In his theory of possessive individualism, Macpherson describes how Thomas Hobbes, one of the original political theorists who laid the philosophical foundation of modern Anglo-Saxon liberal democracy, discards the traditional concepts of society, justice, and natural law and instead deduces political rights from the atomized interest and will of dissociated individuals. See more in C.B. Macpherson, *The Theory of Possessive Individualism. Hobbes to Locke* (Oxford: Clarendon Press, 1962).

[25]Macpherson borrows this view about human nature from John Stuart Mill who derives his normative values about human beings, liberal democratic society and the state from pre-liberal and pre-market tradition, which includes the Christian natural law tradition, and which stresses the human purpose of developing distinctly human attributes. See more in C.B. Macpherson, "Democratic Theory," 8.

In studying privacy in a non-western setting, it makes sense, given the theoretical analysis above, to focus more on certain dimensions of privacy rather than others. James B. Rule conceptualizes privacy broadly understood into two dimensions -- aesthetic and strategic.[26] In the aesthetic dimension, privacy is generally conceived as an end in itself since it embodies a certain humanistic value or set of values which are subsumed under the same philosophical rubric such as human dignity, individual freedom and self-identity. In the strategic dimension, privacy is seen as a means to advance to other ends in the form of rights or interests that do not necessarily reflect the liberal individualistic ideals. Such ends would include social participation, political autonomy, and bureaucratic and democratic accountability, among others.[27] According to Colin J. Bennett who focuses more on data protection issue, the problem can be analyzed at three levels -- humanistic, political and instrumental.[28] The humanistic and instrumental levels correspond directly to Rule's two notions of privacy above. The political aspect, however, emphasizes the political implications of government's control over the collection, use and dissemination of personal information and argues for citizens placing limits on this power of the state to ensure democratic accountability. While I am skeptical of the universality of the liberal ideals from which Bennett's political aspect of data protection derives, there is sufficient justification not to disregard this dimension of analysis a cross-cultural setting. While democratic accountability may be somewhat taken for granted in democratic societies like the US and Western Europe, it is an idealistic end for many societies struggling to advance their democratic development. Privacy or data protection can therefore serve as an intermediate to acquire this political end.

To pursue an analysis of privacy in a culture where privacy is not a substantive social value, I feel that the latter two dimensions of privacy -- political and instrumental -- be emphasized. Through this approach, one can avoid being confined to the value-laden and western-centric liberal concept of privacy and possibly expand it to a broader social significance. After all, what is at stake in the privacy issue is not only an individual right in limiting intrusion by others and in controlling circulation of personal information about oneself. Equally, if not more, important, is the notion that privacy serves as a restraint on how organizations or certain social groups use their power vis-a-vis individuals and other social groups.

---

[26]See more in James B. Rule, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (New York: Elsevier, 1980), 22.
[27]David Lyon and Elia Zureik, "Surveillance, Privacy, and the New Technology," in *Computers, Surveillance and Privacy* (Minneapolis: University of Minnesota Press, 1996), 16.
[28]Colin J. Bennett, *Regulating Privacy*, 23-37.

Just as the philosophical concept of privacy originated in liberal democratic societies of the West, information privacy as a political and legal issue also emerged for the first time during the 1960s mainly in western industrial states. In the scholarly discourse, this emergence is seen as a result of two twin processes that have developed and become characteristic of late industrialization. One was the development of computer technology which made possible automatic data processing. The other was the expanding bureaucratization of large organizations particularly in their record-keeping tasks. The two combined gave rise to the growing tendency to computerize personal files in both public- and private- sector institution and, in turn, provoked public interest in privacy protection. In the US, these trends are best exemplified in the controversial proposal in the late 1960s to rationalize federal data systems through computerization and centralization. Despite official claims that the proposed national data center would be devoted primarily to the gathering and processing of statistics, this did not stop it from being highly politicized and from finally being quashed in congress due to opposing public sentiments. The US early experience with privacy concerns not only suggests a form of technological paranoia but also demonstrates profound fears of the state by the public and their distrust in the ability of public officials to utilize personal information with care and propriety.

It merits emphasis that early privacy concerns were mainly directed at public-sector institutions. Governments, it has been argued, are the worst offenders against privacy, and few governments would refrain from surveillance of the populace if it could be perceived or justified as being in the public interest.[29] As computer systems developed, governments of different political complexions came to realize their advantages particularly in manipulating personal data of citizens for a variety of purposes -- administrative, statistical and investigative. While the modern welfare states in the West may rationalize the widespread use of computers in their personal record-keeping and the quantitative and qualitative increase in the information collected from individual citizens, the modernizing states, which adopt the technology later, are likely to justify it on development grounds.

---

[29]David H. Flaherty. *Protecting Privacy in Surveillance Societies : The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989). 12-13.

In light of the emerging political controversy surrounding public- and private-sector implementation of electronic data processing in the 1960s, a number of studies were initiated during the 1970s by several governments in Western Europe and North America to examine the status of data processing activities with respect to privacy in personal files.[30] Meanwhile, international and inter-governmental organizations such as the United Nations, the Council of Europe, and the Washington D.C.-based World Peace Through Law Center also began to explore and develop policy options and guidelines in an attempt to mediate the impacts of computers on human rights, particularly the right to privacy. These studies and guidelines, which predate national legislation on data protection in primarily industrialized countries, set the tone for the discourse on information privacy in the next two decades. The underlying argument as presented in these studies and several by academics,[31] mainly in law, public policy and civil liberties circles, is that the problem is essentially one of establishing an appropriate balance between the demands of citizens for personal autonomy and the demands of the state for information about its citizens. Many of these studies also argue that it is the citizens' demand for public services, particularly in the context of the welfare state, that pushes governments into massive collection of personal information in the first place. The conflicting demands for privacy protection and for government services are said to be at the core of the privacy issue. In many ways, these contradictory demands that the public is said to be placing on governments are reminiscent of the earlier discussion of the janus face of surveillance. But unlike in the surveillance literature, the mainstream privacy discourse tends to focus on the issues of civil liberty, the application of computers, and the privacy controversy rather than addressing the larger social implications of personal data systems, particularly their role in the process of social control.

In a more critical vein, however, certain writings on privacy take a leap from the proposed argument of "balance" between organizational record-keeping and privacy/freedom to a different theme in discussing the dilemma of privacy. According to Kevin Wilson, for instance, the real dilemma lies in the conflict between the classical liberal tradition of privacy and the reality of structural change in the social-economic order in advanced industrial societies, a change which compels the modern state to deploy increasingly bureaucratic techniques of control to secure stability. As he describes the situation,

---

[30]See, for example, Alan F. Westin and Michael A. Baker. *Databanks in a Free Society: Computers, Record-Keeping and Privacy* (NY: Quadrangle Books, 1972); Norman Lindlop. *Report of the Committee on Data Privacy*, Cmnd 7341 (London: HMSO, 1978); and Privacy Protection Study Commission. *Personal Privacy in an Information Society* , the Report of the Privacy Protection Study Commission (Washington, D.C.: U.S. Government Printing Office, 1977).

[31]For example, Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967); and Arthur R. Miller, *The Assault on Privacy* (Ann Arbor: University of Michigan Press, 1971).

Planning and managing of the social and economic life of the nation is accentuated, expanded and refined. This has political repercussions in the intrusive character of the state's efforts to maintain stability through management of the populace.[32]

To Wilson, the arrays of surveillance apparatuses employed by the modern industrial estate have gone far beyond what could be considered within a rubric of "balance." In the meantime, he notes that the existing legal-regulatory discourse on privacy, particularly in North America, has not reflected an altruistic desire of governments to protect their citizens as would be in the tradition of political liberalism. Often, privacy legislation is only a minimal concession, and the many provisions it accords fail to redress or affect the balance of power between individual and institution in any real sense. According to Wilson, liberal values are in a period of crisis as they are being adapted to the demands of the economic and political order of late capitalism.

Several subsequent writers on privacy concur with Wilson that the idea of "balance" is ludicrous in the contemporary period of widespread informatization. David Lyon points out how today's surveillance is carried out not only by government but also by large corporations. and not only within the nation-state but also in telecommunications networks that transcend geo-political boundaries.[33] In the same vein, David Flaherty notes that new developments in ICTs are galloping ahead of regulation and legal control, and to hope to strike a balance with record-keeping organizations, particularly the government, is pure naiveté.[34] According to Priscilla Regan, the balance of privacy is often outweighed by competing interests and values associated with those interests. She identifies the efficiency of organizational operation as one of the major competing interests in the modern era.[35] As discussed in chapter one, personal-data systems and associated technologies were designed during the control revolution to enable modern organizations to realize the principles of goal-oriented efficiency through a rationalized control of information. To sustain and bolster this rationalization scheme, modern opponents of privacy usually do not challenge privacy as a value but redirect the definition of the issue to other countervailing considerations such as efficiency, crime control and ensuring an honest workforce.

[32]Kevin G. Wilson, *Technologies of Control: the New Interactive Media for the Home* (Madison: University of Wisconsin Press, 1988), 50.

[33]David Lyon, *The Electronic Eye* , 185.

[34]David H. Flaherty, "Controlling Surveillance: Can Privacy Be Made Effective?," in *Technology and Privacy: the New Landscape*, eds. Phil Agre and Marc Rotenberg (Cambridge, Mass: MIT Press, 1998), 173.

[35]Priscilla Regan, *Legislating Privacy*, 32.

Ironically, the modern preoccupation with efficiency can also be felt in the legal-regulatory discourse of privacy. James Rule coins the term an "efficiency criterion" to describe how the regulation of personal-data systems in the US is largely judged by the functional "efficiency" of the systems. By this criterion, he argues, data surveillance of citizens is considered acceptable provided that personal data systems function as fairly, openly, and efficiently as possible. Following Rule's lead, Kevin Wilson draws examples from North American privacy laws in which many of the key principles resonate with the "efficiency criterion." Take the so-called collection principle, for instance Wilson observes how the Canadian Privacy Act and the American Privacy Act do not effectively restrict either the quantity or the types of information gathered by federal agencies. From the start, these laws were never meant to do so. The force of the laws, he argues, is directed primarily at restricting abusive, arbitrary collection practices which are not sanctioned by an institution's lawful functions. Similarly, the access principle, which is stipulated in the Privacy Acts and the Freedom of Information Acts of both countries, is designed to ensure that decision-making on personal files is founded on "accurate" information and to reassure an individual about the fairness of institutional processing of his or her files. While this provision may oblige organizations to be more cautious, the caution is directed at accuracy. It does not affect the fundamental mechanism of control and the linking of the individual to his or her past through documentation.[36]

To counter the blinding effect of prevalence of the "efficiency criterion" in the legal-regulatory framework, Rule urges that one pay less attention to the correctness of the instrumentalities of personal data systems and more attention to the intrinsic nature of surveillance and their social implications. What is missing in the mainstream discourse on privacy and also in North American privacy legislation, he says, is a searching assessment of the risk of large-scale surveillance and the fundamental shift in prerogatives and power involved in the development of new surveillance systems. As a result, these laws only serve to legitimate extensions of surveillance which can possibly lead to totalitarianism. In his words,

> It is the genius of American liberalism that, when faced with a particularly unconscionable practice by some powerful interest, it regulates that interest in such a way as both to mitigate the sting of the abuse and at the same time to consolidate the position of the perpetrators. The (US) Fair Credit Reporting Act stands in this tradition.[37]

---

[36]Kevin G. Wilson, *Technologies of Control*, 57, 59.
[37]James B. Rule, *The Politics of Privacy*, 214.

While warning of the considerable augmentation of centralized organizational power provided by the appropriation of computers and later ICTs. Rule, like several other critical writers on the issue, feels that the key to counter surveillance lies beyond the liberal claims to privacy protection. According to this view, the liberal values associated with the privacy concept may be pivotal in the initial definition of a policy problem and in placing it on the policy agenda, but they do not provide a sound basis on which to formulate public policy for several reasons.

First and relating to what was discussed above, the liberal preoccupation with individual rights and civil liberty has led to an overemphasis on the effects of surveillance on individual privacy with little regard for organizational aspects of surveillance or the mediated relationship between organizations and individuals. Correspondingly, the liberal view also disregards the crucial connection between informatization processes, which threaten privacy, and the ongoing restructuring of capitalism from Fordism to a new regime of flexible accumulation, as discussed in chapter one. In effect, the goal of much privacy legislation has been to achieve the protection of the privacy of individuals rather than curtailing the surveillance activities of organizations. Unfortunately, individual rights turn out to be no match, as a means of controlling organizational power, when contending with the state or large private corporations.

Secondly, when viewed as a type of civil liberty and thereby a negative right, the liberal concept of privacy becomes a not-so-potent political resource. According to Priscilla Regan, civil liberties issues, unlike those of civil rights, do not provoke great electoral supports at least in the US. While there might be a recognizable public concern on the issue, there is usually inadequate public mobilization to take political action to protect it.[38]

In addition to a misguided emphasis and lack of public support for protecting privacy, the discussion of the concept of privacy has also come under criticism for its vagueness, ambiguity, and lack of intellectual clarity. As a value, privacy is recognized as important, but as a goal for public policy, it is seen as fraught with ambiguity. Some contemporary writers have suggested that "privacy" be supplanted with "data protection" or security when it comes to the consideration of groups of policies designed to regulate the collection, storage, use, and transmittal of personal information.[39] Others have noted that we divide privacy concerns in

---

[38] Priscilla Regan. *Legislating Privacy*, 2-3.
[39] Colin J. Bennett. *Regulating Privacy*, 13.

accordance with the specific realm to which they pertain -- information privacy, communication privacy, and psychological privacy.[40] Be that as it may, with new developments in the ICT industry, the borderline between what is considered information and communications privacy, for instance, is becoming considerably blurred. Information is no longer constrained in isolated databanks and subject to only periodic retrieval. With the ongoing innovation of computer technologies, most databanks have become parts of a distributed system of databases whereby information flows constantly and is easily accessible to network users.

In any case, the challenge to make privacy concerns a potent support for resistance is indeed herculean and, as mentioned, cannot rely only on liberal perspectives. Writing in the early 1980s, when the globalization of economic and communication systems was only an emerging reality, James Rule radically proposed creation of a less information-intensive world so that the alternatives would be less conducive to centralized social control. He urged organizations to limit the growth of personal-data systems and to minimize their reliance on them.

From another angle, Kevin Wilson, writing exclusively about privacy in North America in the late 1980s, argues for a reorientation of approach to the establishment of ground rules and limits of accepted institutional behavior rather than continued legal and policy claims to protect the individual from privacy invasions.

In a similar vein, David Flaherty, writing in the closing year of the 1980s, points out how privacy/data protection laws are inadequate to control surveillance and accentuates the importance of privacy/data protection agencies which are in charge of overseeing the implementation of laws and, more importantly, of promoting "bureaucratic accountability" in data use. The latter function, he notes, is at the heart of privacy/data protection agencies, although it is difficult to execute given the harsh reality of power relations in society. Almost a decade later, Flaherty who now has had a first-hand experience as a privacy authority,[41] revisits the role of data protection agencies in the policy arena with more disillusionment. He admits that his power and independence are considerably limited in the policy field by the authority of a legislature that wishes to introduce or to increase surveillance of the population in a certain fashion. Advisory power alone is inadequate, according to Flaherty. Instead, "a

---

[40] Priscilla Regan, *Legislating Privacy*, 9 - 10.
[41] David Flaherty became the Information and Privacy Commissioner of British Columbia, Canada in 1993. He is the first Privacy Commissioner of the province, which has a population of less than four million and is the third largest of the Canadian provinces (after Ontario and Quebec). His term ends in 1999.

privacy commissioner should have regulatory power (particularly an ability to impose a statutory sanction) at his or her disposal."[42]   In the end, however, Flaherty remains skeptical whether data protection agencies will accomplish much of their objectives amidst the rising tide of technological advancements particularly with "the ongoing explosion of the digital economy and online Internet services."[43]

Despite his disillusionment and skepticism, Flaherty still stands by most of the twelve principles he endorses in 1989 in order to curtail intrusion into private lives. Aside from the resource and autonomy of privacy/data protection agencies, the other principles Flaherty suggests should apply to all personal information systems under government control include: openness or transparency of data files; necessity of data collection; minimization and finality of data collection storage and use; informed consent from individual subjects; control of linkages and interconnections of data; accuracy and completeness of data; individual right of access to data files; regulation of use of data; penalty for abuses; and the right for data subjects to be forgotten or to become anonymous.[44]

Writing in the early 1990s, David Lyon argues for a multi-faceted approach in order to circumvent the inherent weakness of personal data law, both in the requirement and enforcement procedures. To complement the legislative approach, Lyon argues that an educative process would have to be carried out through the various media along with a mobilization of public opinion and action. Meanwhile, Oscar Gandy, in concluding his discussion on the panoptic sort,[45] recommends that a moral consciousness be raised among the population in order to counteract the overwhelming panoptic forces. Such a program of moral development involves a process of learning, one that takes historical time. Gandy entrusts this task to critical scholarship which, he says, can raise doubts in the minds of laymen while educating engineers about their social responsibility.[46]

More recently, Colin Bennett, whose main interests are in policy convergence in data protection in advanced industrial states and in advocating an embedding of privacy in international standard regimes, proposes a holistic approach to data protection. According to Bennett, there are clear limits to policy success when it comes to satisfying a highly elusive and

[42]David H. Flaherty, "Controlling Surveillance," 182.
[43]David H. Flaherty, "Controlling Surveillance, 190.
[44] See more in David Flaherty, Protecting Privacy in Surveillance Societies, 380.
[45] Borrowing from Foucault's metaphor of the panopticon, Gandy's "panoptic sort" refers to a kind of hi-tech triage through which individuals and groups of people are sorted according to their economic and political value.
[46]Oscar Gandy, The Panoptic Sort, 230.

subjective value like the right to privacy. The problem, he argues. is more conceptual than political, technological or economic. His proposed remedy to the privacy/data protection problem is possibly by far the most comprehensive, insightful, and tangible. In his words,

> What is needed is a more holistic perspective that sees data protection as a process that involves a wide network of actors (data users, data subjects, and regulators) all engaged in the co-production of data protection. The successful implementation of data protection requires a shift in organizational culture and citizen behavior. Data protection is a learning experience that involves a mutual process of education and mediation from the bottom up as much as it involves regulatory command from the top down.[47]

INTERNATIONAL AND NATIONAL APPROACHES TO PRIVACY AND DATA PROTECTION -- FROM THEORY TO PRACTICE

International legal agreements on privacy and data protection

As listed in Table 6.2, the legacy of international recognition of privacy began as early as 1946 when the United Nations General Assembly proclaimed the Universal Declaration of Human Rights in which Article 12 states,

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Although the above statement provides only a broad definition and semblance of privacy, there is a potentiality for further expansion which has subsequently become a base for signatory countries to build upon in their legal treatment of privacy. According to one observation, an important information and communications privacy concern that grows out of the U.N.'s Universal Declaration is the protection of personal names and identity. For example, where national governments seek to impose the use of a universal identifier, such as a Personal Identification Number (PIN) or Social Security Number (SSN), concern has been expressed in some signatory countries that this will undermine cultural identity and the freedom

---

[47]Colin J. Bennett. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data," in *Technology and Privacy: the New Landscape*, eds. Phil Agre and Marc Rotenberg (Cambridge, Mass: MIT Press. 1998), 120.

Table 6.2
Chronology of international and national recognitions, legal agreements.
and policies on privacy and data protection

Year	Organization/Country	Legal agreements, policy on privacy and data protection
1946	United Nations (U.N.)	Article 12 of the Universal Declaration of the Rights of man
1971	U.N.	Study by the U.N. Secretary-General's Office on the impacts of scientific and technological developments on human privacy
1973	Sweden	Swedish Data Bank Statute (Act)
1974	U.S.A.	U.S. Privacy Act
1976	Germany[48]	West Germany Federal Data Protection Law (BDSG)
1977	Canada	Canadian Privacy Act and Freedom of Information Act
1978	Austria	Austrian Data Protection Act
1978	France	French Legislation on Data Processing, Files and Liberties[49]
1978	Norway	Norwegian Personal Data Registers Act
1978	Denmark	Danish Private Registers Act
1978	U.S.A.	U.S. Right to Financial Privacy Act
1979	Luxemberg	Luxemberg's Data Protection Act
1979	World Peace Through Law Center	Resolution No. 11 -- Computer technology and the right to privacy
1980	OECD countries	OECD Guidelines on the Protection of Privacy and Transborder Data Flow

[48]West Germany or the Federal Republic of Germany had in 1970 a data protection law, the Data Protection Act of the Land of Hesse (1970), but it was not a federal statute and applied only to the public sector.
[49]Loi du 6 janvier 1978 Relative à l' informatique, aux fichiers et aux liberté.

202

Table 6.2 (continued)
Chronology of international and national recognitions, legal agreements,
and policies on privacy and data protection

Year	Organization/Country	Legal agreements, policy on privacy and data protection
1981	Council of Europe	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
1982	Canada, Sweden	Revision of Privacy and Data Act
1982	New Zealand	New Zealand's Official Information Act
1984	U.K.	British Data Protection Act
1986	U.S.A.	Electronic Communications Privacy Act
1988	Australia	Australian Privacy Act
1988	U.S.A.	Computer Matching and Privacy Protection Act
1988	U.S.A.	Video Privacy Act
1989	Japan	Act to Protect Personal Information Kept by Government Organs by Means of Computer Processing (Personal Information Act)
1990	Commission of the European Communities (EC)	Directive on the protection of individuals in relation to the processing of personal data and on the free movement of such data
1991	Japan	Ministry of Posts and Telecommunications (MPT)'s Guideline on the Protection of Personal Data in Telecommunications Business
1994	Korea	The Act on the Protection of Personal Information Managed by Public Agencies
1995	Hong Kong	Personal Data (Privacy) Ordinance
1997	Thailand	Freedom of Official Information Act (including a section on protection of personal data in government files)

Sources: David Flaherty, *Protecting Privacy in Surveillance Societies* ; Mark Rotenberg, "Communications Privacy: Implications for Network Design," *Communications of the ACM* 36, no. 8 (August 1993): 61-68; Priscilla Regan, "The Globalization of Privacy: Implications of Recent Changes in Europe," *The American Journal of Economics and Sociology* 52, no. 3 (July 1993): 257-274; and Tsuyoshi Hiramatsu, "Protecting Telecommunications Privacy in Japan," *Communications of the ACM* 36, no. 8 (August 1993): 74-77 and Privacy International website (http://www.privacy.org/pi)

of minority groups.[50] Nevertheless. it merits emphasis that international deliberations tend to suffer from the lack of precise definition of privacy, another testament, perhaps, to the universal limit of the privacy concept. In 1971, the U.N. Commission on Human Rights requested the Secretary-General's Office to study the impacts of scientific and technological developments on human rights. The resulting U.N. Report on Privacy showed an inability to provide "a concise international definition of privacy." Signatory states are thus left with the difficult task of definition, which always comes into conflict with cultural values, national interests, and national security.

In early 1968, the Council of Europe, which consists of twenty-one member states in Europe, began debating the issue of technological change and individual privacy and concluded that national and international law did not adequately protect privacy in a technological environment. By 1974, the Council had adopted non-binding recommendations following the basic format of "fair information principles" which stipulate that information should be 1) accurate, up-to-date, and relevant; 2) kept confidential and secure; and 3) accessible to individuals about and from whom the information was collected.[51] It was then that some form of common recognition about information privacy/data protection began to take shape on an international scale.

Consequently, in 1978 the Organization of Economic Cooperation and Development (OECD), which is composed of two dozen countries including much of Europe, the US, Canada, Japan, and Australia, instructed a group of experts to develop guidelines on basic rules governing transborder data flow and the protection of personal data and privacy. The OECD Guidelines, which were adopted in 1980, were a result of collaborative work by experts at the Washington D.C.-based World Peace Through Law Center and its affiliated organizations of lawyers, judges and jurists.[52] The Guidelines incorporate eight basic "fair information principles" for national application of data protection. which could be summarized in the following terms: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness or transparency, individual participation, and accountability.

---

[50] Mark Rotenberg. "Communications Privacy: Implications for Network Design," *Communications of the ACM* 36. no. 8 (August 1993): 64.

[51] Priscilla Regan, "The Globalization of Privacy: Implications of Recent Changes in Europe," *The American Journal of Economics and Sociology* 52. no. 3 (July 1993): 261.

[52] The World Peace Through Law Center and its affiliated legal experts adopted a resolution entitled "Computer Technology and the Right to Privacy," which set the precedent for the OECD Guidelines on September 20, 1979 at the Madrid Conference on the Law of the World.

(See Table 6.3). It is worth noting that the OECD Guidelines were partly inspired by economic concerns. From the standpoint of the U.S., in particular, the initiative was based on the belief that disparities in national privacy legislation might create obstacles to the free flow of information between countries, thus having serious repercussions on the economies of the OECD Member States. In any case, the Guidelines were not binding on OECD members, although some members of the group that formulated the Guidelines had recommended that they be adopted by a legally enforceable treaty. Despite being widely recognized as a primary reference for international agreements on privacy and data protection, the Guidelines have also come under criticism. Problems outlined include the absence of a clear enforcement mechanism, inadequate attention to commercial incentives to sell personal data, and lack of consideration of the misuse of personal identifiers.

Following the OECD, the Council of Europe adopted in 1981 the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." Generally, the 1981 Convention incorporated principles similar to the OECD Guidelines but differed in that it was binding on states that signed it and required that national laws be consistent with it.

Another international policy landmark on privacy and data protection of late is the recently-issued framework to protect the transborder flow of personal data outlined by the European Community (EC). Since 1990, the EC Commission has been involved in the promulgation of a general directive on "the protection of individuals in relation to the processing of personal data." After a lengthy and complicated process of bargaining by member nations and concerned sectors, the directive was passed in 1995 and came into effect in October 1998. The directive, it is worth noting, is specifically designed to harmonize public policy throughout the EC. In addition to its general provisions about the conditions for fair and lawful processing of personal data, the directive also includes additional measures some of which have become very controversial, particularly as they pertain to national laws. For instance, Article 25 of the Directive prohibits the transfer of data to a third country that does not provide an "adequate level of protection." In assessing the sufficiency of privacy safeguards, all the circumstances surrounding a data transfer or set of data transfer operations will be taken into account. Particular consideration will be given to the following: the nature and purpose of the data, the rules of law, both general and sectoral, and the professional rules and security measures in force in that country. Article 26 lists a number of derogations, one of which is the provision that data may be sent to countries with inadequate level of protection if certain

Table 6.3

Eight basic "fair information practice" principles incorporated in
the Organization for Economic Cooperation and Development (OECD)'s
Guidelines of the Protection of Privacy and Transborder Flow of Personal Data

- **The Collection Limitation Principle** states that the collection of personal data should be obtained by law and fair means and with the knowledge and consent of the record subject.

- **The Data Quality Principle** states that personal data should be relevant to the purposes for which they are to be used. and should be accurate. complete and timely.

- **The Purpose Specification Principle** states that the purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use should be limited to those purposes

- **The Use Limitation Principle** states that personal data should not be disclosed for secondary purposes except with the consent of the data subject or by authority of law.

- **The Security Safeguards Principle** states that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access. destruction. use. or disclosure of data.

- **The Openness Principle** states that there should be general practice of openness about developments. practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use.

- **The Individual Participation Principle** states that data subjects should be allowed to inspect and correct personal data.

- **The Accountability Principle** states that a data controller should be held accountable for complying with measures which give effect to the preceding principles.

Source: Organization for Economic Cooperation and Development, *Guidelines for the Protection of Privacy and Transborder Data Flows of Personal Data* (Paris: OECD, 1981).

conditions are met.[53] But in cases where the EC Commission decides that a certain third country does not ensure an adequate level of protection, it can mandate member states to prohibit the transfer of data to that country, the equivalent of a "data embargo order."[54] This, according to Colin Bennett, represents a stronger approach of enforcement than that embraced in the OECD Guidelines or the Council of Europe Convention. As a result, there have been debates and concerns arising from the provisions in the above articles in countries outside the European Union. Given the vagueness and unpredictability of the two articles, one of the major concerns has been whether "adequacy" will be judged against the principles of the directive or the method of enforcement -- the existence of a supervisory authority to oversee compliance with the law versus voluntary codes of practice and a reactive regulatory approach. If this is used as a standard, the American approach to data protection, which lacks an agency to oversee the enforcement of privacy law and an omnibus data protection law regulating both the public and private sectors, would definitely be considered inadequate.

In any case, there has been a consensus among policy analysts that the EC Data Protection Directive has been and will continue to be a major influence in shaping the direction of national legislation in data protection in the future.[55] With the ongoing globalization of economic and communication systems through the so-called global information highway, countries around the world have come under intense pressure to conform to the EC policy framework. This issue will be revisited in detail in the later section on policy convergence -- a globalization of privacy.

National approaches to data protection

Since the 1970s, a number of western industrialized countries have developed through their legal systems certain legal procedures to protect information privacy. Gradually, national rules governing institutional use of personal files in these countries have shifted in form from adjudication -- common law and civil lawsuits -- to legislation -- privacy acts, access to information statutes, and fair credit reporting legislation. These laws vary in their scope, purpose and impact and are invariably shaped by socio-economic, political, and technological

---

[53]European Union, "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." *Official Journal of the European Communities* L 281 (23 November 1995): 31.

[54]Paul M. Schwartz, "European Data Protection Law," *Iowa Law Review* 80, no. 3 (1995): 471-496, as quoted in Colin J. Bennett, "Convergence Revisited," 109.

[55]See; for instance, Priscilla Regan, "The Globalization of Privacy," 266, and Colin J. Bennett, "Convergence Revisited," 108-120.

factors in the country in which they are created. In some countries, these laws are not self-executing and rely upon enforcement through the courts. Others follow a data protection scheme whereby a particular agency or agent is charged with the implementation of the legislation. Some national laws, particularly those in European countries, cover the public and private sector in a similar fashion under a single omnibus legislation, while others, such as those in North America, regulate government and private information practices separately in different laws.[56]

Colin Bennett outlines three approaches to information privacy/data protection that broadly capture existing national perceptions of and styles of policy remedies to the problem. Each approach rests on a fundamentally different theoretical perspective on the interplay of four important factors -- information, individual, computers or ICTs, and bureaucracy -- and the priority accorded to sets of relationships among these factors.

1) the technology-control approach

The first approach defines the problem largely as a technological one with the computer and related modes of technological surveillance as the main culprit for the increasing erosion of privacy. The solution to this approach is consequently framed in terms of technical safeguards. Besides safeguards that can be built into the design of the hardware and software of ICTs and in each stage of information processing, this so-called technology-control approach also has safeguards built into the laws and public policies concerning privacy. Bennett points to countries such as Sweden and the United Kingdom in which laws just regulate computerized files and where little or no distinction is made between public and private organizations as exemplary cases of this approach.

In the Swedish case, the first country to develop legislation, all personal data systems are licensed by the Swedish Data Inspection Board (DIB), who stipulate specific conditions on the collection, storage, manipulation, and communication of personal data. According to Bennett, the Swedish approach is typically anticipatory and preemptive. It is based on the assumption that the computer has raised qualitatively new problems that require regulation. On this note, it is worth mentioning that in Sweden there is no tradition for concern of privacy (as an individual right) per se. With a long history of bureaucratic surveillance by the state, the

---

[56]Aside from the US and Canada, four other countries in the OECD had, by the end of 1996, failed to enact a comprehensive privacy/data protection law that applies to both public and private sectors: Australia, Japan, Greece, and Turkey. See more in Colin J. Bennett, "Convergence Revisited," 113.

Swedes regard detailed collection of information on population as a normal thing.[57] In fact, the general public is said to perceive data collection and government surveillance activities as being in the public welfare and not a threat to their own interests, particularly when the process is aimed at such goals as saving tax money in welfare payments or preventing fraud. Also, unlike the confrontational and often antagonistic relationship between the state and citizens in North America, the unitary and paternalistic Swedish state is generally regarded by the people as a benign force and usually with a greater amount of trust. The Swedes do not believe their society is excessively controlled and are not especially interested in protecting or developing their personal rights.

As for the case of the U.K., all computerized personal information systems (manual records not included) are registered with a data protection registrar, though no permission or license is required. Data users are also required to inform the individuals concerned when data is stored and to provide such individuals with copies of the stored information. Like the Swedish case, the enactment of the British Data Protection law was prompted mainly by fear of computers. Strangely enough, conventional English law does not recognize a right of privacy or a right to be left alone as a separate right but as an adjunct to the protection of other interests -- trespass cases. As far as the 1984 Data Protection Act is concerned, its emphasis is not so much to promote individual privacy as to "ensure that the automatic processing of personal data is carried out in a sound and proper manner."[58]

In sum, the technology-control approach, as Priscilla Regan observes, concentrates mostly on the computer and information, as well as on the computer and the bureaucracy's information handling. Little concern is given to the relationship between the individual and his or her personal information, nor that between the individual and the bureaucracy. Insofar as the licensing approach to data protection is concerned, it has been criticized as an excessively bureaucratic mode of controlling surveillance. According to David Flaherty, this approach which is embodied, for instance, in the Swedish legislation, is too formalistic and burdensome for the problems at hand. Licensing agencies are usually too burdened with massive registration tasks for the public and private sectors to give sufficient attention to such central tasks as audits.[59] In a similar vein, Colin Bennett notes that since the problem is viewed

---

[57]A nationwide system of national identification number (PINs) was introduced in Sweden in 1947, while a register-base census of population was implemented in the 1980s. See more in David Flaherty, *Protecting Privacy in Surveillance Societies*. 93-162.

[58] Great Britain, Data Protection Registrar. *Second Report* (London: HMSO, 1986), 16, as quoted in Colin Bennett. *Regulating Privacy*, 62.

[59]David H. Flaherty, *Protecting Privacy in Surveillance Societies*. 394-395.

primarily in technological terms, this approach thus makes no judgment about the propriety or necessity of information collection in the first place. It is simply assumed that vast amounts of specific personal information are necessary for the range of organizational responsibilities. Bennett also takes the analysis of the technological approach one step further by charging it with technological determinism. According to him, this approach exhibits an underlying assumption that a technological imperative is at work and that public policy can only mitigate its worst effects.

2) the civil libertarian approach

The second approach to data protection is to view the problem in fundamentally individualistic terms by recognizing a right to information privacy. As aforementioned, this notion of individual's right is rooted in classical liberal doctrine and is extensively discussed in mainstream privacy literature, which had a widespread influence on the policy debates in several countries in the 1960s-1970s. In these debates, personal information emerged as a property or a resource that could not be taken or misused by government without due process of law. This line of thinking gave rise to the development and diffusion of a set of "fair information practices" whereby individuals are given some control over their personal information through some concomitant procedural rights. This includes,

> the right to see and correct personal data, the right to give consent before personal information is disclosed to other organizations, or before it is used for a purpose unrelated to that for which it was collected; and the stipulation that organizations should maintain only records that are relevant and necessary to accomplish a legitimate purpose.[60]

While Bennett notes that these principles appear in early reports on privacy, in all data protection and information privacy legislation, and in international agreements on the subject, he also feels that the inherent civil libertarian emphasis is most readily observed in the United States Privacy Act. This law, argues Bennett, derives explicitly from the principle that the right to privacy is protected by the U.S. Constitution and the perception that the "privacy of an individual is directly affected by the collection, maintenance, and dissemination of personal information by federal agencies."[61] Likewise, it only regulates federal government personal

---

[60] Colin J. Bennett, "Computers, Personal Data, and Theories of Technology," 59.

[61] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Systems and Individual Privacy* (Washington, DC: GPO, 1986), 552a, sec.2 (a) quoted in Colin J. Bennett, "Computers, Personal Data, and Theories of Technology," 62.

information practices.[62] Furthermore, the U.S. Privacy Act is also distinct from other data protection laws in that it regulates both manual (paper) and computerized files. The method of storage -- computerization or not -- is irrelevant to the perceived threat to individual privacy rights. The law also relies on the assertion of individual rights through the courts rather than on a separate policy instrument to oversee the implementation process.

To conclude, the civil libertarian approach to information privacy prioritizes an individual's relationship, in a primarily possessive sense, to his or her information. While the relationship between individuals and record-keeping organizations that represent a powerful government or private capital also looms large in the background, it is seen as mediated by records kept by public and private organizations about individuals which affect the individuals more directly. Therefore, the focus of public-policy concern has been on creating fair information practices. In the tradition of this so-called "fair information practice" legislation, the individual plays a key role in exercising the sets of rights given by law to check upon organizational record-keeping activities. The assumption is that the individual's exercise of his or her rights will create incentives for the record-keeping agencies to comply vigorously with the requirements levied on them by the law, the effect being an overall upgrading of their information management policies and practices. But according to the assessment by the U.S. Privacy Commission, these assumptions are subject to some powerful constraints particularly in the absence of an institutional mechanism for the oversight of enforcement of the law. In the realm of the federal government, which the 1974 Privacy Act addresses, the Commission finds that,

> many of the record-keeping activities within the Executive branch are mandated by the Legislature or the result of Judicial interpretations. In such instances, the Executive agency often have limited, if any, discretion over the amount of information to be collected or the manner of its use. And even when the Executive agency does have discretion, there is still no mechanism for determining whether a particular record-keeping practice or system should exist at all. In these cases, the value of the rights granted by the Privacy Act is diluted.[63]

---

[62]There are several laws in the U.S. which regulate specific private sector firms. (See in Table 6.2) Nevertheless, many private sector firms that extensively collect, use, and exchange personal information are not regulated by law, although they may have voluntary codes of conduct.

[63]Privacy Protection Study Commission, *Technology and Privacy. The Report of the Privacy Protection Study Commission* (Washington, D.C.: U.S. Government Printing Office, 1977), 43.

Indeed, the pattern of privacy legislation and enforcement in the US reflects the underlying truth about America's capitalist system, that the representation of large corporate interests tends to override intangible issues such as civil liberty and the like.

3) the institutional accountability approach

This approach views the privacy problem as stemming principally from bureaucratic pathologies. Privacy protection is seen as a means to promote bureaucratic accountability through a curbing of the power of the government, which is seen as being significantly augmented with new forms of technological surveillance. According to David Flaherty, the issue of accountability is particularly critical when it comes to government surveillance. This is because bureaucrats constitute a major source of government initiatives in information collection, under a standard assumption that more data will solve problems. Accountability, explains Flaherty, means that bureaucrats must, in one way or another, answer to the data protection agency when making decisions about information collection and use.[64]

According to Colin Bennett, data protection policy with such emphasis is rooted in the fundamental public distrust of the effects of power which includes, but is not limited to, the policymakers and administrators' handling of personal data. The valuing of privacy or the fear of computers, while present, are likely to be secondary to the citizens' skeptical orientations towards political authority, in shaping the policy debate and direction in these countries. As a result, data protection in such countries usually carries an evidently political motivation. Bennett points to the experiences of West Germany, Austria, and Canada, where a data protection/privacy agency or agent was created to act as an intermediary between the citizens and record-keeping organizations and to promote bureaucratic accountability. In some of these countries, data protection laws also include the unspoken agenda to prevent a recurrence of the Nazi and Gestapo efforts to control the population and to prevent the reappearance of an oppressive bureaucracy that might use data on citizens for damaging purposes.[65]

While lacking direct regulatory authority, data protection agencies in these countries can promote bureaucratic accountability via other means -- by reports to the legislature, by facilitating individuals' access to their own data, and by appeals to the public. In West Germany and Canada, where data protection agencies rely primarily on advisory powers,[66]

---

[64]David H. Flaherty, "Government Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." *Science, Technology and Human Values* 11, Issue 1 (Winter 1986): 9.
[65]David H. Flaherty, *Protecting Privacy in Surveillance Societies*, 373.
[66]David Flaherty defines advisory powers as "the right to give advice on personal information use." David H. Flaherty, "Government Surveillance," 9.

data protection commissioners submit annual reports to the legislature and may produce special reports in cases of complicated negotiations with data-collecting agencies. Annual reports have been effectively used as the primary vehicle for informing legislatures and the public about the state of data protection in both countries. Meanwhile, the Canadian and West German data protection agencies also help facilitate access by individuals to data about themselves in government files and intervene in cases of appeals of refusals of access. As a general guidance for the public, the Canadian privacy commissioner publishes, or at least maintains, annually updated indexes to systems of personal records maintained by government agencies. Moreover, due to the absence of regulatory power, data protectors in Canada and West Germany have to rely heavily on the threat of appeal to the public, especially through the media. This is particularly crucial in order to make the data protectors more effective in difficult situations with either a government department or the legislature.

In addition to the above channels of influence, privacy/data protection agencies in this model can also promote bureaucratic accountability through their role as information ombudsmen to receive specific complaints about data-handling practices from the general public or from legislators. Although complaints have not been numerous, this function provides a safety-valve for the concerned public since bureaucrats are aware that they risk audits and investigations launched by citizen complaints and will usually try to avoid this. According to Flaherty, the conduct of independent investigations, inspections, and audits of government information practices has proven to be an outstanding trait of data protection in West Germany, where the regulators are not burdened with the task of reviewing and licensing all personal data systems as would be the case in Sweden, France and the UK.[67]

Evidently, the institutional accountability approach to privacy/data protection is premised upon an assumption about a need to deal with the asymmetrical relationship between individuals and the bureaucracy. The creation of an independent data protection/privacy agency is a direct effort to balance privacy against other competing interests as well as to keep the power of government and other large bureaucratic institutions that collect data on individuals under reasonable control. In this relationship, the challenges facing privacy/data protection agents are massive and multi-faceted. At the most fundamental level, privacy/data protection commissioners, in the process of executing their supervisory functions, run the risk of becoming agents for legitimating information-collecting activities and new ICTs. There is also the harsh reality of power relations in which data protectors may figure merely as toothless

---

[67]Ibid., 11.

watchdogs who are squeezed between powerful technocrats and bureaucrats and powerless individual citizens.

As David Flaherty later recounts on the basis of hindsight from his first-hand experience as the privacy commissioner of British Columbia province in Canada, many of the things he wrote about a decade earlier proved extremely difficult to accomplish in practice.[68] Although he feels his office has been resourceful and vigilant in monitoring data practices, Flaherty also admits he could not stop government bureaucracies from introducing several massive cost-saving surveillance measures such as criminal record-checking and data matching for welfare fraud. His impacts and authority are inherently limited because of the lack of regulatory power. And despite his emphasis on the importance of audits and investigations, Flaherty finds himself having neglected audits, which he say have taken second place to the writing of orders on specific cases -- the main preoccupation of his office. Notably, after five years as Privacy Commissioner, Flaherty never once brings up the task of promoting bureaucratic accountability, which he earlier described as the heart of the functioning of data protection agencies.

Policy Convergence -- a Globalization of Information Privacy/Data Protection?

According to Bennett, the three approaches described above are not discrete categories that find perfect expression in any one national policy since there are clear overlaps and distinct styles of regulation that are shaped by different legal traditions and political cultures. Despite these identifiable tendencies and emphases, Bennett claims that there is noticeable evidence of policy convergence in privacy/data protection approaches, particularly in terms of content -- statutory principles -- among highly industrialized countries. The trends of divergence are said to be manifested more in the instruments that are used to enforce policy requirements.[69]

Prior comparative policy studies tend to base their policy convergence argument on the familiar thesis of development convergence, largely a product of the American functionalist school of social science. This thesis is informed by critiques of convergence assumptions at the core of the intertwining theories of modernization, industrialization, and globalization. In

---

[68]David H. Flaherty, "Controlling Surveillance." 167-191.
[69]Colin J. Bennett, "Review Article: What is Policy Convergence and What Causes It?" *British Journal of Political Science* 21 (1991): 215-233.

214

thematic terms, the convergence thesis runs as follows. As societies adopt a progressively more industrial infrastructure, they are likely to converge over time on a single set of axial principles for their social organization, hence resulting in social structures, political processes and public policies forged out of the same mould. In some interpretations, such as that hailed by post-industrialist proponents like Daniel Bell, this tendency to convergence will lead to stages of economic and political development, which will culminate eventually in a common post-industrial condition. To Bennett, such a conception of convergence, particularly when applied to comparative policy studies, not only reflects a static and overly deterministic logic but also fails to specify the aspects of policy that are supposed to be converging. Bennett thus proposes new schemes for analyzing public policy that conceptualize "convergence" as a process of "becoming" rather than a condition of "being more alike."[70] The proposed framework includes the following four processes underlying policy convergence: *emulation*, *elite networking*, *harmonization*, and *penetration*.

1) *Emulation* is described as the tendency to look abroad for solutions or how other states have responded to similar pressures and to draw lessons from that experience in the process of domestic policy-making. Typically, the policy of another country is employed as an exemplar or model that is then adapted and improved upon. Sometimes the other country's policy may also serve as a blueprint that pushes a general idea about a particular policy onto the political agenda. Emulation may occur at different stages of the policy-making process both for the country doing the emulating and the one being emulated. A number of variables may determine the nature and form of emulation, and one such factor is the timing of perceived urgency of policy in different states. The greater the perception of urgency, the greater the likelihood of imitation and solutions without lengthy analysis and investigation.

2) *Elite networking* refers to a process of idea-sharing among a relatively coherent and enduring network of elites who engage in regular interaction at the transnational level. This group of elites is identifiably bound by knowledge and expertise of a common policy problem and a shared concern for its resolution. The elites who constitute such transnational policy community primarily include, but are not necessarily limited to, regulatory experts and technocrats. Bennett stresses that convergence under this process results from an interaction and consensus amongst an elite group that operates, in the first instance, above the fray of domestic politics. Once a consensus has been reached or some form of solution crystallizes at the transnational level, the participants will then go forth to influence their respective societies

---

[70]Ibid., 219.

215

and governments by explaining what they have determined are the most rational policy remedies.

3) *Harmonization* features a process of convergence that incorporates elements from elite networking -- consonance of motivation and concern, and regular opportunities for interaction -- while also requiring authoritative action by responsible intergovernmental and supranational institutions. In this process, international organizations play a key role in facilitating cross-national learning and co-operation and in providing incentives for the avoidance of unnecessary discrepancies in public policy. The EC Directive on Transborder Data flow and the OECD Guideline on the same topic are clear examples of policy convergence through harmonization of national legislation. Besides the formal existence of an international regime, harmonization efforts also depend largely on interdependence among member countries. The efforts are more co-operative and on a more equivalent basis in nature, unlike emulation, where there is clearly a notion of leaders (policy innovators or trend setters) and followers (imitators).

4) *Penetration* is defined as a process in which states are forced to conform to (policy) action taken elsewhere by external actors. Based on this definition, penetration may appear to contrast directly with the seemingly co-operative relations under harmonization. However, as Bennett points out, certain efforts at harmonization can also have a coercive effect on states that have been slow in developing legislation in a given area. A good example is the experience of the UK in the area of transborder data flow. Since the British state was lagging behind other members of the Council of Europe and the OECD in developing data protection law, it came under pressure from the "clubs" to act or risk being excluded or other trade-related penalties.

In most cases of policy convergence through penetration, however, the penetrative agent is multinational businesses which, through lobbying and political maneuvering, have managed to secure a common regulatory framework internationally. The objective is usually to create a level playing field or to achieve comparative advantage for their products on an international front. A case in point is the deregulation of telecommunications and information-related services, which was an important issue on the agenda of the Uruguay Round of the General Agreement on Tariffs and Trade (GATT), the predecessor of the World Trade Organization (WTO). The American telecommunications industry has been the prime mover in attacks against protectionist government policies in the telecommunications sector and in mounting trade pressures against countries with such policies through multi-lateral trade

216

forums such as GATT and the WTO. The result is a convergent impact as evidenced in more open telecommunications policies in Britain, Canada, Australia, and several other countries.

According to Bennett, convergence of policy through penetration is also a reflection of power relations in international regimes. As the case of the telecommunications deregulation demonstrates, the US dominance as a hegemonic economic power and the significance of its telecommunications industry certainly account for the US efforts, through trade pressure, to pry open an international information services market. Similarly, in the area of data protection, the recently decreed EC Directive has already become a progenitor of penetrative policy convergence. Aside from the harmonizing influence on EC members, the directive also carries external impacts on the data-protection policies of non-EC states that have recently passed or have not yet passed such legislation. Colin Bennett suggests that the New Zealand 1993 Privacy Act had been heavily influenced by the early draft of the directive and so was the 1993 Quebec law. Meanwhile, Hungary, a former Communist state that wishes to seek membership in the EC, became the first country within Eastern Europe to pass data protection legislation in 1992.[71] Outside the Western hemisphere, Hong Kong recently enacted its Personal Data Ordinance in which statutory provisions are modeled after the OECD Guideline and the draft of the EC Directive. Moreover, the formerly authoritarian states like Malaysia and Thailand, which have not shown much respect for human rights, let alone the right of privacy, are drafting data protection legislation by using the EC directive as a major reference.

Evidently, Articles 25 and 26 of the EU's Data Protection Directive are the main factors of concern for countries outside the European Union. Out of fear that they will be alienated in trade and international cooperation, which have increasingly relied on globalized information exchange, governments in many countries feel compelled to pursue policies that were alien to them until recently. As more countries have joined the so-called "data protection club," the pressure to conform has increased even further for the laggards. On top of everything else, there is also the explosive power of the Internet -- today's prominent medium for correspondence, education, research and commerce -- that knows no geographical boundaries. As Colin Bennett aptly notes, "there is an increasing perception that adequate privacy protection is a necessary condition for being on the global information highway."[72]

Commercial motivation aside, there is also a psychological factor at play in the national pursuit of data protection legislation along the lines of the model EU Directive. As the

---

[71]Colin J. Bennett, "Convergence Revisited," 110.
[72]Ibid., 112.

217

majority of countries that have joined the "data protection club" are the highly industrialized liberal democracies, the adoption of data protection legislation has, according to Bennett, become associated with the "modern democratic state" -- a state of being to which many countries of the world aspire.   Since the EC directive is the latest and "most modern international consensus on the desirable content of data-protection rights," it automatically becomes "a valuable model for countries currently without data protection laws."[73] This argument is subject to more profound scrutiny, however. This is because it is questionable whether it is the democratization aspiration or the modernization aspiration that actually leads to an adoption of the EU Directive as a policy blueprint.

Nevertheless, the penetrative effects that the EU Data Protection Directive has on countries outside the EU are also subject to certain limits. Undoubtedly, the directive will extend the process of policy convergence at the level of policy content as more countries emulate its provisions in devising or updating their data protection laws. A greater conformity at the level of policy instruments -- agencies charged with oversight, enforcement and implementation of the law -- can also be expected since the issue of independent oversight may be used by the EU as a criterion in assessing the "adequacy" of data protection law in any given country. Even the US privacy law, which currently lacks an oversight agency, is expected to be strengthened as a result of the EU Directive. However, when it comes to policy outcomes, evidence of convergence may be more difficult to find. The enactment and implementation of similar data-protection laws, enforced by similar data-protection agencies, do not necessarily guarantee similar effects. As I have argued earlier in this chapter, the "right to privacy" which is the central value in this legal-regulatory framework is far from being a universal value. Conceptually, it reflects a fundamentally western understanding about self and relationship to the larger society -- one that is premised upon liberalism and possessive individualism. Therefore, the "right of privacy" may be perceived as more indispensable in western societies than in other societies. The same could also be said about the degree of significance accorded to "personal information," which constitutes an important dimension of privacy. Such perception and associated behavior are highly influential in shaping the pattern of information practice in any given society, possibly even more so than the existence of data protection legislation.

---

[73]Graham Greenleaf, "The 1995 EU Directive on Data Protection -- An Overview," *International Privacy Bulletin* 3, no. 2 (1995): 1-21, as quoted in Colin J. Bennett, "Convergence Revisited," 112.

For several countries that have recently passed a data protection law or are in the process of doing so, the emulation of this new legal-regulatory framework could be seen, at one level, as a technical attempt to cope with the EC's demand in order to sustain their economic interdependence. From a purely trade perspective, non-EC members may well be justified to perceive the controversial Articles 25 and 26 of the EU Directive as a form of non-tariff barriers with which they are being forced to comply. Besides the economic implications of the EU's Data Protection Directive, there is also the general pressure for countries to modernize their legal systems to prepare for the technological complexities of the "information age." In this light, the EC Directive may just happen to be the latest and most updated policy blueprint that is readily available for emulation.

Despite its worldwide influence, the EC directive, like many of the international data protection efforts before it, is likely to be inadequate for solving problems of privacy invasion and surveillance. While providing a rational and broadly applicable set of data protection principles, the directive is mainly aimed at restricting inaccurate, abusive, and arbitrary information practices rather than at limiting key aspects of surveillance. This limitation aside, it is important to remember that the directive was largely inspired by growing fears about computers and by the technical need to harmonize the law of trading standards across national boundaries of EC member countries and their trading partners. In this light, the conceptual meaning of "privacy" has been all but emptied of potential as a weapon in a "dialectic of control." Whether this directive will carry an impact to actually protect people's information privacy and not just legalize information practices remains to be seen.

PRIVACY REVISITED: FROM CIVIL LIBERTY TO TRADE MECHANISM

Over a period of a generation, the discourse on privacy has expanded its scope from the domains of civil libertarians to computer management professionals to international trade circles. Along the way, the aesthetic meaning of the term "privacy" has diminished as its instrumental value inflated. As Simon G. Davies, a privacy activist aptly notes, "privacy has metamorphosed from an issue of societal power relationships to one of strictly defined legal rights."[74] In the case of the EC directive, for instance, we are witnessing an example of strategic use of a category of privacy right -- that of personal data protection -- for economic

---

[74]Simon G. Davies, "Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in *Technology and Privacy: the New Landscape*, eds. Philip E. Agre and Marc Rotenberg (Cambridge, Mass: MIT Press, 1998), 143.

and technical reasons. While this conceptual shift may make an otherwise ambiguous and highly contested concept become more practical and transferrable to different cultural contexts, it is also likely to deplete "privacy" of its rich and culturally unique meanings. The liberal and democratic values that had defined privacy and placed it on the policy agenda in the West will not be perceived with the same significance in other cultures where privacy is traditionally more dispensable.

Similarly, the enactment of data protection law as a result of globalizing pressure is unlikely to create any discernible change particularly in a social environment where there is no true recognition of or concern about the right of privacy. In such settings, the passing and implementation of a data protection law will be like paying lip service to another international mandate. Social behavior and organizational culture do not change overnight and certainly not by a top-down imposition of a new policy whose central concept is utterly unfamiliar to the majority of the population. Privacy and data protection are undeniably a learning process and ones that can take a long time for people to realize as the effects are not immediately visible, yet subtle and pervasive.

CONCLUSION: A MULTI-FACETED APPROACH FOR A STUDY OF INFORMATION PRIVACY IN THAILAND

While the simplest way to conceptualize "privacy" is to place it at the opposing pole from surveillance or to view its protection as a defense against surveillance, the truth remains that "privacy" is a social, cultural, and legal concept, all of which vary from country to country. Also, as the account in this chapter has shown, the protection of privacy through legislation and public policy does not necessarily strike at the core of surveillance problems, and in some cases it may not even be inspired by concerns about the augmenting of powers and authority associated with surveillance.

Certain problems of definition are bound to occur in an inquiry about "privacy" that draws upon the experience of a society quite antithetical to the western notion of privacy like Thai society. To make such an inquiry manageable, I find it necessary at the start to block off my personal bias and predisposition that might have been tainted by years of exposure to western ideas and culture. It is not my definition and understanding of privacy that matters in

this study; it is what members of Thai society feel about issues relating to privacy, especially information privacy, what they have done about them, and whether they have even been concerned about these issues at all. Due to time and financial constraints, I decided to learn about these conceptions by carrying out five focus group interview sessions on the topic of information privacy and government databases in Thailand. Drawing on the idea of cultural and class-based relativism in perception of privacy in the literature review, I postulated that socio-economic factors play an important role in shaping the focus group participants' attitudes and behaviors towards privacy, and I used this as a main criteria in selecting focus group participants. The detailed methodology of the focus group interviews and its rationale are discussed in Appendix 2, and the next chapter provides the focus group results.

Besides the focus group sessions, I, following the framework set out by Barrington Moore and James B. Rule, also examined the largely limited and fragmentary anthropological evidence about privacy in Thai society to learn more about the range of known behaviors related to privacy in the Thai context. Alongside, an inquiry into plausible philosophical basis of these behaviors is undertaken. For the most part, I have concentrated on Buddhism and the historical development of "rights" in Thai society. Liberal democratic concepts that underpin the western understanding of privacy are also examined in an effort to assess their compatibility with the Thai political and cultural context. Furthermore, the concept of "rights" in Thai society is juxtaposed with changes in the country's economy and polity, focusing in particular, on the recent political reform and the promulgation of the new constitution in 1997. These findings, together with results from the focus group sessions, are essential to develop a conception of privacy rights in the Thai context.

In addition, a detailed analysis into the legal-regulatory framework of privacy and data protection in Thailand is undertaken. In this part, I rely on an institutional analysis similar to the one used for the analysis of state surveillance in part one. The role played by local economic and government institutions, international organizations, local NGOs, academics, and local citizens in shaping the emerging regulatory scheme for government information practices and general personal data protection is analyzed. Much emphasis is given to the penetration of global policy networks, local policy elites' fervent aspiration for an information-oriented modernization, and the rise of a more liberated information sphere as checks and balances to the bureaucratic polity.

CHAPTER 7

PUBLIC PERCEPTION AND EXPERIENCE
OF INFORMATION PRIVACY IN THAILAND:
A FOCUS GROUP REPORT

This chapter is a summary of results from five focus group interviews carried out to explore the perceptions and experiences related to privacy of subsets of people from different socio-economic groups in Thailand. The reasons why focus group interviews were selected as a methodological tool, detailed discussion on the method, as well as the recruiting of participants are discussed in appendix 3. The following summary provides the list of questions administered in the group interviews, the characteristics of the focus group participants, and the results of the group interviews.

THE BIG QUESTIONS AND QUESTIONING ROUTE

The biggest and central question in this chapter is: how do selected subsets of the Thai public understand and experience "privacy" particularly "information privacy"?

As suggested by many writers, a person's conception of privacy is culturally relative and dependent on his or her socio-economic position.[1] In a society like Thailand which is primarily dualistic in nature, and where privacy is not a prevailing social value, this consideration is particularly relevant. Therefore, I decided to add this class-based dimension to two sub-questions to the above and to use it as a criteria in recruiting participants to the focus groups.

1) What do the selected participants in different socio-economic groups consider as "privacy" and "information privacy"?
2) How do the selected participants in different socio-economic groups view their status of "privacy" particularly "information privacy" in contemporary Thai society?

Although topics for the discussion were carefully pre-determined and sequenced into a plausible questioning route, it was not possible or desirable to follow the exact same line of

---

[1]See. for example, Colin J. Bennett, "Regulating Privacy." 13

222

questioning for all the sessions. The varying responses from participants in different sessions made it necessary to adjust the questions accordingly to pertain to their understanding of the issue being raised. This was particularly true with the participants in the lower socio-economic group. Some of the pre-designed questions about privacy were entirely irrelevant to their experiences, and they were in no position to answer them. Overall, however, the questions asked in the five focus group sessions largely included the following:

1) Have you or anyone you know ever experienced an intrusion of "privacy"?

2) What do you think of when we mention the word "privacy."?*[2]

3) How do you draw a line to determine when one's privacy has been encroached?**

4) What do you think the government is using your personal information in civil registration files for?

5) Do you feel the government's rationale in collecting information about citizens for personal identification and civil registration purposes is justified? Should there be limits to such collection?

6) The Ministry of Interior has since 1982 computerized its massive civil registration database and is now completing on-line civil registration information network nationwide. Other major record-keeping government agencies either have recently completed or are in the process of computerizing their databases. How do you feel about this widespread computerization of citizen information?

7) A consortium of Thai bureaucratic agencies are currently contemplating developing a new personal identification system in which a microchip card will be used to store all types of crucial personal information about the citizens. The various ID cards -- personal identification, driver's license, revenue, health care and social security -- will be merged under one single card while the databases of these different organizations will be interlinked. How do you feel about this project?

8) Do you feel that you have the right to know when your private information is made known to others whom you did not directly release the information to?

---

[2]An asterik (*) indicates that the questions were used only for participants in the lower socio-economic groups while a double asterik (**) indicates that the questions were raised only in the sessions with the upper and middle socio-economic groups. Questions with no asterik were used in all sessions.

9) What do you think are the citizens' rights in protecting their own personal information?**

10) Do you feel individual's privacy is adequately protected in Thailand? If not, who or which institution do you think should be responsible for promoting people's right to privacy?

11) Do you think there is really an alternative to the present situation in Thailand in terms of protection of personal data?**

In all sessions, I tried to ask the questions in the numbered order, starting with the general notion of privacy to the specific notion of information privacy. This sequencing was determined by an informal pilot test I did with a few colleagues at Chulalongkorn University prior to the first session. All the colleagues agreed that for a topic that is so "far-fetched" to Thai culture as privacy, it is reasonable to begin exploring in the broad scope before narrowing to a specific area of concern.

THE FOCUS GROUPS PARTICIPANTS

A total of five focus group sessions were organized. The size of each group ranged between 7-9 persons. As earlier mentioned, the selection of participants in each focus group was based on the presumption that a person's sense of privacy depends on one's culture and socio-economic position. In the recruitment phase. I tried to achieve a reasonable homogeneity in the participants' socio-economic background and age group while striving for diversity in other areas -- profession, education, and ideological predisposition. As will be discussed below, I was successful at controlling these factors in some groups and not others. It should be noted also that the determination of socio-economic group was based not only upon income but also on other factors including level of education, occupational status, and family background. As most of the participants were recruited through a peer referral system, I was somewhat familiar with their backgrounds and was able to evaluate, with little difficulty, their socio-economic grounding.

Out of the five groups, two were comprised of participants who belong to the middle to upper socio-economic group. The average age of one group was about ten years higher than the other, however. The participants in these two groups come from various educational backgrounds -- medicine, law, police, political science, business, engineering, natural science, literature, journalism, and mass communication. They also brought with them

diverse professional experiences from their work in academia, government bureaucracy, financial sector, the media, industry, as well as non-profit non-government organizations. The breakdown in the participants' demography -- the level of education, profession, age, gender as well as their exposure to Western culture -- is provided in Table 7.1. Some of these participants were friends and acquaintances of mine but they were from different peer groups. Most did not know each other before. Others were people I had developed personal relationships with during the site visits to the Police Department and the Ministry of Interior in the earlier stages of the field research.

I recruited the participants in these first two groups through a telephone screening. I drew up a list of potential participants and called up each one two weeks prior to the planned focus group session. I informed them about the topic and the objective of the research, the nature of the group interview, and the date, time and place where the session was to take place. Out of a list of fourteen persons, I was able to get an agreement to participate from nine persons for the first session. I overrecruited a little as I was aiming at seven or eight participants. In the end, eight actually showed up at the session venue in the conference room of the Faculty of Communication Arts, Chulalongkorn University, Bangkok. I followed the same method for the second group session and was able to receive an agreement to participate from eight persons. For this latter session, all the recruited participants showed up at the meeting venue.

Aside from the two groups above, two other groups were strategically recruited from the lower socio-economic group to contrast with the first two groups. I was unable to screen the participants in the latter two groups through a telephone conversation as none of them had a telephone at their home. For the third group session, I recruited the participants through a personal connection. Thanks to a friend who owns a restaurant, I was given permission to recruit her employees to participate in this group interview.[3] After obtaining consent to participate from all seven employees, I set up the time of the meeting during one of their afternoon breaks. For convenience, I also organized the restaurant, which was closed in the afternoon, into a meeting venue. Tables and chairs were rearranged into a U-shaped circle to facilitate the group seating. The seven participants included a cook, an assistant cook, three waiting persons, and two cleaning workers. All were from rural provinces and were, at one point, farmers.

---

[3]Each participant was promised Bt250 (about US$4) for spending one and a half-hours in the focus group session.

Table 7.1: A breakdown in selected attributes of participants in each of the five focus group sessions

Group	Age group	Gender	Education	Income level	Extensive exposure to Western Culture
1	24-30	three females, five males	university and post-graduate	medium-high	five out of eight have spent time studying in North America
2	35-40	six males, two females	university and post-graduate	medium-high to high	five out of eight have spent time studying in the U.K. and North America
3	25-40	three males, four females	grade four to grade six	medium low to low	no one in the group has spent any time overseas
4	30-48	three males, four females	grade four to grade six	low	no one in the group has spent any time overseas
5*	29-53	two males, six females professionals have gone	grade six to post-graduate	medium low to medium who were health	two of the participants for a training course in Australia and the US

* Participants in this particular group are exceptional in their composition. The group comprised a few health officials -- nurses, doctors, psychologist and health specialist -- as well as a few AIDS patients and HIV-positive persons. While they were not necessarily homogenous in the general demographic attributes, they share a common experience in handling sensitive health information

None had completed high school but all finished the compulsory level of education in their time.[4] As mentioned before, it was impossible to maintain a sense of unfamiliarity among the participants in this particular group since they worked so closely together. Similarly, in the other lower socio-economic group, the fourth group session, five out of the seven participants worked as construction workers for the same company and have been friends for some time. The other two in the group were security guards working on the construction site. Similar to the third group, these participants were migrant labor from the rural provinces. The construction workers were seasonal farmers and usually returned to the fields, if possible, during harvest time. I recruited the seven participants in this group also through a friend's personal connection. The group interview session took place at a front yard of this friend's house, which was next to the construction site where the participants worked.

The fifth and last focus group session was unlike any other group. The notable difference was that half of the participants in this group were people who have tested HIV-positive and are suffering from the various stages of AIDS (Acquired Immune Deficiency Syndrome). The rest were health professionals -- nurses, a physician, a counsellor, a psychologist -- who have worked closely with AIDS and HIV-positive patients. This focus group interview took place in Chiang Mai province, where the participants reside and where the number of AIDS and HIV-positive cases are the highest in the country. It was not until the other four focus group sessions in Bangkok were completed that I decided to pursue a focus group study of AIDS patients and health personnel in Chiang Mai on the same topic. Unlike the participants in the other sessions, these HIV-positive and AIDS patients in Chiang Mai have all the reason to be apprehensive about privacy because of their vulnerability and their desire to keep their personal information strictly confidential. Their attitudes, opinions, and personal experiences in protecting their personal information are deserving of a study not only for this reason but also because their insights could reveal the perception and behavior of people from a non-urban setting. I was able to recruit the participants for this group, at quite short notice, through the help of a family friend who is the director of the center for communicable disease control in Chiang Mai province. Aside from posting an advertisement at the center's bulletin board about the planned focus group interview, this friend also helped encourage some of the more active and articulate members of the "For a

---

[4] Most of the participants finished grade four, which was the compulsory level of education when they were attending school. The youngest participant, who was twenty five years old, finished grade six, which became the new level of compulsory education when she attended school.

new life" club, a community counselling group for AIDS and HIV-infected persons, to join in the discussion session.

THE FOCUS GROUP INTERVIEW

In the beginning of each group session, I would introduce myself and explain briefly my objective in conducting the focus groups interview and why each participant was recruited to participate in the process.[5] I did not mention any predisposition I might have about each group of participants' attitudes towards privacy lest anything I said would be misleading. Appendix 4 is my "opening speech" before throwing the first question on the table. This first question was the round-robin question that everyone answered at the beginning. I asked whether each participant had ever experienced any form of intrusion of his or her privacy. The term "privacy" was not defined but left open for the participants' own interpretation. As the answers were solicited from all participants for the first question, I listened attentively, made notes, before going down the list of the other questions. The session typically lasted from one and a half hour to two hours. All the sessions were recorded by an assistant moderator whom I had interviewed and selected from a group of graduate students in Journalism at Chulalongkorn University. Besides making sure all the equipment -- microphones, cassette recorders -- worked properly, the assistant moderator was also responsible for taking complete notes of the conversation during all the sessions.

Throughout all the sessions, I tried to exercise a mild, unobtrusive control over the group. Probing was infrequent as I maintained it was more important to hear from all participants within the limited timeframe rather than letting a few participants dominate the session.[6] If a participant raised a very interesting point that I thought should be clarified further or a participant appeared uncertain about what he or she had to say, then I would probe. Often, irrelevant topics were introduced by participants, and I had to carefully guide the conversation back to the target. It was more difficult to do so in some sessions than others. The second group session, which was comprised of participants in the upper socio-economic group in the 35 - 45 age group, was the most difficult to control. This is because all participants were very enthusiastic and would get into a passionate debate about certain issues relating to privacy, leaving little room for interruption. On the other hand, the

---

[5] It should be noted that all five focus group sessions were conducted in Thai.
[6] Despite my effort to prevent this from happening, this was exactly what happened. The more senior participants in the group or those with more experience or background in the topics being discussed were always the ones dominating the conversation.

participants in the construction-workers group appeared quite unenthusiastic about the issue of privacy and would always bring the discussion back to issues reflecting their central concerns such as poverty and inadequate government assistance. It was sometimes difficult to try to interrupt and bring the discussion back on topic while making sure the participants realized their input was respected no matter what their level of education, experience, or background.

In addition to my limited control over the flow of the conversation, there was also the problem of unavoidable leading. In the session with the participants from lower socio-economic group, for instance, after the first question was raised, there was a long pause and empty look on the participants' faces. I was asked to provide them with some examples as they did not understand what "privacy" really meant. The situation presented a dilemma to me as a moderator who understood little of the culture or the environment of the target participants but had to lead the discussion without overtly influencing their thoughts with my ideas and perceptions of things.

THE RESULTS

The results of the five focus group sessions will be organized around the key questions, which are in turn grouped under the rubric of big ideas as follows.

On the conception and understanding of privacy

- Have you or anyone you know ever experienced an intrusion of "privacy"?
- What do you think of when we mention the word "privacy."?
- How do you draw a line to determine when one's privacy has been encroached?

In the first two group sessions -- the upper and middle socio-economic group, the participants spontaneously recounted stories of how they or someone they knew experienced some form of intrusion of privacy ranging from telemarketing and direct marketing to probing intelligence inquiry for employment in the civil service. A couple of participants in the second group, one a physician and the other a personnel manager, admitted they might have unintentionally encroached upon other people's privacy in their line of work. Most participants in the first two groups agreed that Thai people tend to take intrusion of privacy lightly. While some people might feel more irritated than others from telemarketers' calls,

the chances of an individual filing a lawsuit against someone who might have crossed what they consider a "privacy" borderline is very slim.

The discussion dwelled for some time on this issue of how one can determine if one's privacy has been encroached. One participant in the first group, an engineer by training, argued that names, addresses and telephone numbers are not necessarily private information since they appear in telephone directories, which are public resources. In rebuttal, another participant, who is a young district judge, argued that the fact that such information appears in such publications does not mean it is not private. The key criteria, he argued, lies in the objective in using the information. If a piece of personal information is being used for a purpose different from what is originally intended by the data subject, then it can be considered an abuse and, thereby, an invasion of privacy. Interestingly, this judge who tended to dominate the discussion with his legal insights also gave a meaning of "privacy" as "the right to be let alone" following the classic definition given by Samuel D. Warren and Louis D. Brandeis in 1890.[7] Meanwhile, a couple of participants, one from each of the first two group sessions viewed privacy more from a moral dimension. According to these two participants, a recognition of someone's privacy stems from a respect of that person as an equal and dignified human being. It merits mentioning that both of these two participants were educated for an extensive period of time in the US and England.

Unlike the first two groups, in the third and fourth group sessions -- the lower socioeconomic groups, the participants were generally unsure about their understanding of privacy. After being asked about their personal experience of privacy, there was a long pause and uneasy laughter from the participants in both group sessions. The moderator had to probe by asking what they regard as "privacy," but the participants were still uneasy and inarticulate. Finally, the moderator had to lead by providing the general notion of privacy before answers could be elicited.[8] Interestingly, the first thing that was mentioned in association with the participants' understanding of privacy in both groups was finance or their financial condition. As will be discussed later, the issue of finance, which directly reflects their personal insecurity, would come up consistently in the discussion. Interestingly, however, the participants in the lower socio-economic groups did not seem to feel as threatened about their privacy or what they perceive to be "privacy" as the former two groups. In the third group session, for instance, the female cook, who dominated the

---

[7] Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 193 (1890) : 193.
[8] After this long and uneasy silence, I broke the ice by helping define "privacy" as "the ability to be let alone without intervention from others and the ability to determine for oneself which personal information one would rather keep to oneself or within one's immediate circle rather made known to others."

discussion, was resolute that it is up to each individual to protect his or her own personal privacy. Her understanding of privacy, when probed, was largely equated with personal secrets. When asked specifically if she ever felt her privacy was encroached, she replied, "if we don't mention our secrets to others, how in the world would anybody know it?"

As for the fourth group session, despite the moderator's consistent effort to redirect, the conversation always revolved around the issues of finance and material necessities.[9] A senior female construction worker, who was the most outspoken in the group, set the tone for the entire session with her remark that "financial constraint is most directly the matter we want to keep to ourselves as it is the most crucial thing in our lives. Without money, we would not be able to do anything." When asked if there is anything else aside from money that the participants would value and prefer to keep to themselves, the participants went silent. Two participants admitted it was difficult to answer and that they did not know how to respond. One participant asked the moderator to provide an example. I pointed out possible examples such as romantic affairs, medical information or something that could possibly be construed by others as their vulnerable point. The outspoken female participant retorted that her most identifiable vulnerability is her desperation to keep the family together. In this light, she regarded as an intrusion of privacy the event in which an outsider has an influence on their ability to feed the family and to keep them together. Other participants nodded in agreement and elaborated further. Their comments went along this line: they were once farmers in rural provinces but were forced to leave their family behind and came to Bangkok because of the drought in their farmlands. Even now, their wages from being construction workers were too low to cope with expenditures such as food, shelter, and their children's tuition. So they feared that their family lives would be disrupted again because the pressure to make ends meet might force them to be apart. One of the male participants, who was less outspoken, cited an incident in which someone 's "privacy" was violated by his peers at the workplace. According to this participant, the violation of privacy took place when fellow construction workers reported to the boss about other construction workers' complaints about their financial constraints. As a result, the complaining construction workers were fired as the boss saw them as potential instigators who could cause widespread dissatisfaction among the workers and possibly a labor uprising. "We have to be really careful when we discuss or complain about financial constraints now. We can't really talk

---

[9] It is, perhaps, important to note that the participants in the fourth group were the most economically destitute. As construction workers and security guards, they were able to earn a minimum wage of Bt120 (Can$6) daily which would amount to about Bt4,000 (Can$200) per month. Job security and fringe benefits were also minimal. Although shelter is provided by the construction company, it is only temporary until the construction project is completed.

about it anymore for fear that we might get fired too. It is a very sensitive issue," said the participant.

With regard to the fifth group session, there was no need to define for them what "privacy"was. Both the health professionals and the HIV-positive participants said that they encountered some form of intrusion of privacy almost on a daily basis in their line of work and activities. One of the participants, who is a middle-aged nurse, admitted that she never fully realized the meaning of "privacy" and "right to privacy" until she came to work with AIDS patients and HIV-positive persons. AIDS, she said, is a sensitive matter and yet people are still behaving quite insensitively when it came to dealing with the infected persons or their personal information. Other health officials participating in the group also recounted incidents where strangers would come in to the center and ask to see "AIDS-infected persons" for reasons ranging from academic research, news reporting, to sheer curiosity. According to one of the health personnel, these intrusive visitors, many of whom were westerners, considered AIDs-infected person almost as some sort of exhibits.[10]

The violation of privacy did not come from outsiders alone, however. Some of the health surveillance practices conducted by the Ministry of Public Health had also in the past violated many AIDS patients' right to information privacy. According to an AIDS patient, even when the Public Health bureaucracy guaranteed that HIV-blood test results would be confidential, there was in the past rampant breaching of confidence and relating of information to unauthorized persons. Citing her own personal experience, this patient said she went through the trouble of getting her blood test at a city hospital in downtown Chiang Mai, a long distance from her village, so that no one would recognize her. Nevertheless, the test result, which came out positive, found its way back to her village as the community hospital officials and village health volunteers one day contacted her and asked her to come in for immediate counselling. Regarding this matter, a medical doctor and a health official apologetically admitted that the dissemination of health information as such was part of the public health ministry's information network system to keep the spread of communicable disease under surveillance and to render the needed home care to contacted patients. A nurse asserted that she felt very uncomfortable with this system, particularly when sensitive information about patients was carelessly photocopied and distributed from one health center

---

[10] An AIDS patient humorously asserted that some visitors acted as if they were going to the zoo when they were paying a visit to the "For the new life center," which is a community-based counselling and rehabilitation organization for AIDS-infected persons. This patient said he had now gotten used to people asking questions such as "what stage of AIDS are you now?" Or "how many years do you have left?"

to another. "Sometimes I was the one who signed the report, and the fact that the report carried my stamp and signature made me feel personally responsible," she said.

On government surveillance and computerization of citizen files

- What do you think the government is using your personal information in civil registration files for?

The participants in the first two group sessions were not as spontaneous in their response to this question as they were with the question regarding their personal experience of privacy. After pondering for a moment, a few participants in the first group session came up with lists of official uses of civil registration files such as population statistics, electoral listing, means to distinguish Thai nationals from immigrants, and tracing of a citizen's whereabouts for crime investigation purposes. As the list became exhausted, one of the participants in this group noted that these systems exist more for bureaucratic control of the population by the state rather than for public services. A few other members in the group agreed and admitted that they had never really given it much thought in this way before. One participant began complaining about how irksome it is to have to supply photocopies of personal ID and household registration documents for almost any semi-formal to formal transaction. Others followed suit with complaints about the unpleasant bureaucratic red tape in most district civil registration offices and the rampant inefficiency which usually results in unnecessary delay in issuing or processing certain documentation. According to one participant, "I always feel small every time I have to go to the district registration office for any paperwork unless when I have some connection that could bypass their annoying red tape."

While participants in the first group only raised questions about the objectives and the inefficiency of civil registration and personal identification systems, some of the participants in the second group session went further to question the justification and political implications of these systems. A few of the participants in the second group, who were openly liberal in their political standpoint, were very critical about the historical existence of the systems.[11] For instance, one participant who is a journalist, plainly called the two

---

[11] To recap, the participants in this group were mainly middle-level professionals in the thirty-something to forty-something age group. They are from various backgrounds such as political science, law, journalism, public policy, science and medicine.

233

systems government schemes of social control. He argued that such large-scale documentary systems have long thrived in Thailand without any viable dissent because they have always been rationalized and legitimized on security grounds. In his words,

> The public did not question these governmental practices, which would have been out of the question in many countries, because they felt the reason was justified. But even after the cold war and border crisis have pacified, the same legitimacy ground continued to be used and became embedded in Thai political culture. Many illegal surveillance practices such as wiretapping on political figures continued to be carried out in the name of national security. So, despite the supposedly more secure and more democratic context of the present political regime, certain forms of government surveillance are said to be necessary and citizens are expected to sacrifice a certain degree of their privacy in exchange for the so-called *public peace and well-being.* (emphasis added)

In addition, this participant, who notably has spent years in Britain, is also critical of government information-handling practices, which he sees as non-transparent. "Access to official information is always reserved for the powerful status quo like powerful bureaucrats, politicians and their business associates. The press or a common citizen still have very limited access to most official information."

As for the third group session (the construction worker group), most of the participants were not the least critical of the civil registration and personal identification systems. They viewed these systems entirely at face value and even felt that the systems exist for good reasons. For instance, a few participants mentioned crime prevention and protection of citizens from labor infiltration by illegal immigrants. Most seemed to agree that these systems are useful public services provided by the government and that all "good" citizens must comply with them. However, one participant who is a young man working as a security guard admitted having had doubts about the legitimacy of government use of his private information in civil registration files. But since he knows of no means nor channels to challenge it, this participant said he just feels obliged to go along with the system.

Similarly, in the fourth group session, most of the participants also unquestioningly saw civil registration and personal identification systems as useful public services provided by the paternalistic bureaucracy. According to one participant who dominated the discussion, "these systems exist to make things right. The bureaucracy enforces the systems on our behalf." Accordingly, other participants tended to view compliance with these bureaucratic schemes as a duty for a good citizen. For instance, a couple of more senior participants explained their willing compliance "because the law said so, we have to follow

them." They even viewed the possession of ID cards and household registration cards as a form of passport that makes formal and official transactions more convenient. "Like when we have to send our kids to school, if we have the proper documents -- household registration and personal ID cards -- readily available, things become much easier," was one of the remarks made.

- The Ministry of Interior has since 1982 computerized its massive civil registration database and is now completing on-line civil registration information network nationwide. As we speak, a consortium of Thai bureaucratic agencies are contemplating a plan to develop a new personal identification system in which a microchip card will be used to store all types of crucial personal information about the citizens. The various ID cards -- personal identification, driver's license, revenue, health care and social insurance -- will be merged under one single card, while the databases of these different organizations will be interlinked. How do you feel about these new developments?

Most of the participants in the first group session were surprised to learn that the computerization of the Ministry of Interior's civil registration databases has been in place since 1982. While many participants voiced their concern about the potential threat to privacy from such large-scale computerized record-keeping, they remained vague in their comments about adverse impacts of the project. Then, one participant, a police official, spelled out the interconnection between government database systems and the relatively loose protection of access to these systems. This police officer participant also recounted how his police peers would habitually look up records of certain individuals as a favor for friends and families through the on-line terminal connection that links the Police Department with the Registration Administration Bureau's database. The participant who is a district judge voiced a similar concern -- threats to privacy and information abuse -- and elaborated on the many ways in which a licensed lawyer can get access to information in civil registration files even when s/he is not supposed to. In his words,

> By decreeing "stakeholder" as persons entitled to information in the file, the law opens way for many forms of abuses to citizen information since the term "stakeholder" is fairly vague. Besides, since the bureaucratic officials who handle requests are usually inundated with workload, they have to operate on common sense rather than legal sense and thus would not take enough time to thoroughly check the requests and supporting documentation. Often, a shrewd lawyer would request to look up someone's record by falsely adding that person's name to a subpoena and submit it as

part of the request. The official at the data provision section would not know the difference and would most likely grant him or her access to the file.

The judge's comment opened the way for a wider debate on legal safeguards on privacy and the accountability of the Thai bureaucractic officials in handling sensitive citizen information. (For the sake of coherence, however, this part of the discussion which overlaps with another set of key questions will be dealt with in the next section on right to privacy and data protection.)

One participant who is an engineer by training raised an interesting point about technological diffusion in a developing country like Thailand, citing the widespread computerization in the public sector. According to this participant, in adopting the new technology, Thai organizations have made no or little effort in adopting the social framework surrounding that technology or technological system. He was referring specifically to technical and legal safeguards as well as a preliminary feasibility study, which would have been commonplace in a western setting. Thais, he argued, are usually and easily fascinated by new technologies as evidenced in their spontaneity in adopting the technologies without considering the consequences. "It is difficult to say whether they really blindly believe in the power of technology or they just do it for the sake of being modern. Perhaps, both."

As far as the planned microchip card is concerned, however, two diverging views were apparent. About half of the participants in this first group session said they would not mind a single card that would contain all the crucial information about themselves so long as there are adequate technical and legal safeguards in place. This group of participants said they found the convenience of carrying only one multi-purpose card appealing. The other half admitted they were too skeptical of the bureaucracy's ability to maintain sufficient data protection measures. A few voiced serious concern about the possibility of all their personal information be stored in one card.

As for the second group session, participants were even more earnest in debating the implications of the new computerized databases. Although privacy was first raised as the viable impact of such development, the participants did not really delve into the issue of privacy or data protection per se. They were more interested in the political dimension, particularly how the new technologies would help increase the political power of the bureaucrats and politicians vis-a-vis the citizens. Participants in this group actively exchanged their opinions on the basis of their knowledge and expertise. For instance, a

participant who is an official at the Ministry of Interior explained that the computerization and interlinking of databases of citizen information were carried out mainly to increase the efficiency of the system and to facilitate the exploitation of information for wider purposes. "The objective is simply to systematically maximize the use of existing resources. So, it just never struck the planners of this upcoming civil registration information network that data protection should be a major concern." This official was also sincere enough to admit that the Ministry merely pays lip service to data protection as evidenced in the very loose enforcement of their rules and regulations in their data-handling practices. "Anyone who knows the data entry operator can get information about anyone they want. It is that simple," he remarked.

Meanwhile, another participant, a lawyer/activist, argued that the interlinking of databases and any further computerization plan would only help reinforce and enhance the power of the status quo. According to this participant, the wealth of information contained in civil registration files has always been used and manipulated to stabilize the power of the dominant group at the expense of the less privileged. He pointed out how information in the electoral listing file has become such an essential tool in vote-buying and vote-canvassing particularly in the rural provinces. Under a sophisticated election fraud scheme designed by provincial politicians and local administrators, electoral rolls are widely used to identify the target voters in small districts and villages. Peasant villagers are thus kept under surveillance by these corrupt politicians and district or village administrators who would directly affect the channelling of resources to the areas in accordance with the proportion of votes received. If any village turns out a number of votes lower than targeted by the vote canvasser, chances are that that village will not receive the necessary infrastructure in the future -- fresh water, electricity, telephone lines, etc. In some cases, corrupt politicians and the conspiring local administrators would even be able to identify who did and did not vote for them. As this participant puts it, "if you cannot expect confidentiality in the ballot box, forget the large databases," he asserted.

While the topics of computerized database and microchip ID card stirred up a lively discussion in the former two groups, things were quite different in the third and fourth group sessions. The interest in the topic was noticeably low and some participants appeared quite uncomfortable to respond to questions about which they had little knowledge. In the third group session, only one participant, a young female construction worker, recalled having heard on the news about the project to computerize transactions at civil registration offices. However, she admitted that she had no interest in it since she did not see how this new

development would directly affect her life. The other participants in the group admitted having little knowledge about computers, and they tended to see its widespread application as an evolutionary path of development. A few mentioned higher efficiency and faster services as benefits of computers in records-keeping. With regard to the planned interlinkage of databases of different public organizations and the new ID card, no one seemed to mind. A few even supported the idea mainly for reasons of convenience.

In the fourth group session, all participants admitted that the computerization of civil registration databases and the proposed microchip ID card were all new knowledge to them. Like the members of the former group, they too did not think these developments would affect their lives in any significant way. One participant, a middle-aged female cook, said the computerization project would have more impact on the bureaucratic agencies than on the people and that the effects would most likely be positive. "Otherwise they would not do it. It is probably going to make it more convenient, As for how, I don't really know, and I don't understand." A few other participants also agreed with the positive effect notion. One participant, a cleaning worker, mentioned an increased capacity to verify the identity of criminals using computers to match fingerprint records while another, a waiter, mentioned potential benefit for the cardholding citizens in cases of card loss or damage. "If everything is on computer, I believe it will be much easier to replace the card. It is quite a hassle now to replace a lost card with all the bureaucratic red tape." This same participant also supported the idea of the future ID card, which he believed could facilitate many other useful applications. According to this participant, being a migrant labor from another province has made it difficult for him to cast his vote during election times. Since he had to be physically present at the ballot station in the constituency where his name is registered, he often missed a chance to vote because he could not take time off from his work in Bangkok. "I would vey much like it if the new card came out like a credit card and I could use it to vote from a distance. That way, I could save the time and expenses of travel if I need to do any transaction from afar."

As for the fifth group session -- the HIV-positive patients and health workers group, the participants were divided in their opinions about the computerization and interlinking of public databases of personal information and the planned microchip ID card. A few participants were ambivalent about the new plans. They supported the increased efficiency and convenience but had reservations about access to the database and data confidentiality. A participant who is a nurse suggested that there be restricted levels of access to information in both the databases and the new ID card to prevent abuses. Another participant, a man who

has tested HIV-positive, urged that a public opinion survey be carried out first to assess people's views toward the new ID plan. Although he liked the idea of a multi-purpose ID card, this participant stressed the important fact that some people are more vulnerable than others in terms of their personal information. In the meantime, another participant, also an HIV-positive person, was entirely opposed to the proposed interlinking of databases and the new ID card. Not only did she view the rationale for more information as unnecessary, she also argued that more information was bound to be lead to more discrimination. Talking from personal experience, this participant pointed out how, even in the present circumstances in which less information is being passed around, the social stigma against AIDS-infected persons is already high. "The new ID would only help to make AIDS-infected people become more easily identifiable and transparent. Who knows, discrimination might run so high AIDS people may have to set up their own colony then," she commented.

On the right to privacy and data protection

- What do you think are citizens' rights in protecting their own personal information?
- Do you feel individuals' right to privacy is adequately protected in Thailand? If not, who or which institution do you think should be responsible for promoting people's right of privacy?
- Do you think there is really an alternative to the present situation in Thailand in terms of protection of personal data?

In the first group session, participants viewed the right of privacy primarily in two dimensions -- legal and moral. On the legal plane, a few participants voiced their concern that the existing law and public policy are inadequate to cope with technological changes and to ensure bureaucratic accountability in the protection of personal data. The participant who is a district judge disagreed and argued that the right of privacy is already guaranteed under the Thai constitution and other laws. The problem, he said, lies in the lack of enforcement of the law and the public unawareness of their legal rights. As for the moral dimension, three participants maintained that the issue of privacy boils down to a moral problem. Due to the general lack of respect for human autonomy and dignity in Thai society, bureaucratic officials who are in charge of handling the citizens' personal information do not have genuine respect for the confidentiality of the data. They also do not feel obligated to limit the uses of the data only for the purpose for which it was collected. This general lack of respect for human dignity, said one participant, also accounts for the widespread corruption involving

manipulation of civil registration data, while the deeply-entrenched patronage system is seen as the culprit for selective treatment and services.

Meanwhile, participants in this group did propose several ways to promote the right of privacy in Thailand. Participants in the legal and law enforcement professions stress the importance of bureaucratic accountability. To achieve this, the police officer participant proposed establishment of a disciplinary entity which could monitor and impose disciplinary measures on bureaucratic officials in cases of misconduct or mishandling of public information. The participant who is a judge argued for a more stringent enforcement of existing laws and a campaign to provoke the bureaucrats' good conscience when it comes to handling citizen's personal information. Two participants who work in the private sector argued for establishment of a non-profit, non-governmental organization comparable to the pollwatch committee, which was set up four years ago to act as a watchdog for the notoriously corrupt election process in Thailand. Yet, these participants also felt that such an organization was most likely to be powerless and unable to withstand the powerful network of control of the bureaucrats and politicians. An NGO worker and two university professors agreed that the problem of privacy protection, like many other social problems in Thailand, is fundamentally a moral problem. In their view, so long as privacy was not a value respected by most people in society, the issue would not appear as problematic. One participant responded, "Therefore, a gradual inculcation of values and a promotion of public awareness on the issue has to be carried out on an extensive basis so that people will be educated about their own rights to privacy and to their own personal information."

In the second group session, most of the participants agreed that the right to privacy is not recognized equally and in the same way by different social groups in society. The peasants and the working class, in particular, are considered to have a vague understanding of privacy. As far as information privacy is concerned, one participant, a scientist with an elite background, asserted that the working class people possiby do not consider their personal information as something valuable and worth preserving. In this light, another participant, a corporate executive with backgrounds in political science and public policy, asserted that since privacy is not a fundamental cultural value in Thai society, it would likely take more than a generation for such consciousness to develop and evolve into a social value. This same participant also argued that in Thailand the right to privacy and its recognition has constantly been undermined by the use of national security to justifiy surveillance practices.

As far as legislation in privacy and data protection is concerned, over half of the participants agreed that the existing laws are inadequate and obsolete for coping with new privacy-intruding technologies.[12] Yet, most did not see new legislation as an effective solution to the problem. Instead of imposing new legislation from the top, they argued that the action should start from the bottom, that is, the individual citizens. A significant number of citizens would have to first develop consciousness about their rights to privacy as a fundamental democratic right and publicly express their concern before any policy or legislation could be drafted. At least two participants, the journalist and the corporate executive, asserted that the general notion of privacy and data protection will evolve as a learning experience for most Thais. In the words of the corporate executive,

> It could well take over a generation before Thai people will come to realize these rights. People who have been abused in this generation have to sacrifice themselves so that the next generation can learn from their lesson and attempt to change things for the better.

Although appearing to agree with the above statement, the journalist said he had little faith in what he considers the main institutions of Thai society -- legislative, administrative, and judiciary. These three major institutions, he argued, have consistently failed to deliver a sound public policy or legislation that would benefit the public at large, be it in political, civil, economic or social terms. "It is within this juncture of institutional failure that Thailand now stands in history."

The lawyer/activist voiced a different view. Although he also agreed that the issue of privacy can be considered in socio-cultural terms, he was convinced that all issues are subject to some forms of legal, policy or civic resolution. He stated that in order to develop a standard principle that all sides in society can agree upon, some form of public discussion that will incorporate public opinion as well as the views of the institutional structure is necessary. This, he argued, will enable a detailed and thorough examination of the existing government surveillance practices so that a more transparent process can be developed. "In the meantime, it will help stabilize the emerging civil society which rests on the ability of a society of private individuals to check and balance against the dominant power structure."

---

[12] It should be noted that all the focus group sessions took place between October and December of 1996. This was before the passing of the freedom of official information act, which contains a section on protection of personal data in government files. The Act, which in turn established the Office of the Official Information Committee, was passed in 1997.

The lawyer/activist also put forward important ideas about the interplay of power between different institutions in Thai society. Contradicting the journalist's earlier argument about the three major institutions in Thai society, this participant argued that power can also be mobilized from other sources aside from legislative, administrative, and judiciary institutions. For instance, the royal family, the *sangha* (Buddhist religion institution), the military, the NGOs, labor unions, professional and business associations and more. The NGOs, he claimed, have played an increasingly visible role in spreading people's awareness about certain social issues which eventually resulted in a socially significant legislation or policy. This participant also urged the other participants not to underestimate the understanding and consciousness of peasants and the working class about the implications of government surveillance practices on their lives. In his words,

> Many people in the underprivileged classes do understand that they
> are being taken advantage of through bureaucratic surveillance
> schemes. Yet, they feel powerless because these rights to privacy,
> in both the physical and informational sense, are closely tied with
> other legal and political rights. Their understanding of the problem
> is thus not systematic enough to advance any action. Likewise, it
> will depend upon the more knowledgeable academic and legal
> people to educate and disseminate information about the danger of
> government surveillance among the public at large.

Nevertheless, this participant admitted that it is a difficult task to create overnight awareness and understanding of something as delicate and intangible as privacy. A social opinion or views about privacy are likely to arise only when someone has personally experienced some form of a threat or intrusion to privacy.

As far as the participants in the remaining three group sessions were concerned, the lawyer/activist participant may have a valid point. The participants in the third group session could care less about unauthorized disclosure and dissemination of their personal information in public files. Feeling small and unimportant, the participants in this group said they did not think there would be anything worth knowing about them. As mentioned earlier, the participants in this group were less interested in discussing issues of privacy but were more enthusiastic about airing grievances regarding their economic condition. Similarly, the participants in the fourth group session also expressed little concern about misuses of their personal information. While one participant, a waitress, admitted having a small worry about the possibility of someone copying the information from photocopies of her ID card to make a fake ID, she also did not think this could be entirely jeopardizing because "as long as

242

I have the actual ID with me and they only have photocopies, how could they possibly violate me?"

- Do you feel that you have the right to know when your private information is made known to others whom you did not directly release the information to?

When probed with this question, most of the participants in the first and second group sessions agreed that organizations should seek a person's permission before they share any information about that person with others. While agreeing in principle with the basic idea to establish limits on the sharing of personal information, some of the participants from these two groups also expressed doubts if any such measures would work in practice. They felt that without effective legal and organizational mechanisms to ensure that such practices are respected, it is unlikely that any organization would take the responsibility to inform certain individuals that the sharing of their personal information had taken place, let alone to seek consent for it.

In the third group session, the participants appeared quite confused at first when this question was raised. They could not really bring themselves to understand why anyone would want to "know anything about" some unimportant poor citizens like them. When the moderator described the situation of fingerprint record checking at the police department's criminal records division and how this form of data sharing may inadvertently affect ex-arrestees' employment opportunities, the participants became more pensive. Nevertheless, their comments on the issue of appropriateness in the use of citizen records seemed double-standard, at best. The crux of their argument was that so long as the person's record is unclean, it is legitimate for authorities to look into his or her personal records or even to match records in different files or databases. But if a person's record is clean and has not done anything wrong, then it would be inappropriate to use the stored record for other purposes. It is worth noting that at no time did the participants mention the word "privacy" or "abuses" even while describing the inappropriateness of the bureaucracy using someone's record for a purpose different from when the information was collected.

In the last group dominated by HIV-positive patients, most participants were vehement about the harm that might flow from the sharing of personal information. They would like to restrict the sharing of harmful or sensitive information with a particular emphasis on health information. One participant asserted the idea of a "consent form"

whereby a citizen could waive the right to reveal certain information about him or herself so that undesirable information may not be stored in the databases nor in new types of ID cards capable of storing electronically-encoded information. Meanwhile, a few of the participants felt it would be good to facilitate the sharing of "beneficial information," which they vaguely defined as any information that, if released or shared, would be useful to the subject of the information. In this light, general civil registration information -- name, age, address, number of people in household -- is considered useful information that can help benefit the data subjects in one way or another.

CONCLUSION

It is clear from the above focus group sessions that participants from different socio-economic backgrounds utilize quite distinct cognitive schema when thinking about privacy, particularly in relation to government surveillance. These differences are partly reflective of the recognition and acceptance of individuals in each group of their power relations vis-a-vis the state and their faith or trust in the state not to use their personal information for illegitimate ends. Most of the members of the first two groups -- those higher in the socio-economic strata -- were more critical of the state and exhibited less trust in the handling of personal information in government files than the third and fourth group who are from lower socio-economic backgrounds. Because of their greater exposure to western social philosophy which places a high value on individual autonomy, members of the first two groups appeared more apprehensive of government surveillance and were more definite in maintaining a boundary between public and private realms. Furthermore, their educational and professional backgrounds also contributed to a higher degree of awareness of the application of new ICTs in organizational record-keeping and surveillance techniques. By contrast, the members of the third and fourth groups tended to have a greater trust in the government and to see its documentary activities as a benign force that benefits the collective interests of the public. This tendency to trust was reinforced by their feelings of powerlessness vis-a-vis the paternalistic state and their ignorance of the ramifications of new surveillance technologies that are already in widespread use. As for the last group, personal experiences apparently played a crucial role in helping to crystallize the group members' orientation to certain aspects of privacy. As far as information privacy is concerned, members of these groups readily produced examples of problems with the government's health files to support their views that government organizations cannot be trusted with the handling of citizen's sensitive personal information. Unlike the members of the third and

fourth groups, participants in the last group not only expressed strong criticism of the government's approaches toward health surveillance, but they also felt that they were in a position to politically mobilize against any unfair government information practices or in support of legal measures that would restrict serious invasions of privacy.

The assumption that an individual's socio-economic status is likely to influence his or her orientation towards privacy seems to have been supported in the discussions in the focus group sessions. A further inference that can be derived from these experiments is that people with particular vulnerability and personal experiences of privacy invasion are likely to be more apprehensive about the issue and more cognizant of the importance of a reliable body of laws that could restrict serious invasions of privacy. This is best evidenced in the case of the last focus group involving AIDS patients, HIV-positive persons, and health professionals working in these areas. In addition to these findings, a number of interesting issues related to privacy were also raised during the several focus group sessions which could be explored further, possibly in future research. Meanwhile, the clear indifference and economic utilitarianism in evaluating surveillance by the lower socio-economic groups also warrants a deeper reading. Fundamentally, it is possible that these participants do not value privacy much because they see it as not a part of their basic need. They can get by with less of it in their daily lives. To them, the greater priority is to make ends meet; this is precisely reflected in their frequent digression to financial and workplace problems. Another way to look at their indifference is through their interaction with me as a moderator and a representative from a different socio-economic class from theirs. It is very possible that these participants were not at all interested in discussing the seemingly abstract topic of privacy with me but were obliged to because of the pay I offered, or the influence from their employer.[13]

Be that as it may, the lack of interest of participants from the lower socio-economic groups, who also represent the majority of the Thai population, also raises interesting questions with regard to the possibility of mobilizing change on surveillance issues. Since "privacy," especially on an aesthetic level, does not seem to arouse fears and strong feelings among these social groups, it may not be an appropriate concept to use to politically mobilize against state control in the Thai context. Privacy strategists, should they emerge, may be

---

[13] Nevertheless, they were kind enough not to show their boredom during the session. All were in fact trying to be as cooperative as possible.

better off focusing on its instrumental dimension, particularly the way in which loss or intrusion of privacy affects other forms of rights or interests of individuals and groups.

CHAPTER 8

INFORMATION PRIVACY IN THAILAND:
A HISTORICAL AND PUBLIC POLICY OVERVIEW

This chapter traces the evolution of privacy, particularly information privacy, in Thai society in two broad realms -- cultural and public policy. In the cultural realm, a brief anthropological survey on privacy is attempted. This is followed by a discussion on Buddhism and the history of Thai political development, both of which are taken to be important philosophical and contextual basis for the development of privacy rights in Thailand. Then, a more empirical analysis into the legal statutes, constitutions, and public policy from past to present will be carried out.

In keeping with the historical framework used throughout the study, the following analysis will be historical in nature. Secondary reviews of existing literature, bodies of law and draft laws, as well as policy reports provided the basic sources for the investigation. Whenever possible, semi-structured interviews with legal experts and policy-makers were carried out to seek first-hand opinions about contemporary changes in technology and public policy and their wider social repercussions.

ANTHROPOLOGICAL EVIDENCE OF PRIVACY IN THAI SOCIETY

The Thai language does not have a word for privacy but refers to it by descriptively translating from English as *khwam pen suan tua* or *khwam pen yu suan tua* , meaning "the state of being private." According to a prominent Thai anthropologist, the Thai public-private divide is inherently distinct from that of the West.[1] Citing the example of an interior design of traditional Thai houses in the Northeast, this anthropologist points out how the room which is considered most private -- the "spirit room" -- can be shared by all members of the family. This "spirit room," he explains, is usually located in the center or in the least accessible corner (from outsiders) in the house and is considered a sacred space that needs to be protected from outside intervention. Meanwhile, this room is also designated as a space where all family members perform religious rituals and functions together since it is where the ancestral shrines and the ashes of the ancestors are kept. What this signifies, he says, is that traditional Thai

---

[1]Dr. Nithi Aeusriwongse, professor of Anthropology and Sociology, Chiang Mai University, interview by author, 13 October 1996, Chiang Mai University, Chiang Mai.

conception of privacy is fundamentally collectivistic. It is the kind of privacy that is shared by intimate members of the same household. By this token, individualistic privacy is said to have no place in traditional Thai culture.

Similar to the interpretation above, a recent anthropological study at a local university finds privacy implications in the evolution of house forms and habitation patterns of a group of Thai peasants in the Central Region over the past one hundred years. When these peasants were first settled in this region, their habitation units featured large common space, which was used for several purposes -- social rituals, work space, and playground -- and relatively small living space -- kitchen and sleeping areas. It should be noted that most of these traditional houses do not have separate bedrooms as the family members usually sleep together in one big central room. Most of the common space, which was regarded as social space, was located outdoors so that neighbours could join in the activities. But as the capitalist economy grew and took over the peasant community, traditional farming was no longer adequate to cope with the modern way of life. Many farmers became migrant labor to the city and new farming technologies were adopted by those who still do farming to increase production. With more time freed up and with the penetration of television, many farmers find themselves spending more time indoors. This directly affects the house forms. Most evident is the way that the private space has been increasing at the expense of the common space. Separate rooms with doors are now common in peasants' houses and so are rooms with new functions. For instance, the emergence of TV/living room has become a norm for architectural patterns across the peasant community in the Central Plains.

What this means is that privacy in the physiological sense may be increasing in this peasant community. But this may have no bearing whatsoever on "privacy" in the sense of private rights against the intrusion of others, particularly those with authority.

THE CONCEPTION OF RIGHTS IN THAI SOCIETY
-- A PHILOSOPHICAL AND HISTORICAL UNDERPINNING

Buddhism and human rights

In studying the conception of "right" in Thai society, many scholars, foreign as well as Thai, turn to one preeminently potent philosophical force that has shaped Thai culture for centuries -- Buddhism. One of the central concepts in Buddhism that has greatly influenced the Thai world view is that of "karma." Under the law of "karma," a person's status or duty in the present life is dictated by the deeds done in his or her past life. As a result, social inequality is traditionally looked upon as part of one's destiny, and as something that is not necessarily problematic. A mainstream and somewhat reductionist interpretation of this Buddhist outlook gives rise to a widespread impression that most Thais, who are Buddhists, do not believe in natural rights or freedom that make all human beings equal. Such predisposition, it is argued, leads Thais to be apathetic and disinterested in struggling for human rights in the fashion understood in the West. Similarly, another influential Buddhist concept of the "middle path," which emphasizes moderation and implies conflict avoidance has also been interpreted as an obstacle to the development of human rights in Thai society.[2]

While it is true that Buddhist philosophy may not be very conducive to the development of the human rights and values that are esteemed in the West, one should not stretch this observation so far as to fall into the trap of religious determinism. After all, religions, whether they be the philosophical ideas or the institutional establishments, are frequently exploited by human actors as a means to achieve certain social ends, with varying results. Such is the case with the law of "karma," which has been narrowly interpreted to justify strict class divisions in traditional societies so that the domination of the ruling classes could be sustained. Apart from its discouraging message of predestination, there is also an inspirational dimension to the law of "karma," according to another more recent interpretation. Since this law is seen in the Buddhist view of the world as propelling the existence of beings through cycles of death and rebirth, it is also said to provide a condition for each human individual to attain emancipation through good deeds and enlightened understanding about life during one's lifetime. In other words, freedom is not something that human beings are born with in Buddhism. It does not

---

[2]Thanet Apornsuwan. "Rights in the Thai States," in *Imagine the Year 2000: Innovation of Paradigm in Thai Studies?*, ed. Chaiwat Satha-anand (Bangkok: Thailand Research Fund, 1996), 186.

come naturally but can be acquired through such means as self-control, meditation, and knowledge derived from the study and observation of "dharma" -- the teaching of Buddha.[3]

With the emphasis on individual capacity to seek and attain emancipation, Buddhism is said to bear some resemblance to liberalism.[4] However, the two philosophical traditions diverge in their goals and conception of human emancipation in accordance with the different social contexts in which they evolve. While liberalism emphasizes emancipation as the creation of individuals who struggle to achieve rights and freedom in secular and material terms, Buddhism teaches the transience of matter and being and encourages individuals to discard material belongings and worldly comfort in order to achieve spiritual freedom as embodied in the ultimate condition of "nirvana."

Insofar as the right of privacy is concerned, it is incongruent with Buddhism at least in two important ways. First, the philosophical environment of Buddhism is anchored in the idea of inter-relatedness rather than a model of individual versus the society or the state. In this regard, the problem is the relationship between the "inner" and the "outer" rather than the "private" versus the "public." The fact that Buddha himself leaves the household life behind to seek enlightenment may indicate that Buddhism leaves the "liberal" problematique behind or is fundamentally indifferent to it.[5]

Secondly, unlike liberalism which focuses on individualism, natural rights, and human dignity, Buddhist thinking sees the obsession with one's individual self and one's possessions, material or not, as the root source of suffering. Emancipation, as mentioned above, means disillusionment with and relinquishing of preoccupation with the self and worldly desires. Therefore, individuality can be seen as both the beginning and the end to human emancipation in Buddhism. It must be remembered, however, that the above interpretations are filtered mainly from classical Buddhist teaching, which may not necessarily reflect the behavior of relatively secularized Buddhists in contemporary Thai society.

In the final analysis, it is clear that Buddhist philosophy operates on a different level from that of liberalism upon which the theory of privacy was originally founded. Aside from

[3]Suwanna Satha-anand, "Regarding Buddhism and Human Rights," (wa duay putta sassana kab sitthi manussayachon) in Views in Eastern Philosophy (manussaya that nai pratchaya tawan ok) (Bangkok: Chulalongkorn University Press, 1990), 120.

[4]Thanet Apornsuwan, "Rights in the Thai States," 223.

[5]Dr. Suwanna Satha-anand, professor of Buddhist Studies, Chulalongkorn University, correspondence with author via electronic mail, 24 June 1999.

its relatively modest contribution to promoting rights-oriented political culture, Buddhism also pays little attention to physical freedom, which is a crucial basis for privacy.

"Rights" in the history of Thai political development

While anthropologists and sociologists may ponder over Buddhism as the framework for understanding the conception of "rights," or lack of it, in Thai society, political scientists tend to feel that this is better grasped within the structure of power relations in a given period. Within the political realm, the conception of "right" has clearly undergone significant changes throughout the extensive history of Thai political development. During Ayutthaya, "rights" were theoretically seen as a privilege and an exclusive entitlement for the king. As divine ruler and proprietor of all rights, the king was in the position to bestow any types of privilege, as he deemed fit, to his immediate subordinates -- the nobles -- who would in turn pass on some of the allocated privileges to those in the lower layers of the social hierarchy. In return, all people -- nobles as well as *phrai* -- were obliged to serve the king in their variable capacities -- controlling of *phrai*, soldiering, performing corvée labor, and so forth. These obligations were generally known in Thai as *tham ratchakarn*, which generally means "doing the work in the service of the king." This structure of social relations between the king and the rest of society is well illustrated in the *sakdina* system.

According to conservative Thai historians,[6] *sakdina* rights and duties were the product of a harmonious reciprocity between the so-called patrons and clients. In this patronage relationship, people in the lower social groups voluntarily surrender their services for those in the higher social strata out of respect and loyalty, while the more privileged provide them with protection and security. In addition, despite the differences in their social status and duties, all patrons and clients were said to be equal "before the law." This is explained in the following terms,

> Everyone in Ayutthaya society, whether he be a prince, an aristocrat, or a *phrai*, is considered equal as servant of the king. Under the absolute power of the king, all persons in Ayutthaya society are guaranteed to be uniformly protected and are hence equal before the law. The close-knit relationship and

---

[6]Prominent among this early group of historians are Prince Damrongrajanuphap, who is better known as the father of Thai historical study, and M.R.. Kukrij Pramoj, also a member of the royal family, a former prime minister and a renowned statesman. Because of their royal lineage and aristocratic background, their historical accounts tend to carry a bias in favor of the ruling class.

interdependence between classes also made it impossible for people in each class to be completely isolated from each other.[7]

According to this view, since equality could be guaranteed and social relations took place in harmony, free of class conflict or contradictions, there was thus no need for people to struggle for rights or freedom in a formal sense.[8] This positive outlook on Ayutthaya society stems partly from the tendency among some scholars to romanticize the ideas associated with the paternal system of government, which Ayutthaya incorporated from Sukhothai (the prior Siamese kingdom) into its autocratic regime. Under such a paternal governing system, the relationship between the state and society is sustained by interdependence and compromise, resembling the relationship within a family. In this light, an important collaborative study by Thai scholars from interdisciplinary backgrounds -- history, anthropology and political science -- concludes that "compromise" is an important framework in understanding the Thai conception of rights especially in the pre-modern period.[9] Many of these scholars also point to Buddhism as the source of the Siamese's compromising predisposition and to the deep-seated patronage system as its perpetuating agent.

This group of scholars also invariably argue that such predilection has enabled the ancient Siamese state to constantly expand its power at the expense of society without provoking significant rebellious outbreaks. The *sakdina* system thrived for several centuries, in effect confining the scope of social relations within a limited vertical axis of manpower control. Since the majority of people -- the *phrai* -- were heavily bound by obligations to the *mun nai* and to the king, it was impossible, so it is argued, for them to evolve into free men who would realize that their "rights" could, let alone should, extend beyond what was "mercifully" bestowed by the more privileged class.

Even after the abolition of corvée and slavery during the Chakkri Reformation in the early twentieth century, ideas about rights in Siamese society did not change much. The so-called "transformation of *phrai* into citizens" by Chulalongkorn was at best a strategic move to

---

[7]M.R. Kukrij Pramoj. "The Ayutthaya Society." (*sangkhom samai ayutthaya*) in *History and Politics: a Supplemental Reading for the Subject of Thai Civilization* (*prawatsart lae karnmuang nangseu aan prakob wicha araya tham thai*) (Bangkok: Thammasart University Press, 1973), 51.

[8]It should be emphasized that while there were no open confrontation or struggle for rights in the formal sense, the *phrai* who constitute the majority of people during Ayutthaya often resorted to informal avenues to protect themselves against arbitrary interference by state authority. Important informal defenses against the state include bribery, maintaining of distance from state officials and through maneuvering through loopholes of the patronage system.

[9]Report of the Working Conference on the Project to Develop Human Rights in Thailand." *Newsletter on Thai Studies* 1, no. 5-6 (December 1983): 8 - 27.

centralize and stabilize royal power rather than an effort to create a free society of liberal-minded individuals. As a result of the government reform, the scattered loci of *mun nai* power were unified under the new and royally-dominated bureaucracy. Most of the former *phrai* became tenant farmers in the rural area and would continue to be subordinate clients of the patron bureaucrats in subsequent decades. In the context of the perceived threats of encroachment by western colonial powers, "rights" began to incorporate new rhetorical dimensions. While the old meaning of "privilege bestowed by the more powerful (*phu yai*) to the less powerful (*phu noi*)" remained intact, the conception of "rights" in this period also evolved to include concerns about national survival with an emphasis on the collective interests and rights of the nation.

According to a 1928 poem composed by Chulalongkorn's half brother, Prince Naradhip, who was also a cabinet member and a poet, the "natural rights and freedom of Siamese citizens" include four basic types of rights: 1) the right to live without threat from others; 2) the right to earn a living; 3) the right to learn and educate oneself; and 4) the right to help maintain the liberty and sovereignty of the nation. The last type of right clearly reflects the influence of the relatively new and modern concept of "nation" on the notion of "rights." It implies a collective rather than an individual basis as in the West.[10] It also shows how "rights" might have been confused with "duties." Under royal absolutism, the borderline between the two concepts was vague. Although the new peasantry might have been freed from the old bonds of labor indenture, they now entered into a new type of autocratic relationship with the institutions of the absolutist state and were inculcated with a new authoritarian national ideology. This ideology is defined by three major institutions -- nation, religion (Buddhism), and king -- which are fused together under the idea of Thai-ness. Citizenship in the modernizing Thai (Siamese) nation thus demanded absolute loyalty and obedience to the two key institutions of religion and monarchy. The preoccupation with the above ideology of the absolutist state left little room for the development of individual rights in the realms that are nurtured in the West -- civil, political and economic. In addition, without proper institutional locales where the above categories of rights could be defended and advanced, it was difficult for citizenship rights as understood in the West to emerge in Siam at that point in time.

---

[10]"Nation or *"chat "* in Thai conveyed quite powerful conceptualizations about the new absolutist state. Although the word *"chat "* was previously used to convey the idea of birth, race, or ethnic identity, it was converted, roughly in the last decade of the nineteenth century, to express the idea of a "nation," a population enclosed within a given territory and owing political allegiance to a common authority. This semantic shift reflected a significant change in the relationship of king and people. Under *sakdina,* the Crown dealt directly with the *mun nai* and only indirectly through the *nai* with the rest of the population. But during the Chakkri Reformation the monarchy was brought closer to the population through various ritual and ideological means. As part of this great reform, the notion of "nation" (*chat*) is defined as a single community through the shared relationship between the king and the people.   See more in Pasook and Baker, *Thailand,* 233-235.

Even after the 1932 coup which replaced the absolute monarchy with a democratic government and opened Siam to an era of modern politics, the understanding of citizens' rights in Thai society remained as limited as before. Possibly the best indication of the conception of "rights" in the post-coup period may be found in the constitution and several of its subsequent amendments. In the very first constitution enacted in the period immediately following the coup, only a few articles addressed people's rights and freedom. This was stated under the section on "rights and duties of Thai people" which addressed such topics as freedom of religious worship, freedom in life and property, freedom of speech, freedom of association, and duties towards national law and national security. Notably, there were no specific stipulations on "rights" per se until the first amendment in 1947 when the right to a fair trial was added to the above section although freedoms imply rights, an interpretation reinforced by the title of the section, "rights and duties of the Thai people."

A noticeable change appeared in the 1949 version of this section when a number of new articles on rights were introduced. According to legal analysts, these changes were a direct outcome of the Universal Declaration of Human Rights adopted by the United Nations (U.N.) General Assembly in the previous year. The Siamese government had by that time become a member of the U.N. and, although the declaration was not legally binding, the leaders at the time were compelled to support its adoption in the Thai constitution. Apart from incorporating twenty new articles on rights and freedoms, frequently by translating directly from the U.N. Declaration, the Siamese government also published the new articles in the Royal Gazette and repeatedly disseminated details about them through radio broadcasts of the Public Relations Department.[11]

The adoption of new articles setting forth a diverse catalog of rights in the 1949 constitution turned out to be merely a political fulcrum in an effort to impress the local populace and international observers. As time passed, this amended version of the constitution even drew accusations of hypocrisy. As one critic contends, some of the provisions on rights and freedoms specified in this amendment only created an illusion of constitutional protection and guarantees that were in fact filled with loopholes.[12] The 1949 constitution allowed for laws,

---

[11]Pridi Bhanomyong. "Democracy and Fundamentals of the Constitution: the Drafting Process." (*pracha thippatai lae ratthathammanun beung ton kab karn rang rattathammanun*) in *The Democratic Thoughts of Pridi Bhahomyong* (*naew khwam khid prachathippatai khong pridi phanomyong*) (Bangkok: Pridi Bhanomyong's Foundation and the 60th Year Democracy Project, 1992), 139 as quoted in Thanet Apornsuwan. "Rights in the Thai State," 210.

[12]Borvornsak Uwanno, *Law and the Alternatives for Thai Society* (*kot mai kab thang leuk sang khom thai*) (Bangkok: Nititham Press, 1993), 43, 63.

both provisional and organic, to be subsequently enacted which could curb the specified rights, and the exercise thereof, to any extent possible. Therefore, the degree of legal protection for citizen's rights or freedom actually depends on the content of future laws and the actual enforcement of constitutional protection.[13] In many ways, the 1949 constitution set the course for an interesting paradox in Thai political history. Following this constitutional amendment, Thai politics became more authoritarian than ever before. The irony is best illustrated by the prolonged rule under oppressive military dictatorship in which even presumably basic human rights were quashed.

To date, the stipulations on rights and freedoms in all Thai constitutions prior to 1997 reflected a political orientation that was clearly authoritarian. Instead of focusing on the certification of people's rights and freedoms, these constitutional provisions were typically more concerned with the exercise of authority by government officials on matters regarding those rights and freedom. Too often, the provisions opened ways for organic laws to enable government officials to limit the people's claim. In this light, some legal analysts have argued that the rights and freedom which are stipulated in the Thai constitution are in fact negative rights and freedom. This is because they are by no means natural rights, nor do the people have legitimate grounds to defend those rights and freedoms without political interference from the state.[14]

It merits emphasis that the past versions of the Thai constitution have often come under criticisms for their many inherent contradictions. For a fair assessment, these discrepancies ought to be understood within the context in which they are bred. Unlike the U.S. constitution, which evolved out of a fervent struggle for freedom from colonial rule, the Thai constitution was imposed upon the people from above by the bureaucratic elites who toppled the absolute monarchy. For the same reason, it could not possibly embody the objective to limit the power of the ruling group as was the case of the U.S. constitution. Far from being a manifestation of a social contract between the state and the people or among the people themselves, the Thai constitution, as several local analysts observe, only served as a synopsis of laws and public policies that would facilitate the state power to control the populace. At best, it is merely a reflection of power relations in Thai society rather than a representation of

---

[13]The only right or freedom that was fully protected and guaranteed in this constitution was the freedom of religious worship. The provision on this topic prohibits the legislature from passing any future laws that would bridle a person's freedom to religion. This exceptional provision is usually attributed to the long-standing tradition in Thai culture to be relatively open to other religious beliefs.

[14]Thanet Apornsuwan, "Rights in the Thai State," 209.

the supreme law of the land.[15] One social critic boldly asserted in 1995 that the actual constitution for Thailand lies in the political culture since it cannot be drafted, amended, violated, or revoked but is indeed a living reality.[16]

PRIVACY RIGHTS AND DATA PROTECTION IN THAI LAW

Thailand has no coherent legislation, which directly and exclusively regulates "privacy" or *khwam pen (yu) suan tua* in Thai. Although there are a number of articles in different legislation and the constitution that address matters related to privacy in its multifarious dimensions, these provisions mainly deal with privacy in conjunction with other rights and legal protections. There are no direct stipulations about violation of "privacy" per se as abuses have typically been framed in terms of trespass, defamation, or breach of trust or confidence instead.

Insofar as data protection is concerned, there is evidence of legal protection of government information since the ancient period of Ayutthaya.[17] However, the protection of personal data belonging to individual citizens, or information privacy, was not legally recognized until some time in the early twentieth century after the Chakkri Reformation. Evidently, it was not possible for the more liberal and individualistic notion of privacy to take roots in the inhospitable soil of traditional *sakdina* society. Even after the abolishment of the *mun nai- phrai* system by Chulalongkorn, the people were still not entirely free from the shackles of the patronage system. Furthermore, given the looming threat of colonialism, they were instructed to be obedient citizens of the king and to give up their personal freedom for the collective good of the nation. Privacy would thus have seemed an anachronism at that point in Thai history.

It was during the reign of King Vajiravudh, Chulalongkorn's son, that the first trace of legal protection for information privacy would emerge. Following the Chakkri Reformation, new information and communication technologies -- radio and telegraph -- were introduced.

---

[15]Saneh Chamarik, *Thai Politics and the Development of the Constitution (karn muang thai lae phattanakarn ratthathammanun)* (Bangkok: Thai Studies Institute, Thammasart University, 1986), k.

[16]Nidhi Aeusrivongse, "Constitution: the Cultural Edition," *(ratthathamanun chabab watthanatham)* in *Chat thai muang thai baeb rian lae anusawaree* (Bangkok: Matichon Press, 1995), 136, 138.

[17]For instance, a law was passed during the reign of King Trailok in 1454 which was designed to prevent spying and unauthorized leakage of government information to enemies. Offenders were subject to severe penalty.

They significantly altered the predominantly oral culture of the past. The Radio and Telegraph Act was enacted in 1914 to govern the use of the new technologies. Besides addressing security concerns and prohibiting the transmission and dissemination of confidential government information, this law also contains a section that indicates, for the first time, a recognition of a principle that can be classified as privacy rights. This section prohibits and sets forth penalties for unauthorized opening of documents or telegraphs that belong to others. A decade later, an existing law called the Attorney Act was amended with a new section added to establish protection of confidentiality of attorney-client information exchange. Although both laws impose only light penalties on offenders, they reflect a significant step in a new direction for the still obscure legal disposition towards information privacy.

After the 1932 coup, legislation to protect personal privacy increased. For instance, in 1934 the Telegraph and Telephone Act was passed, and two of its articles regulated against unauthorized opening, eavesdropping, and disclosure of information transmitted by telegraph or telephone. Up until this point, the legal trend had been toward a conception of privacy focusing on ownership and property rights rather than on personal freedom. A slight shift occurred in 1949 with the amendment of the constitution to incorporate the new section on rights and liberties, which followed the Thai government's adoption the U.N.'s Universal Declaration of Human Rights. In this section, article 47 lays down the first constitutional protection of a set of rights that are akin to the rights of privacy in the West. Here, the conceptual basis appears to be personal freedom rather than property rights or ownership. It reads,

> The rights of individuals in their families, dignity, honors, reputation, and privacy are recognized and shall be protected. Public communication and dissemination of personal information, using whatever means, which may affect the rights of individuals in their families, dignity, honors, reputation, and privacy are prohibited unless they are done in the public interest.[18]

This provision remained unchanged for the next sixty years and was adopted again in the section on "rights and liberties of Thai citizens" in the latest constitution promulgated in 1997 as part of a major political reform. From it, one can deduce that "privacy" is understood not as a separate category of right but one that is recognized in conjunction with other types of rights. Based on the wording of the above article, it is not clear whether privacy right is seen as an end in itself or a means to realize other related values -- family life, dignity, and honors.

---

[18] Article 47 of the Thai Constitution 2534 B.E. (1991), amended version (No. 5), section 3 : Rights and Liberties of Thai Citizens.

In many ways, the above article reads like a modest translation of article twelve of the famous UN's declaration which only offers a broad definition of privacy. Likewise, it seems we can only find a semblance of privacy in the Thai constitutional provision since no precise definition of the term is given.

Following the 1949 constitutional amendment, a number of laws were subsequently passed with contents addressing matters relating to privacy and data protection. Although the focus of this chapter is on the protection of people's information privacy from government interference, I feel compelled to include these civil and criminal laws that regulate information practices between private parties so that a broader trend can be grasped. The laws reviewed below are still in effect today.[19]

- The 1941 Press Act contains three articles that set guidelines for protecting the privacy of individual citizens who are subject to publicity in the press. Individuals who have been adversely affected by publicized information in the press are legally entitled to a correction or a public apology by the publishers as well as to pursue litigation under the tort of defamation.

- Article 420 of the 1949 civil code defines a civil wrong as a willful or negligent injury against life, body, health, freedom, property or other right and as contrary to law. The law warrants compensation to the affected party from the damage done from such wrong, if proven in court. In this light, personal information can be classified as property and is entitled to the same legal protection.

- The 1951 Juvenile Justice System Act includes a measure to protect the privacy of juvenile suspects. Article 57 of the law prohibits the press or anyone from releasing the name or any information that would reveal the identity of youthful suspects.

- The 1956 Criminal Code contains three articles and one section that address three different models of protection of the rights to information privacy: 1) protection against unauthorized opening of "sealed" personal documents, letters, telegraphs with or without intent to

---

[19]These laws are compiled from a review of two master's theses in law at Chulalongkorn University. See more in Kittiphan Kiatsunthorn, "Criminal Measures for the Protection of Personal Data," (*mattra karn thang aya nai karn khum khrong khor mun suan bukkhon*) (Master's thesis, Chulalongkorn University, 1995); and Cheun-Arie Maleesriprasert, "The Protection of Right to Privacy and the Communication of Information," (*karn khum khrong sitthi suan tua kab karn seu sarn sonted*) (Master's thesis., Chulalongkorn University, Thailand, 1996).

disclose such information: 2) protection of personal secrecy or confidential personal information from unauthorized disclosures by professionals who obtained the information in their professional capacity; 3) case of defamation from unauthorized disclosure of personal secrecy.

- The 1962 Commercial Bank Act was amended in 1979 with the addition of article 21 which stipulates against unauthorized disclosure of confidential clients' information by authorized personnel of financial institutions.

- The 1965 Statistics Act, article 21 sets forth a measure to protect the confidentiality of important personal data particularly personal income. Authorized officials -- officials at the National Statistics Office -- are prohibited from disclosing any information (facts or figures) as held in the organization's files under any circumstances.

- The 1991 Civil Registration Act, articles 12-17 establish guidelines for protection of civil registration information. (This shall be discussed in more detail shortly.)

- A collection of regulations and ministerial orders governing the conduct and professional etiquette of people in several professions including physicians, attorneys, nurses, engineers, architects, and accountants. These regulations contain articles or sections which stipulate the confidentiality of information obtained from their clients.

Despite the existence of these legal provisions, information privacy is hardly given adequate recognition and protection in practice. While it may be unfair to blame this deficiency solely on the laws and the lack of implementation given the general apathy towards the issue in Thai society, there are undeniably shortcomings in existing privacy-related laws that need rectifying.

First, the penalties for violation are usually minimal. Take the Juvenile Justice System Act for instance, the penalty prescribed in cases of abuses involves a maximum fine of 500 baht (about US$20) or a maximum six-month jail term. It should come as no surprise then that Thai newspapers routinely and openly report the identity of juvenile suspects in their coverage. Often, photos of young suspects are featured on the front page together with personal details such as the suspect' s name, name of his or her parents, name of school attended, and home address. The fact that this law is still in effect today and imposes the same

penalties as half a century ago indicates how low is the ranking of privacy in legislative priorities.

Secondly, civil and criminal law causes of action as well as appeals to constitutional law are not adequate to protect privacy, especially when it comes to the regulation of computerized files. As mentioned, the protection of privacy under civil and criminal law depends upon litigation brought under torts of trespass, defamation, or breach of confidence. To establish a civil or criminal wrong against a person or his/her property, it is essential to prove the wrong was either intentional or an injury arising from negligence. In the case of defamation, for instance, the truth of a statement is the basis for litigation. In the context of computerized record-keeping, use, and transfer, a file could be true but nevertheless cause injury when used in a different context or when combined with other data. With the now common practice of computer matching across different databases and inter-agency record linkage, an individual's privacy can be invaded without causing "harm" as recognized by law. Furthermore, within the routine environment of automated data practices, it would be very difficult to demonstrate the intention to cause harm.[20]

In addition, like most legal statutes on rights and freedoms in Thailand, these privacy-related laws are subject to limitations usually argued on the basis of collective public interests. In the last version of the former constitution (amended in 1995) prior to the newly-enacted one in 1997, article 47, which enshrined the right of privacy in conjunction with a set of related rights, (quoted above) places a disturbing restriction upon those rights with the following clause:

> No restrictions shall be placed on the exercise of these rights and liberties as indicated above except through provisional laws allowed by this constitution. These provisional laws must be for the purpose of national security, public safety, for the prevention of disorder or crime, and for the protection of the people's good morals.[21]

As a result, public authority is given a constitutional leeway to interfere with the people's right of privacy under the guise of national security, public safety, and so forth. While such interference may be viewed as having a devastating effect in most liberal democratic states, it tends to gravitate towards a norm in Thailand given the country's extensive history of dictatorial rule, its security situation during the Cold War, and the constant threat of a coup

---

[20]See more in Kevin Wilson, *Technologies of Control*, 54.

[21]Article 47 of the Thai Constitution 2534 B.E. (1991), amended version (No. 5), section 3 : Rights and Liberties of Thai Citizens.

d'état under civilian governments. During the problematic period of the late 1960s and early 1970s, in particular, national security became a shorthand for the government's suppression of suspected insurgents and dissidents. Many repressive laws were then passed in the name of protecting national security, in effect undermining the constitutional protection of people's rights and liberties. Consequently, the people's private rights against government interference were in a tremendous retreat and it would take decades before a movement would coalesce to question the government's information practices, which also have privacy ramifications. This will be discussed in detail in the next section.

Insofar as laws that regulate the collection and use of personal information by the government are concerned, a similar trend of making "exceptions" in the interests of national security is also evident. In the 1991 Civil Registration Law, which was enacted in response to the introduction of computerized record-keeping and data processing, article 17 deals with the privacy aspect of personal data in the files. It reads, in part:

> Civil registration information must be held confidential. Registrars are to ensure that the collection, storage and use of the information comply with the objectives as stipulated in this Act. No one shall disclose statements or figures in the civil registration files to the public or to any persons other than those who have authority as prescribed in this law. Under no circumstances can civil registration information be used as evidence that will harm the owner of the information.

However, the above protection can be misdirected and rendered useless by the "exceptions" set forth in the latter portion of the article:

> The exceptions to the above stipulations are (as follows): when a stakeholder wishes to inquire about the family status of someone he or she has a legal relationship with; when it is necessary for statistical purposes, or in the interests of national security or public safety, or for the investigation and operation of law and order.

Interestingly, although this law designates the central registrar (director-general of the Department of Local Administration) and registrars at civil registration offices nationwide as the lawful authority of civil registration operations, it also allows other government departments to share in the use of civil registration information. Article 15 of the law addresses this inter-agency data transfer and linkage, to wit:

> Government departments and agencies may request registrars to make and submit copies of civil registration information in cases which are necessary for the operation of that department or agency.

If a government department or agency wishes to establish a computer linkage with the civil registration database in order to exploit the stored information, registrars may allow permission for the linkage only to information contained in the following databases -- household registration, birth registration, and death registration.

The above provision will no doubt facilitate computerized manipulation of personal data which continues to grow by leaps and bounds.

DEMOCRATIC MOVEMENTS
AND THE FREEDOM OF OFFICIAL INFORMATION ACT

Information privacy has never been a central legislative or public concern in Thailand but has been subordinated to constitutional provisions on human rights and provisional laws such as the above civil registration law. More recently, however, information privacy has emerged, or more accurately put, became hidden away, in Part III of the newly-enacted Freedom of Official (Government) Information Act B.E. 2540 (1997), the first of its kind in Thai history.[22]

An important preamble to the drafting and enactment of this new legislation lies in the movements of political dissidence which began in the 1980s and gained significant momentum in the early and mid-1990s. Driven mainly by NGOs and progressive academics, these movements evolved in different social realms but shared common objectives, that is, to mobilize against the domineering state and to further the growth of democracy. The interest in government information practices began with several conflicts between the general public and the government over the lack of public access to government information. Many of these conflicts took place during the economic boom of the late 1980s and early 1990s when several mega-projects were conceived involving the construction of new infrastructure such as roads, mass transit, telecommunications networks, and dams. Although these projects have far-reaching implications for people's lives, the people were usually kept in the dark and not informed about the projects until construction had started or was being completed. In some cases, distorted and misleading information was given to the public in order to disguise possible adverse impacts. Shielded from public scrutiny, these projects often turned out to be disastrous to the environment and the livelihood of the people residing close to the construction

[22]I consider it "hidden" particularly because the protection of personal data and privacy has never been politicized as a cause for the enactment of this new law.

site. Once the damage was apparent, an inevitable clash between the government and the people erupted, leading in some cases to violence and long-lasting grudges against the state.

A case in point is the controversy surrounding the Electric Generating Authority of Thailand (EGAT) plan to build the Pak Mul dam in the rural Northeast in the late 1980s. In the beginning, EGAT, in its zeal to generate electricity from the proposed dam to the urban area, presented to the public a one-sided report on the feasibility study for the proposed project. This report generally focused on the pros of the dam while underestimating the adverse impacts to the locality. In the absence of a public inquiry and open access to official information, crucial information was withheld and misleading figures were presented to make the construction of the dam and the related process of land expropriation seem innocuous.[23] As far as the local populace who would be displaced were concerned, they were encouraged "to sacrifice their habitats for the greater benefits of the nation which was facing the risk of energy shortage."[24]

Despite heavy opposition by local villagers and NGOs, who were able to discredit EGAT with information that had been illicitly withheld, the construction of the dam took off. From 1989 to 1993, there were numerous protests and demonstrations by the rural villages and NGOs against the project and the fact that EGAT was not truthful to them from the very beginning. On several occasions, these protests developed into open and violent clashes between the rural protesters and the police. Some protesters went on a hunger strike, while others burnt their national identity cards as a symbolic repudiation of their Thai citizenship. It would soon become clear to these rural protesters and the untrusting environmentalists that their skepticism was well-founded. The new dam has indeed been proven destructive to the forest and the surrounding region. After the construction of the first segment of the dam was completed, a large area of surrounding farmland became flooded, seriously disrupting farming and fishery resources, both of which had been the lifeline of the rural community. Furthermore, the displaced households were given inadequate compensation for their expropriated lands. This led to further public outcry and distrust of the state. [25]

---

[23]For instance, in calculating the cost of the dam, only the construction cost and the expenses of land expropriation were included. Opportunity and social costs arising from deforestation, disruption of the ecological system, and other environmental degradation that would directly affect the agrarian economy were entirely ignored.

[24]Sayamol Kaiyuravongse, *People's Freedom of Access to Government Information* (*sitthi nai kam rab ruu khor mun khao sarn khong prachachon*) (Bangkok: Association of Rights and Freedom of the People, 1993), 50. The author also poignantly notes that most of the electricity generated is consumed by the industrial and business sectors (about 77% of the total), which account for only a small portion of the country's population.

[25]Ibid., 48-50.

There were several other incidents in which people were denied access to official information that could affect their lives and well-being and had to suffer the consequences. Such instances of social injustice became politicized by NGOs and academics who voiced their critical opinions through the mass media -- mainly through the privately-owned press.[26] A number of journalists also joined in publicizing the cause of the protests, which focused largely on environmental degradation. In the early 1990s, these movements expanded their concern to the information realm when issues were raised about government restrictions on information and the need for more access. A group of academics and activists, who had long been active in the NGO movement, spoke out to urge the government to allow a freer flow of information to the public, arguing its necessity on democratic grounds. Existing laws, they argued, did not provide adequate public access to official information. Government officials were accused of maintaining an arrogant attitude toward members of the public seeking access to official information. Critics stated that unless the people requesting information had money and power and special connections with relevant officials, they were bound to be turned down with a standard reply that "this document is a government secret."[27]

The above justification by government officials is, however, not entirely groundless. Prior laws that govern government information practices were primarily designed to protect national security and therefore emphasized the protection of official secrets. The prototype of such laws was first passed in 1940 to protect information about military installations, missions, plans, and projects. Over the years, many other types of official documents have come to be treated as government secrets. In the height of the insurgency crisis and dictatorial rule in 1968, the PM's Office issued a directive on national security which contained guidelines for government officials on how to handle sensitive information. The directive mainly covered documents related to national security particularly military information. In 1974, this directive was amended to expand the scope of sensitive materials -- ones not for release to the public -- to the files held by agencies and departments of the civilian bureaucracy. This directive, it should be noted, was amended and implemented during the year of the country's bloodiest military and police crackdown on pro-democracy demonstrators. Although the directive clearly divides sensitive government documents into categories and provides examples for each (see Table 8.1), it still gives the head of each government section or department the

---

[26]Except for a handful of programs developed by NGOs, the electronic media, which were still mostly owned by the state, tended to develop under close state control.

[27]Satchunij Pornpong, "Easy Access to Government Information is Vital in a Democratic State." *The Nation* , 17 September 1995, B 3.

Table 8.1

Levels of sensitiveness of government documents, definitions, and examples

Level of secret	Definition	Examples
Top secret	Information which could cause tremendous damage to national security if it were to fall into the hands of unauthorized persons or enemies of the state.	Sensitive national policies and strategies; bi-lateral treaties with other countries on certain affairs; military information relating to warfare; estimates of the enemy's military power and the country's need of certain natural resources; and research and development in scientific fields.
Secret	Information which could seriously damage national security if they fall into the hands of unauthorized persons or enemies.	Anti-terrorist plans and monitoring of suspected criminals.
Confidential	Information which could damage national prestige or that of government agencies.	Draft legislation, proposals to create, abolish or reorganize government agencies minutes of important meetings on policy matters; orders or declarations which are being processed, and documents on the government's handling of diplomatic problems with other countries.
Restricted	Materials for the use of authorized personnel only.	Handbooks and instructional materials for government officials handling sensitive issues; information about the need to purchase and acquire equipment and facilities; and the creation of official standards in trade and commerce.

Source: The Protection of Official Information Act 1940 (amended version) (*phra ratchabanyat kumkrong khwam lab nai ratchakarn phor sor 2483*) (Bangkok: Sutrpaisal Press, 1994), 19-24.

discretion in assigning the level of sensitivity of the information. As a result, most information is treated as government secrets and stored away without a retrievable system or service for the public, let alone a routine dissemination mode such as a government information index. The directive also does not stipulate the rights of citizens to appeal through the judicial system if they happen to disagree with a decision of the official regarding the information.

However, amidst the rising tide of support for democratic reform following the bloody clash between the armed forces and pro-democracy demonstrators in May 1992, the subsequent government became more responsive to demands by democratic movements.[28] In late 1992, for instance, the government passed the Environmental Promotion and Preservation Act which, for the first time, gave the public the right to obtain from government agencies and officials any information -- about projects, plans, and government contracts -- that may affect the environment. This government also set the tone for a more open attitude about releasing government information by making a government contract for a controversial two-million telephone line project with a private company publicly available.

More importantly, this government, which was uniquely composed of a group of well-known and experienced technocrats, appointed in 1991 a "committee for the improvement of state bureaucratic administration" out of which come the draft bill for the freedom of official information act. A member of the committee, a local university professor and activist, was the author of the very first draft of the new legislation. Like many of his peers in the ongoing democratic movement, he wrote the draft out of a belief that allowing public access to official information would also encourage greater public participation in the government's decision-making process, which would help discourage corruption by government officials and serve as an effective check on the power of the country's administrators.[29]

In late 1991, a seminar was jointly organized by the Institute of Policy Studies and the Association of Social Science of Thailand to provide a platform for the exchange of ideas and opinions about the draft legislation. As a result, new input was solicited from participants in the seminar -- mostly NGO representatives, academics, and journalists -- and changes were made to the draft. It was not until late 1992 under a newly-elected government that the new

[28]It should be noted that the government at the time was headed by PM Anand Panyarachun, a former diplomat-turned-businessman. In his second term as prime minister, Anand and his technocratic team of ministers passed several new laws and initiated new and constructive practices in the government bureaucracy.

[29]This first draft was written by Thienchai Na Nakorn, a faculty staff of law at Sukhothai Thammathirat University. See Thienchai Na Nakorn, *Proposal for the Freedom of Official Information Act and Draft of the Freedom of Official Information Act* (Institute of Policy Studies and the Association of Social Science of Thailand, 1992).

bill carrying its current title would make it to the legislature.[30] Then, the draft bill was presented to parliament by members of the Palang Dharma Party (PDP). In the beginning, the proposed draft failed to win approval from the Ministry of Defense and Interior when the parliament forwarded it to concerned government agencies for comment. The Office of the Juridical Council had to step in to modify the draft by adopting ideas from existing laws in other countries and trying to find a middle ground that would be acceptable to all concerned local government agencies.

Although both the original draft and the improved version of the Office of the Juridical Council were accepted in principle by the Chuan Leekpai government in 1994, they were aborted when there was an abrupt dissolution of the House in June of that year. During the subsequent government, another version of the draft for the same law was written and proposed to parliament by members of the Chat Thai and Democrat Party. It would take another House dissolution (in September 1996) and change of government before all the three drafts would finally be made into a law. In early 1997, the three drafts, which had overlapping contents and were considered concomitantly, sailed through the lower House, making their way to the Senate where several new articles were added. The new legislation was enacted in September 1997 after being declared in the Royal Gazette. It became in effect three months later.

According to a review by a local legal scholar, the new law has two important objectives: 1) to grant the public the right to be informed about "official (government) information" with certain exceptions of non-disclosures; and 2) to protect privacy rights associated with personal information as contained in government files.[31] Judging from the history of the law, however, it is dubious whether the second principle is really an intended objective or a hidden yet compromised agenda. By comparing the content in the section on "personal information" in the first draft of the proposed law and the one in the enacted version, it is clear that tremendous changes were made during the drafting process. In the first draft, only two articles address "personal information" and to regulate matters of use limitation and disclosure of information. In the enacted version, however, the entire section is dedicated to the management of personal information in government files with much more extensive details and stipulations.

[30]The newly-elected government was led by PM Chuan Leekpai from the Democrat Party.

[31]Charnchai Sawaengsak, *Useful Information: The Freedom of Official Information Act B.E. 2540 (1997)* (*sara naroo phraratchabanyat khomunkhaosarn khong ratchakarn phor sor 2540*) (Bangkok: Vinyuchon, 1997), 47.

The section entitled "Personal Information and Data" contains five articles the content of which clearly imitate the eight basic "fair information practice" principles of the OECD's Guidelines for the Protection of Privacy and Transborder Flow of Personal Data (see Table 6.3 in chapter 6). For instance, article 23 under subsection 1 and 2 reads like the collection limitation principle, to wit:

> 1) Government agencies are to ensure that their personal data systems be relevant and necessary with regard to the purpose for which they have been created and that they be discontinued when they are no longer deemed necessary;
> 2) Government agencies must attempt to collect personal data by obtaining it directly from the owner of that information, through lawful and fair means, particularly in cases where the information may directly affect the person's personal interest.[32]

Although the legislated version may contain detailed regulations that follow internationally recognized principles of data protection, it can only grant a freedom of information that is significantly compromised. Unlike the original version of the draft, where an individual is given the right to file suit against the government and to seek punitive damages for the violations of his or her personal data -- unauthorized use and disclosure with adverse effects to the data subject,[33] the legislated version does not have these provisions. It is left understood that to pursue such action, the individual would have to seek solace in other laws or constitutional provisions.

Besides providing no provisions on lawsuits and damages, the stipulations on the protection of personal data in the new legislation are, like the constitutional provision on information privacy, invariably subject to limitations. Take article 23 under subsection 3 which adopts the idea of the openness principle, for instance. This article requires that government agencies regularly publicize and update in the Royal Gazette the following:[34]

> a) categories of persons from whom information has been collected and stored in the agency's personal record-keeping systems;
> b) categories of personal record-keeping systems held by the agency;
> c) the nature of the use of information in the system;
> d) the means for the owner of the information to inspect his or her personal data;

---

[32]Ibid., 73.

[33]Thienchai Na Nakorn, "Proposal for the Freedom, " 48.

[34]In Thailand, the Royal Gazette or *ratchakijjanubeksa* in Thai, serves as an official means of publicizing or acknowledging the existence of new laws, their nature, and the main purposes of their use.

e) the means for the owner of the information to correct his or her personal data:

f) the origin of the information.[35]

While the above provisions may reflect the general principle of openness about developments, practices, and policies with respect to personal data, holes appear with the exceptions set forth in article 20. According to this article, the National Intelligence Office, the National Security Council, and other government agencies as prescribed in the Ministerial Orders (to be subsequently enacted) can bypass the above requirements in article 23 (3), with the approval of the Office of the Official Information Committee. Once again, the customary upholding of national security prevails over the legal measures to protect personal data.

More disturbing loopholes in the form of exceptions are found in article 24, which articulates the principles of use limitation and disclosure limitation. This article forbids government agencies to disclose personal data in their record-keeping systems to other government agencies or to third parties without first obtaining the informed consent of the data subject. However, a number of problematic exemptions again punch holes into the protections promised. These exemptions include disclosures for the following purposes: internal uses, planning, statistics, census, research, national archives, criminal investigation and litigation, and matters of life and death. Furthermore, the court, government officials and/or government agencies or departments that are identified as the appropriate authority by other laws are allowed to obtain information about data subjects from any government database. This lengthy list of exemptions closes with an open-ended provision to allow as exceptions any other cases that may be stipulated in subsequently enacted royal decrees.

In addition to the above provisions and guidelines, this freedom of information legislation new law also created a new measure of assistance for individual citizens, in the form of the Office of Official Information Committee (OOIC). The committee, which is chaired by a minister appointed by the Prime Minister, is comprised of twenty two appointed members. Thirteen are high-ranking officials from the government bureaucracy, and eight are experts appointed by the Cabinet from both the public and private sectors.[36] According to article 28 of

---

[35]Charnchai Sawaengsak, "Useful Information: The Freedom of ," 73.

[36]According to article 27 of the law, the following high-ranking officials are to sit in the committee on government information: permanent-secretary of the PM's Office, permanent-secretary of the Ministry of Defence, permanent-secretary of the Ministry of Interior, permanent-secretary of the Ministry of Commerce, permanent-secretary of the Ministry of Foreign Affairs, permanent-secretary of the Ministry of Agriculture and Cooperatives, secretary-general of the Office of the Juridical Council, secretary-general of the Office of the Committee of Civil Servants, secretary-general of the National Security Council, secretary-general of the Parliament, director of the National Intelligence Office, and director of the Budget Office.

the law, the committee is empowered to oversee and advise government officials and agencies in matters related to official information. As far as personal data is concerned, the committee is granted powers to investigate and advise on complaints filed by individual citizens regarding alleged violation of their rights. The scope of these investigations includes violations of disclosure rules, and agency failures to grant access and/or to amend records as requested as regulated by the act. The committee is also required to produce a periodic report to the cabinet at least once a year on provisions listed in the act.

I have doubts about this new committee, as well as the new legislation itself, when it comes to the protection of personal data. While the committee may be granted some oversight powers regarding the handling of personal information in all government files, it is not likely they will act as an effective mechanism to ensure enforcement of the principles embodied in the new law. First of all, given that all committee members have full-time jobs and convene on matters concerning government information only periodically (or whenever a complaint is received), they are likely to be too preoccupied with their regular work to devote time to enforcement of the act on a par with their full-time counterparts in Europe or Canada. Secondly, as more than half of the committee members are high-ranking government bureaucrats, their views are bound to be shaped by what is considered acceptable practice in government bureaucracy. This bureaucratic predisposition aside, there is also the stark reality of patronage relations which is endemic in the Thai bureaucracy. Likewise, it is hard to imagine what would motivate some of these bureaucrats to reprimand government officials or agencies for non-compliance with, say, use and disclosure provisions of the act.

Regardless of whether they are adequately motivated, the committee is almost powerless when it comes to the imposition of penalties for non-compliance in the area of personal data protections. Civil and criminal liability for violations of the act are reserved almost exclusively for unauthorized disclosure of "sensitive government information" (article 20 under Part II: sensitive information which shall not be disclosed).[37] The only liability enforceable by the committee in the case of personal data is when a person summoned to testify, produce evidence, or appear as witness for the committee's investigation fails to comply.[38] There is no statute on liability cases of denied requests for access to a personal record or unauthorized disclosures of personal information in government files. Although a data subject may register a complaint concerning unauthorized disclosure of his or her personal

[37]According to article 41(under section 7 of the act), violators in this category are subject to a maximum of one-year imprisonment or a maximum fine of Bt20,000 (about $525), or both.
[38]In such cases, the person is liable for a maximum of three-month imprisonment or a maximum fine of Bt5.000 (about US$130), or both (article 40).

information through the committee, he or she still has no legal basis for a lawsuit against the government or for compensation even if the disclosure affects him or her adversely.

It is evident that the focus of this bill, as its name suggests, is on granting public access to official information, which has been inaccessible in the past, rather than protection of information privacy. Data protection is merely a bonus that comes with the new legal package. According to a local and well-respected lawmaker who has been involved in many important legislative processes including this one, the inclusion of the part on protection of personal data in the new law is an initial step towards further legislative efforts in the future. Since public awareness about data protection is still minimal, it made sense to introduce the issue to the legislature under the umbrella of access to government information, which is a more timely topic and one that has significant public support. Also, by incorporating data protection within the freedom of government information act, defensive government agencies are more likely to let their guards down due to the pressure from representatives of the public who have been vying for a greater access to government information.[39]

Despite its shortcomings and long lists of exemptions, the section on data protection in the new bill is not without merit. First, because of the political basis of the law, the technique used in information storage -- manual versus computerized -- is not an issue. Personal information is broadly defined to cover both manual and computerized personal records. That both types of records are subject to regulation is a good thing since government tampering with manual records can be just as dangerous. Also, the rules and principles incorporated in this part of the law definitely represent an improvement over the previous status quo since they recognize, in principle, that the individual citizen has a legitimate legal interest in the information pertaining to him or her contained in government files. This is a step in the right direction, but the state still clearly has the upper-hand over Thai citizens. As things are, it is difficult for the new law to be an effective measure to redress the power imbalance between individual citizens and the state. The OOIC notwithstanding, the enforcement of the act depends more on the initiative of individual citizens since an investigation can be launched only when there is a complaint registered.

Between 1997 and 1998, a total of thirty-two complaints were filed with the OOIC. Most of the complaints registered were triggered by failed requests for access to supposedly confidential information held by government agencies. Of all the 32 complaints, there was

[39]Dr. Borvornsak Uwanno, Dean of Faculty of Law, Chulalongkorn University, interview by author, 11 October 1998, Vancouver, Plazcek Residence, Vancouver.

none that directly raised the issue about violation of personal information by a government agency. In one of the cases. a parent had requested on his daughter's behalf for the release of her raw scores on the countrywide university entrance examination from the Ministry of University Affairs but was turned down. So he filed a complaint with the OOIC. From the OOIC's perspective, one of the major points of debate in this case was whether the requested score reports should be considered "government information" or "personal information." In other words, freedom of information was seen to be in contention with personal privacy. In the end, the committee ruled that "since the score report is in the possession and control of the Ministry of University Affairs, which is a government department, it is a government information." Therefore, the requester should have the right to inspect it.[40]

A similar complaint was also filed by a mother of another child who failed the grade 1 entrance examination of a primary school affiliated with a prominent public university. Questioning the transparency of the exam, this parent lodged a complaint with the panel of the OOIC and has been campaigning publicly, mainly through the mass media, for the disclosure of the exam results. At first, the university administration, following the OOIC's order, agreed to disclose the exam results but only exclusively to the complainant, citing the need to protect the privacy of other students whose scores were also included in the sets of results. However, the complainant was not satisfied with this resolution as she wanted a third party, in this case a member of a local press, to also witness the sets of exam documents. Like the above case, this case of seeking access to an "official information" clearly bordered on violating personal privacy rights. But since privacy was almost completely overshadowed by the freedom of information wave, the privacy issue was never brought up in the media. Press reports focused mainly on the controversy sparked by the case and how it has led at least three other individual and organizations, including a relatively new NGO called the Society of Information for the Public, to file a request to Kasetsart University, the university in question to unveil the exam results. In the end, the Ministry of Education launched a probing investigation into the exam and student selection processes at the school.[41]

---

[40]Office of Official Information Committee (OOIC), *Annual Report of the Committee on Government Information (1997 - 1998) (rai ngan prajam pi samnak ngan khana kammakarn khor mun khao sarn khong ratchakarn)* (Bangkok: Ministry of PM's Office, 1998), 17-18.

[41]See, for example, Supara Janchitfah, "Teething problems for the new Official Information Act," *The Bangkok Post*, 20 December 1998, C 6, and Sirikul Bunnag, "Sumalee to check school entrance exam scores," *The Bangkok Post*, 23 March 1999, A 2.

272

THE ASPIRATION TOWARDS AN "INFORMATION SOCIETY" – ANOTHER DRIVING FORCE OF POLICY CONVERGENCE?

As discussed in the context of the development of an "information society" in chapter four, the Thai state is expected to provide a role model for ICT diffusion in Thai society. In assuming this role, it is also expected to remove obstacles that may stand in the way of realizing the central aspiration. Among the major obstacles that a 1995 National Electronics and Computer Technology Center (NECTEC) report suggested should be dealt with are the outmoded telecommunications law and the lack of information laws, particularly those that address automatic information-processing. Although the two are separate legislative areas, the report's approach to them are fundamentally the same; that is, to reform or design them to make them more relevant and accommodating to modern technological and global business environments. With regard to information laws, the report is explicitly concerned with "the introduction of legislative measures that are useful to facilitate and promote IT use in society."[42] Prioritized issues include the legality of electronic orders or signatures, data and information ownership, freedom of public information, and personal privacy protection. Since the report gives no precise definitions for "freedom of public information" and "personal privacy protection," and makes no effort to associate them with limiting surveillance, it is safe to assume that these legislative concerns are taken plainly at face value. Void of any political or philosophical groundings, such legislative matters are reduced to instruments to meet the technical requirements for the envisioned information society.

In the same vein, NECTEC published in 1996 another report, which came out of a study it sponsored to research the legal implications of the introduction of an electronic data interchange system (EDI) in Thailand.[43] The research team for this study was comprised of high-profile academics from diverse backgrounds including computer science, electrical engineering, public policy, and law. The report concludes that there are three areas of law which need modification or creation in order to accommodate EDI applications in Thailand. One of these is data protection legislation.

---

[42]National Information Technology Committee Secretariat, "Towards Social Equity and Prosperity: Thailand Information Technology (IT) Policy into the 21st Century," (Bangkok: National Electronics and Computer Technology Center, 1995), 13.

[43]See Chula Unisearch, *The Project to Study Laws Related to Electronic Data Interchange (EDI) in Thailand : a Complete Report (khrong karn seuksa kot mai karn laek plian khor mun duay seu electronics nai prathet thai)* (Bangkok: NECTEC, 1996).

Before arriving at this conclusion, the report briefly reviews other privacy and data protection legislation efforts in industrially advanced countries and the recent enactment of data protection law in Hong Kong. Consistent with the 1995 report, this study views the passing of data protection law in other countries as basically economically motivated. The purpose of such legislation, it is argued, is the protection of the rights and economic interests of individuals whose personal information is kept in computerized databases. This protection is based on "creating a proper balance between individuals' right of privacy and new ICTs which are privacy-eroding by nature."[44] The study also briefly identifies three principles that are said to govern information practices in overseas legislation: data quality, individual participation (right to inspect and verify), and use limitation.

According to the report, the Thai legislature needs to pass a data protection law as quickly as possible because "this law is crucial to strengthening Thailand so that the country will become internationally recognized as readily equipped to develop into a full-fledged information society."[45] The content of the law, says the report, should be developed out of existing data protection laws in other countries, with special consideration given to the EU Data Protection Directive. It was never made clear why the EU directive is given the emphasis.

In addition to the NECTEC report, another study on a similar topic came out in 1996 featuring an effort to draft a guideline for a data protection bill for Thailand and to explore the perceptions and viewpoints of experts in related sectors about the draft bill.[46] The study, which was authored by two academics at Chulalongkorn University in Bangkok, was sponsored by the National Research Council.[47]

Unlike the NECTEC report, which was only exploring any possible legal problems that might arise from EDI applications and giving broad recommendations, the latter study had clear and specific objectives. The study's objectives were laid out, in chronological sequence, as follows: to study data protection acts and privacy acts of various countries; to develop for Thailand a draft for data protection and information privacy legislation using the studied foreign laws as a model; to obtain and analyze experts' reactions to the draft; and to propose a guideline

---

[44]Ibid.

[45]Ibid., 5-85.

[46]See Pateep Methakunavudhi, "A Guideline for Data Protection Legislation in Thailand," *Computers and Society* 30 (September 1998): 28-30.

[47]Pateep Methakunavudhi and Apirat Petsiri, *A Guideline for Data Protection and Information Privacy Legislations in Thailand (Naew thang nai karn ork kotmai khum khrong khor mun lae sarn son thet suan bukkhon nai prathet thai*) (Bangkok: National Research Council, 1996).

for data protection and information privacy legislation in Thailand (by using these experts' ideas and opinions as input in revising the original draft). This study had a well thought-out research design with appropriate methodologies, a comprehensive report of research results, and lucid recommendations.

Nonetheless, the research undertaken is, like the NECTEC study, primarily administrative in nature. The researchers assume a generally value-neutral position, maintaining no ideological positions on the topic studied. They also offer very little historical background and almost no cultural considerations in the positioning of data protection laws in the Thai context.[48] The rationale for the study echoes the same rhetoric as that in the NECTEC study -- the need to modernize the country's legislative structure to cope with the changing technological and business requirements of the emerging global information society. The pressures to keep pace with the changing technological environment and to appear "modern" in the perception of other countries are placed on a par with concerns about citizens' rights and interest. As stated in the study's expected contributions,

> ...to stimulate public interests and recognition of the importance and necessity of data protection so that wrongdoing and abuses of personal data can be prevented; and to create a good image of the country in the eyes of trading partners.[49]

Although the study makes clear that protection of "privacy" is its central concern, the term is defined most generally as "freedom or liberty from intrusion in person or in business."[50] Data protection is seen as a segment within the right of privacy, more specifically -- "the part that addresses the principles in collection, management, use, and processing of personal data."[51] According to the study, there has been little public concern in Thai society about information privacy and security of personal records, despite the widespread use of computers in both the public and private sectors. The researchers frame their privacy concern mainly in terms of security and accuracy of personal records and unauthorized disclosure and use in a computer-mediated environment, rather than examining issues of social control and technological surveillance and fundamental rights of and protection of natural persons from such control and surveillance.

---

[48]The two researchers did point out to sociological and anthropological ideas that privacy is culturally constructed and may not be a basic need in every society. It is with this consideration, they say, that they devise questionnaires to solicit opinions about the draft data protection bill from local experts in various fields.
[49]Ibid., 6.
[50]Ibid., 8.
[51]Ibid., 9.

While the researchers acknowledge anthropological and sociological theorizing that privacy is culturally constructed and may not figure as a basic necessity in all societies, they openly review and use as their drafting model privacy and data legislations in seven countries most of which are in the West with their own culturally specific ways of thinking about privacy. The legislation reviewed includes the following:

1) Swedish Data Act (1973);

2) US Privacy Act (1974);

3) French Legislation on Data Processing, Files and Liberties (1978);

4) Japanese Act to Protect Personal Information Kept by Government Organs by Means of Computer Processing (Personal Information Act) (1988);

5) Australian Privacy Act (1988)

6) Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981); and

7) Commission of the European Communities' amended proposal for Council Directive on the protection of individuals with respect to the processing of personal data and on the free movement of such data (1992).

Following the summary review of all the above documents, the study came up with its own version of a draft for the Thai information privacy and data protection law. Generally, this draft law adopts its regulatory model from prior statutes in Western European countries -- Sweden, France, and the United Kingdom, among others -- with the licensing approach to data protection. Like its European prototype, the Thai draft proposes the creation of a Data Inspection Board in Thailand and assigns it with the authority to oversee the collection and dissemination of personal data, to regulate the usage of the resulting personal files, and to enforce a system of responsible keepers for computerized data banks. The draft law establishes a detailed set of duties for such keepers by enforcing upon them the customary code of fair information practices. The Data Inspection Board is also authorized to launch an investigation into any keeper's personal file system if a complaint has been filed with sufficient evidence. There are also stipulations on criminal penalties for breach of the Act.

Although the draft contains provisions on the protection of personal data that are worthy of consideration, it is also inherently problematic in many aspects. First of all, this draft legislation tends to concentrate only on automated data. One of the mandates states that it is unlawful to maintain a database of personal information (the exact term used in the report was "personal file") in machine-readable form without first applying for and obtaining a license

from the Data Inspection Board. While the reason for targetting only automated data may be simply a pragmatic decision to avoid the heavy workload of registering all personal data systems, it is still a known fact that manual records can be equally invasive of privacy. In Thai society, in particular, abusive information practices tend to take place in the most informal of settings shaped by patronage relations system. Often, this involves the mismanagement of manual files.

Secondly, although the main intent of this draft law, as its name suggests, is to protect personal data and information privacy, it contains no explicit definition of "personal privacy." Article 22 (1) of the draft law provides that "the Data Inspection Board will examine whether the automatic processing of personal information excessively encroaches on personal privacy"[52] but it stops short of indicating how the Board should define "personal privacy." Given a socio-cultural historical and contemporary context that is not particularly sensitive to privacy, it is certainly difficult to come up with suitable definitions for the term within the drafted statute. Yet, the lack of a more precise legal definition could result in confusion and problems of interpretation in the future.

The ambiguity in terms and definitions in this draft law is not limited to "privacy" and "encroachment" alone. "Personal data," which should be the most basic term, is defined briefly yet broadly as "data which concerns a natural person."[53] Evidently, this definition is not very helpful since it still contains another undefined term "data" -- that is also subject to many interpretations. Another more central term that is used consistently throughout -- "personal file" -- is generally equivalent to databases of personal information. Article 3 of the general provision of the draft law defines "personal file" as "files, lists, or other notes, kept in automatic and identifiable form, that refers to an individual person."[54] That this draft legislation does not give the same weight to nor use the same meaning for "personal data" as that in the recently-enacted freedom of government information act reveals that the two laws are not entirely compatible and that their drafters did not coordinate their efforts.[55] David Flaherty discusses briefly a situation in the US where the incongruity between two laws -- the

---

[52] Ibid., 154.
[53] Ibid.
[54] Ibid., 133. "Personal file" is referred to in Thai with a literal meaning as "faam suan bukkhon."
[55] In the freedom of official information act, "persomal data" is defined as "any information relating to an identified or identifiable natural person, such as education, income, medical records, criminal history, professional background, or any information that contains the name or identification number of that person, or anything that contains identifiable attributes of the person such as fingerprints, voice-recording cassette, photographs, including identifiable information about a deceased person. Charnchai Sawaengsak, "Useful Information: The Freedom of ," 102.

Access to Information law and the Privacy Act — resulted in the former being used to circumvent the provisions in the latter.[56] Obviously, this is something that the drafters of the Thai draft law need to consider.

Based on the wordings in this draft legislation, it is also unclear whether personal files maintained by government agencies are necessarily covered by the statute. There is no indication in the general provisions of the draft law how to differentiate between public and private agencies. The same is also true of the provisions on permission and licensing to maintain personal files in Section 1 of the draft. Article 4 under this section simply states that "all personal files are to be created and maintained by persons or agencies who have applied to and obtained a license from the Data Inspection Board only."[57] However, the draft legislation also contains a number of provisions that list exemptions from the above stipulation. For instance, the same article lists as an exemption "data files which are created under the agreement of the government." There is no clarification if "the government" refers to only the cabinet or government agencies and the bureaucracy in general. Similarly, article 10 of the draft law provides that "responsible keepers of all personal files are to ensure the correctness and currency of the information in their files" but rules as an exemption "personal files kept by government agencies and used for the objectives in line with the operation of those agencies."[58] Considering that government bureaucracies are by far the greatest collector and manipulator of personal information in Thailand, the point of enacting this draft law will be entirely moot if it fails to include government agencies.

In addition, the draft law also fails to provide details on the composition and characteristics of the Data Inspection Board who evidently are to play a pivotal role as an enforcement and supervisory mechanism for the developed statute. Section 6 of the law provides that members of the Board shall be appointed by the Prime Minister and that the Board members shall not exceed six years in each appointment term. Members of the Board must also not be older than sixty five years of age. Nothing is mentioned about the qualifications, personal backgrounds and preferred characteristics of the Board members. As David Flaherty could not emphasize enough, an enactment of a data protection law alone is not adequate to control surveillance; an effective agency charged with the implementation of the law is equally, if not more, important. Flaherty accords the same importance to the personality of the privacy or data commissioner, whom he sees as a major ingredient to success in data

[56]David H. Flaherty, *Protecting Privacy in Surveillance Societies*. 248.
[57]Pateep Methakunavudhi and Apirat Petsiri, "A Guideline for Data Protection." 136.
[58]Ibid., 142.

protection. Aside from experience in the area of privacy and data protection, good data protectors also need to have strong leadership, a firm ideological position, and to be articulate activists. That these considerations do not appear in the Thai draft legislation may be a simple reflection of the fact that controlling surveillance is simply not the concern of the authors. Their understanding of the role of the Data Inspection Board appears to be only superficial and one that transpires in a socio-political vacuum.

In spite of the inherent contradictions and problems described above, the draft law was generally considered a good idea by the selected team of experts who were invited to comment on it. These experts came from three groups, each group consisting of ten representatives from the following sectors — general, education, and law and administration. Those in the general sector were professionals from such business concerns as manufacturing, distribution, services, data processing, import and export trade, state enterprises, and hospitals. In the educational sector, experts were recruited from computers and engineering and from law. As for those in the legislative and administrative sector, a selected group of civil servants from the Ministry of Interior, Ministry of Justice, Department of Police, Office of the Juridical Council, and parliament were invited to provide opinions.

These experts tended to welcome the benefits of the new draft law in three general areas: promotion of the right to privacy and data protection; establishment of guidelines and ground rules in information management with an oversight mechanism; and contribution to national development by fostering an international recognition of the country's modern legal standing. One of the computer academics who was not named was quoted as saying that the passing of a data protection law was long overdue in Thailand. Eight years ago, he said, he had pushed for such a law to be enacted, but there was not enough interest and awareness of the social implications of computers at that point in time. However, a few members in the same group were also concerned about disadvantages and inconvenience (in doing business) which might arise from the highly bureaucratic and regulatory mode of control of personal data systems as proposed in the draft law.

Opinions also varied as to the urgency in passage of such a law. According to an expert in the general group, a more immediate problem was the protection of business data, particularly with regard to security safeguards. This was perceived as a more pressing matter than protection of personal privacy because of its looming economic implications. Another expert in the legislative and administrative sector voiced a concern that the passing of a data protection law would be a stumbling block in the ongoing development of data processing in

both the public and private sectors in Thailand. The legal implications of such law, it was argued, might discourage some people from endeavoring in ICTs or other data-processing activities. He argued that "To rush into such a legislation scheme at this early stage of technological diffusion may be a disservice to national development."[59] This expert thus felt that the enactment of the law should wait until ICTs had diffused more pervasively in society. Meanwhile, another expert in the same area observed that as the idea of data protection was quite new for Thai society and without adequate public awareness, the effort to pass a new law in such an area was likely to be futile. On this note, several members of this expert team raised doubts about the viability of the draft law in practice.

Experts who were law professors tend to limit their criticisms to the more technical elements of the draft law. A few commented on the ambiguity of terms and definitions used. One argued that "privacy" needed to be more properly defined by giving due consideration to Thailand's socio-cultural background. Another felt that the overall draft lacked a genuine structure of an Act and was merely a collection of fragmented statutes from different laws. Furthermore, the draft law was said to inadequately address such aspects as individual participation -- access to personal records so that the accuracy of one's data can be verified and the keeper's information-handling checked -- regulatory mechanism, and compensation and liability in cases of abuse. While agreeing with the basic principles of data protection, these law academics did not endorse the idea of passing entirely new legislation at the present time given the local conditions wherein data protection and privacy were barely understood by the local public. It was proposed instead that these fair information practice principles be incorporated into existing laws and regulations such as the penal code, professional codes of ethics, and departmental policies and regulations, or issued as a guideline for future legislation.

In addition, there were a few comments made about the need to control linkages between different databases of personal information. One law professor was particularly critical of the massive computerized database of citizen information held by the Ministry of Interior's Registration Administration Bureau and the plan to establish interagency data linkage to more departments. His remark, however, was only cautionary and did not contain any suggestion as to how to deal with such government surveillance.

Many of the ideas and comments of the thirty experts consulted were incorporated into the second version of the draft law which will, according to the authors, be proposed to the

---

[59]Ibid., 90.

legislature for consideration in the future. This revised version maintains the same rationale as the original draft but puts more emphasis on the importance of data protection legislation to national development. Part of the rationale reads,

> Since 1973, many civilized countries have passed privacy and data protection legislations. However, Thailand does not yet have such law in place. Since it is the national goal to become an economic, trading and industrial center in Southeast Asia, it is therefore necessary to prepare in advance the drafting of the data protection or information privacy law...[60]

Like its antecedent, the revised draft law also refers to the need for Thailand to comply with international guidelines for data protection and transborder data flow. Interestingly, the OECD's Guideline and not the recently-decreed EU Directive has been referred to as the basis for international harmonization of data protection law. It was never made clear in the draft why the OECD's Guideline was given more significance.

In general, the revised draft law is an improvement over the original draft in many aspects. For instance, the general provision clearly specifies that the licensing and fair-information practices statutes will apply to both government and private agencies that are keepers of personal-data systems, with few exceptions.[61] Based on the definitions of terms and succeeding provisions, it can well be assumed that both manual and automated files are protected under the statutes of the draft law.[62] Aside from the expanded scope of the law, there are also two newly added sections in the revised draft. One addresses in detail the disclosure and use of data in the personal register (same as "personal file" in the original draft), while the other takes up the issue of access to and correction of information in the personal register by the data subjects. Both are areas of data protection that were overlooked and inadequately covered in the original draft.

In addition, the revised draft has more detailed provisions about the composition, qualifications and background of candidates for the renamed data protection agency -- the Personal Data Protection Committee, the "Data Inspection Board" of the first draft. According to article 4 in the general provisions, the Personal Data Protection Committee shall be appointed by the Prime Minister and be considered an official entity within the Ministry of

---

[60]Ibid., 132
[61]It should be noted that there are fewer cases of exemptions from the licensing mandate in the new draft law when compared to the original draft. These exemptions include criminal record databases, and personal data systems that are crucial to national security, international relations and international policy.
[62]The revised draft law uses two separate terms to refer to manual and computerized data -- personal data (*khor mun suan bukkhon*) and processed personal data (*sara sonthed suan bukkhon*).

the Prime Minister's Office. Article 29 mandates that the committee be comprised of no more than ten members, who shall be appointed according to expertise or specialization in the following areas: national security, economic and fiscal policy, international trade, law and order, social security, civil and human rights, and information and communication technology. Aside from their licensing duty, the committee is also assigned in advisory and supervisory role over personal record-keeping organizations as well as authority to appoint a data protection sub-committee to assist with the committee's operations when needed. More importantly, the Personal Data Protection Committee is given regulatory power if a public agency or private organization fails to comply with the fair-information-practices provisions. Article 45 of the revised draft law states that the Committee has the power to impose on offenders statutory sanctions — withdrawal of licenses, fines, and criminal prosecution — depending on the seriousness of the breach.[63]

Despite the many changes made, this revised draft law is far from impeccable. Like its predecessor, the revised version fails to achieve compatibility with the freedom of official information act in its definition of the most commonly used term — "personal data." In fact, "personal data" or *khor mun suan bukkhon* in Thai is never properly defined but is referred to consistently alongside "processed or automated data" or *sara sonthed suan bukkhon* — defined as "information which have undergone processing by devices or procedures that rely on computers and telecommunications technologies."[64] There was also no effort to define "privacy" nor to situate it in the Thai context.

As this draft is still in its early stage of what could be a lengthy legislative process, it is likely to undergo more revisions and modifications in the future. Thus, all the criticisms and analysis made of it now may prove fruitless when the actual legislation surfaces. The real hurdle, however, is more likely to be felt in the implementation process. Unless a massive education effort is launched to prompt awareness about data protection and privacy issues, the new legislation is bound to be meaningful to only a small minority of the population. In fact, a public awareness campaign as such may not necessarily succeed in securing public interest in the issue. Data protection is a learning process and one that may take a long time to take root especially in a "surveillance society" like Thailand. Under these circumstances, it much depends on the regulators, provided that they are sincere in promoting data protection and privacy interests by developing an understanding about these concepts and issues in society

---

[63]According to article 50 of the draft law, the Data Protection Committee is authorized to impose a penalty in the form of a fine on offenders of the law up to a maximum amount of Bt5 million (about US$15,000) and to sentence offenders to a maximum three-year jail term, or both.
[64]Ibid., 134.

and by clarifying how individuals might be harmed by the lack of protection. However, the revised draft law prescribes no such educational mandate for the Data Protection Committee. A statutory provision that comes closest to the pursuit of such a role is the function to "promote research and development of privacy-enhancing technologies and data protection principles." (article 37 (5)). Even if there is such a role prescribed, it is unclear if the committee, given the diverse backgrounds of its members, will be able to work in collaboration to pursue that mandate. It should be noted that at least half of the committee members are representatives from the sectors that are inclined to support data surveillance; for instance, national security, law and order, social security, economic and fiscal policy. Therefore, if the committee makeup remains unchanged in the actual legislation, its watchdog role in data protection matters will remain in serious doubt.

These recent public policy and legislative efforts concerning data protection in Thailand may be further evidence of ongoing international policy convergence in this area. In the Thai case, convergence is quite apparent in policy content and policy instrument. This is because the existing legislation in other countries and international agreements, which have clear overlaps, were used either as blueprints or for reference by the Thai public policy and legislative community. While the Thai initiative to conform to the international institutionalization of data protection could be attributed partly to the penetrative effect of the influential EU directive, this is certainly not the only reason. The larger and more important motive lies in the desire of a group of local elites to facilitate an ICTs-oriented course of development which, they feel, is "the way" towards the future. The introduction of policies and laws that address data protection is reduced to producing means for achieving that future vision, one which clearly embraces the assumptions of a technological imperative, a perspective that has swept most economic and political elites worldwide. In fact, data protection law is one of many information-oriented laws, or in the Thai term, "information technology laws," (*kot mai technology sara sonthed*) that the Thai information policy authorities plans to launch in the near future. Aside from data protection, other draft legislations that the National Information Technology Committee (NITC) is working on addresses the following areas: computer crime, electronic data interchange (EDI), electronic signature, electronic transfer of funds, and information infrastructure. Six sub-committees have been assigned to study the standard of international laws in each of the six respective areas before drawing up six draft laws for submission to the legislature.[65]

---

[65]Pichet Durongkaveroj, director of the National Information Technology Committee Secretariat, interview by author. 20 August 1996, Bangkok, National Electronics and Computer Center (NECTEC), Ministry of Science and Technology, Bangkok.

CONCLUSION

While the supposedly emerging information age may have raised fears of loss of privacy in the West, it has provoked little of such sentiments in Thailand. The preoccupation with the technological catch-up that the "information society" embodies has overshadowed these less intangible concerns, especially in the policy sector. Ironically, however, in the face of this powerful technological imperative and in the absence of perceivable public concern over privacy, technological change may yet generate a greater awareness about personal privacy in Thailand. As evidenced in the ongoing legislative and policy efforts in data protection, the motivations behind these efforts may be mainly economic and technological, but the end result can lead to an improvement in the level of information privacy. Nevertheless, one should not be misled into seeing these policy movements as altruistic endeavors to curtail government surveillance or to protect citizens' right of information privacy. The data protection draft law is indeed a regulatory endeavor for and by the elites and is likely to be executed in a top-down fashion, with little input from the bottom up.

Aside from the ongoing technological diffusion of ICTs, there is another, and possibly more important, force that has put information privacy on the legislative and public policy agenda. This is the democratic movements that have grown since the 1980s, which gave rise to the recent enactment of the freedom of official information bill, which includes a section on the protection of personal data. Although the political basis of this law may carry more weight than the data protection draft bill above, the fact that data protection is merely an appendage to the law may undermine its significance. Besides, the enactment of the new law is not likely to bear any fruitful results unless it is accompanied by a public education program that will arouse public interest and incite demand for realization of information rights, both in terms of access to government information and protection of personal data.

The gradual expansion of democratic freedoms and rights for individuals in Thailand has finally begun to penetrate the information realm in the 1990s. This realm, as the preceding analysis has shown, has been a site of social control and social struggle between the state and society of people for centuries. Whether the legislation and policies recently launched and in the process of being introduced will amount to counter-measures against government surveillance, and to what extent, remains to be seen.

284

CHAPTER 9

CONCLUSION

In his recent book, *Visions of Privacy*, Colin Bennett explores the following theme "whether the privacy solutions of the past are equal to the surveillance challenges of the future." While this is a worthy issue, it is clear that this thesis is not intended to address it. In trying to bridge the two parts of the thesis together, I find myself faced with a somewhat contrary question: "whether the emerging privacy regime will suffice to cope with the firmly institutionalized state surveillance that has been re-engineered with new technologies?"

Unlike Bennett's work which draws entirely upon the experiences of western industrialized countries where privacy is a significant value for most citizens, this study takes place in an entirely different context. This is a context where aggregate surveillance of the populace by the state has been ongoing for centuries and where privacy is not a substantive social value. Furthermore, because large-scale state surveillance has assumed an institutionalized place in society, it has become a multi-dimensional phenomenon. Throughout recorded Thai history, surveillance has helped entrench patterns of state domination and social inequality in many areas of people's lives. Meanwhile, it has also become a means through which modern citizenship rights are engendered. Considering the complexity of state surveillance and the novelty of privacy issues in Thai society, it would be a mistake to view the two phenomena strictly as a zero-sum game or as opposing forces, as would be the conventional understanding of the two terms. In the Thai experience, although surveillance and privacy may have implications for each other at broad social levels, the relationship between the two is not necessarily restricted to a negative cause and effect pattern. This is particularly true at the public policy level. A number of factors are at play that make the growth of state surveillance and the emergence of privacy in this social context unique and significant.

As any reader of the prior historical analysis will agree, the Thai state has always been a "surveillance state." On this note, it appears that the definition of a "surveillance state" which is conventionally associated with modernism and modernity is challenged in this work. As demonstrated in chapter two, systematic and large-scale collection and keeping of personal records for social control purposes had been in place in Thai society since 1454, long before the development of the modern state and centralized bureaucratization in Western Europe. In the past six hundred years, the expansion and

institutionalization of state power, which was chiefly accomplished through rigorous surveillance systems, has left Thais with an underdeveloped civil society. Had this not occurred, Thais would have likely obtained a necessary foundation for the development of democratic polity and of privacy as political rights. Although the Thai state's impressive effort at surveillance and social control had met with resistance of various types or foundered as a result of ineffective technologies and patronage system throughout recorded history, it must still have created an unfavorable condition for the development of privacy rights among the people. This is exacerbated, of course, by extensive authoritarian rule, national security problem, as well as Buddhist philosophical environment, which is indifferent to the liberal public-private problematique.

Though there has not been a large-scale survey undertaken to assess public opinion about privacy in contemporary Thailand, it can be somewhat gauged from the focus groups results in chapter seven that different social classes in Thai society think about privacy in ways quite different from one another. While representatives from the upper and middle classes express forms of concern and draw upon frames of reference that are comparable to those in the West, those in the lower classes display an entirely distinct schema when talking about the same issues and tend to see the government's major record-keeping system – the civil registration and national identification system – not as a means of surveillance but rather as an entitlement to citizenship rights. Incidents such as the burning of (or the threats to burn) identity cards and the peaceful return of the cards by peasants to authorities as a form of protest against the government also confirm this particular ideology. The politicizing of the ID card has nothing to do with the privacy element, but is rather the symbolic link with the state and a broad bundle of citizenship rights that the card represents. Evidently, the conventional public-private dichotomy of the western privacy discourse has no relevance to this experience whatsoever.

Based on the evidence here, however, it appears that Giddens' notions of the dialectic of control and the janus-face of surveillance are empirically substantiated, but with an interesting twist. According to Giddens, the struggle over citizenship rights is a major form of dialectic of control in modern nation-states. As an arena of conflict, each of these rights – political, civil, economic and social – is said to be integrally linked to a distinctive type of surveillance that is both necessary to the power of superordinate groups and an axis for the operation of a dialectic of control by subordinate groups.[1] Therefore, surveillance can have

---

[1] See detailed discussion in chapter one, p. 22-26.

both enabling as well as constraining features for parties at opposite ends in a power relation. In the Thai experience, protesting villagers were clearly using the ID card as a lever of struggle but the essence of the protest was not directly to counter the control that the government has maintained over them through this means of surveillance. It was instead to show repugnance against the government for failing to provide what they are supposed to provide to their citizens. By destroying (or threatening to do so) or relinquishing the card, the protesting peasants were making a statement that they were so fed up that they were willing to give up their Thai citizenship. So, even though the "control" element in the surveillance was not contested, the card could still be negotiated for use for political possibilities by subordinate population in this incident.

While the ID card may have become a contested terrain between the state and the peasants in the latter's struggle for social and economic rights, the significance of this event is entirely different from the efforts by the *phrais* to avoid or to manipulate the system of surveillance via tattooing in the traditional past. First, unlike the modern peasants who were tapping into the symbolic (citizenship) dimension of the ID card, the *phrais* were directly resisting the means and modes of state surveillance that have caused hardships in their lives. Secondly, when viewed in terms of the spatial relationship between the state and the people, the case of the *phrais* shows a more levelling arrangement despite the rigidity of the social structure and the unavailability of formal institutions for interest representation and contestation in that time period. Aside from factors such as geography and patronage system that allow them "segmental autonomy," the *phrais* were also unaffected by nationalistic ideology and associated schemes that were at work during the modernizing years. It merits emphasis again that the modern civil registration and national identification systems were given birth as part of the process of nation-building by Chulalongkorn and gained momentum during the nationalistic period of the 1950s and the security crisis of the 1960s and 1970s. The construction of national identity that was based upon three popular institutions – the Thai language, Buddhism, and the royal family – and the appeal to national security not only helped justify the introduction of new surveillance mechanisms but also helped normalize the thinking and behaviors of the people in a way that is conducive to the operation of state surveillance. In this historical context, the general notion of individual rights, let alone the obscure right of privacy, was sidestepped for the "greater" and collective good of the nation.

Ironically, as the Thai polity became more democratized with general elections taking place regularly at all levels of governance, the practices of state surveillance that explicitly contradict democratic norms became even more consolidated. The case in point, of course,

287

is the civil registration system, whose existence has always been rationalized in association with the institution of democratic elections. Although originally designed for administrative and security reasons, the system has gradually grown to become the central information base for the electoral process in the country's parliamentary democracy. As discussed in chapter four, the voters' listing of the Registration Administration Bureau has been increasingly used in the past two decades by dirty politicians and bureaucrats to coerce voters to cast votes in a certain fashion and to keep track of the patterns of vote casting in each constituency. In this light, the pursuit of a participatory democracy that is espoused by local democratic movements is faced with a potentially destructive blow. Without a certain degree of privacy, an individual citizen would not be able to exercise his or her participatory freedom by making an uncoerced political choice. So long as this illicit information practice continues to characterize the local political culture, the exercise of political rights through free elections will be very restricted, if not futile.

In many ways, the operation of state surveillance in modern Thailand contains elements that are reminiscent of Foucault's metaphor of the Panopticon. Although Thai people are not incarcerated in an enclosed institution like the Panopticon, the many aspects and events in their lives are subtly affected by the tools of state surveillance and the system that administers it. At least for the past forty years, most Thais have been disciplined to participate in a bureaucratic mode of surveillance as the requirements for national identity card and household registration card became more regularized not only in state administration but also in other spheres of social life, including politics, workplace, finance, education and consumption. In this scenario, the inscription of power was blended into various forms of rights and gradually learned by individual citizens through social rituals and practices. Weber was right in pointing out how habituation could become a major basis of compliance to surveillance strategies and in turn a reflection of state's legitimacy in administering such measures.

In the context of the late twentieth century, the Thai state's legitimacy in collecting and manipulating personal data of citizens has been augmented by two relating factors – technocratic ideology and the "information society" rhetoric. The notoriety of bureaucratic red tape in local government agencies has made computerization an appealing solution to almost all types of organizational and service-oriented problems since it ensures greater efficiency. As demonstrated in the case studies of contemporary state surveillance in chapter four and five, the bureaucrats' technocratic obsession with efficiency is a major impetus in the development of the PIN project and the criminal records database. A similar ideological

predisposition is also found in the relatively positive attitudes of most participants in the focus groups towards plan to merge government databases, with the exception, of course, of HIV-positive participants. When combined with the euphoric message of the "information society" thesis, this technocratic ideology became infused with optimism and an alluring invitation for people to participate in the new scheme of things.

With advances in database technology that made possible such new techniques as the ATM/ID card project, the "surveillance state" may well be transforming into a "participatory panopticon," since government surveillers are now acting in concert with and sharing information with private sector counterparts, hence creating a more decentered form of surveillance. Moreover, the appeal to convenience of the project also demonstrates its consensual aspect which will likely engender less resistance than earlier forms of surveillance. After all, this new face of surveillance does not inflict physical pain as in the wrist-tattooing days or cause inconvenience from bureaucratic red tape as in the paper age. Given that it makes people's lives easier by facilitating processes and transactions that would have been an impossibility in the past, few card-holding citizens would care that they are being assigned a new identity – that of a consumer – and that their personal information is being shared by different organizations and used for different purposes from which they were collected. In this "participatory panopticon," it will also become more difficult for people to resort to fraud or evasion as avenues for resistance due to the complex crisscrossing network of data collection and supervision of behavior and the growing pressure and need to comply.

As new surveillance developments transpire, we are also witnessing signs of an emerging privacy regime in Thailand in the public policy arena. This regime involves two separate movements – the democratic movement that gave rise to the enactment of the freedom of official information law and the technocratic movement that is propelling a passing of a data protection law. Unfortunately, there are inherent problems with both. The freedom of official information law may have been successful in inciting public consciousness and action regarding their rights to access government information but it has achieved little in defending the information privacy of individual citizens. In fact, the overemphasis on granting the public access to government records may have inadvertently undermined the importance of privacy. The incorporation of data protection statutes in a freedom of information law also illustrates an underlying paradox in information laws, that is, laws restricting access to data on private citizens are usually passed in tandem with freedom of information statutes. But, conceptually privacy protection is inherently in tension with freedom of information. In a couple of the complaint cases that were lodged to the

Office of the Official Information Committee (OOIC), there was already clear evidence that freedom of information overrides privacy protection.

Even among the members of contemporary movements to build a local "civil society," there has been no other effort to influence the new privacy regime, apart from the section on personal data in government files in the freedom of official information law. It seems that the linkage between privacy-protecting processes and the development of a strong "civil society" has not yet been realized in Thai society. Information practices that infringe upon citizens' rights and liberties like the ones documented in the two previous case studies and in the focus group report usually go by unreported and unanalyzed. At this stage, the orientation is more towards gaining access to information held by government agencies which have previously guarded it as administrative secrets. NGOs have demanded that the transparency and accountability of the government bureaucracy to democratic voters be rendered feasible partly through this open access to government information. But this transparency is only one-way since it does not address the principles of state surveillance that are in operation at both aggregate and focused levels of society. It is true that privacy may not reflect a significant local social value and may be indicative of a type of democracy that is felt to be unfit for Thailand – liberal-pluralist democracy. Nevertheless, it is undeniable that certain dimensions of privacy are also implied in participatory democracy which is the goal of the current political reform. The ideal of participatory democracy emphasizes the capacity of citizens to act politically through freedom of choice, which includes, among others, freedom of speech, organization and assembly as well as free elections. The instrumental and political dimensions of privacy are evidently essential to create conditions that are necessary for such participatory freedom. Although the general Thai public may not relate to the types of government information practices as analyzed in this study as surveillance/privacy issues, interested persons will have to, for lack of better terms and theoretical concepts, approach these practices from that vantage point. As the ongoing political reform evolves, it may be advisable for members of the local NGOs or academics to begin to examine seriously the above dimensions of privacy and their significance as an institutional feature of the emerging Thai "civil society." Without such endeavor, their effort to expand this space of uncoerced interaction, not just with regard to people's relations with the state, but even in the culture of their daily lives, is bound to be fraught with problems.

As for the technocratic movement to pass a data protection law, there is an underlying irony in that this movement has nothing at all to do with local experiences of surveillance. Instead, it is a result of the penetration of international policy frameworks and a reflection of

local policy elites' desire to keep up with globalizing technological and economic trends. Like the international regime that gave rise to it, this emerging privacy regime focuses almost entirely on regulating the collection and use of personal information or the data protection component of protecting privacy. It is designed mainly by academics and a handful of technocratic elites with backgrounds in computers, law, and government administration. The content emulates the statutes and regulations of data protection legislations in a selected few countries. There was no representation or participation from interest groups that might be apprehensive about state or corporate surveillance. Clearly, this is by no means a pro-privacy or an anti-surveillance endeavor, but merely a policy effort to cope with globalization and the technical requirements of an increasingly networked world.

Whether the new technocratic movement will result in higher privacy standards and expectations in Thai society is difficult to evaluate at this early stage. To the extent that this new policy action will introduce instruments for data protection, it may at least constitute a symbolic stand against further drift in misuse of personal data by public and private organizations. But because of its orientation towards business information practices and lack of political foundation, it may not be a potent force in mobilizing against government surveillance practices or in galvanizing a privacy which is effective in achieving other social interests. Since data protection is being articulated on the policy agenda in such a top-down fashion, with so little participation from the public, it will likely take some time for the concept to take roots in the local culture and for people even to start making use of the available statutory instruments once they are in place.

Unlike the emergence of privacy regimes in Europe and North America, the Thai experience has had little to do with human rights and civil liberties – the aesthetic and political dimensions of privacy – which usually are an important basis for the politicizing of privacy in the western context. Placing the restriction of personal information on the policy agenda does not reflect an identifiable public concern about privacy as an end in itself, nor an interest in using it as a means to place limits on the power of the state. It also does not really suggest a viable public concern about how information and communication technologies may be used by government or private organizations. Like the fair information practice principles from which they derive, the principles of data protection that dominate the Thai privacy agenda are primarily means to ensure against mistakes and misuses of personal data during data processing rather than to stem the growth of surveillance in any meaningful sense. With the pressure of privacy standards through the EU directive, the instrumental effect of the regime will likely be to facilitate the globalization of international data traffic rather than

291

anything else. In this scenario, questions concerning the moral and ethical basis of surveillance practices seem to get lost amidst all the talk about globalization and the urgency to modernize the country's legal and regulatory infrastructure to cope with these technological-led currents of change.

WHAT IS TO BE DONE?

It is clear that privacy or data protection approaches may not suffice as a solution for an exceptional case of a "surveillance state" like Thailand. Aside from the inherent deficiency of data protection principles, the inadequacy of the privacy agenda in the Thai context may be attributed to such factors as political culture, historical experience, as well as the local prevalence of technocratic ideology and wide acceptance of the information society thesis. Understanding the interplay of these factors is crucial to any effort at designing a social action to counter the momentous force of state surveillance and the growing tide of corporate surveillance.

As I have stated at the outset, this work is a project to apply critical communication theory to a cross-cultural and cross-national analysis of surveillance and privacy and to render an informed critique of related social practices in Thai society. Insofar as generating a critical assessment of the character and consequences of the development of state surveillance and an analysis of the emerging privacy regime is concerned, I feel that I have met my objective.

As to the question of what is to be done to remedy the situation I have so painstakingly analyzed, I feel, with all the personal constraints and disillusionment, that I can only speak strictly from an academic armchair. What I can offer is a humble conceptual path of resistance and an alternative against the growing networks of surveillance in Thai society, that is, by increasing the "knowledgeability" of the public. It is a task for critical scholarship, regardless of disciplines, to examine both the quantitative and qualitative costs and implications of surveillance systems maintained by state bureaucracies and corporate organizations. It is important that these scholars keep abreast of new developments, both technological and bureaucratic. Experience from most local and foreign diffusions of surveillance technologies show that once an infrastructure is established, it is impossible to prevent either legal incremental uses or illegal abuses of the system. So it is important to address potential problems from the start before the technological momentum of surveillance

292

system increases. Through an ongoing study of surveillance system and related institutional factors, it will be possible to show how certain modes of surveillance can become precursors to a number of dangerous practices. Once such kind of study is disseminated to the public through the appropriate channels; for instance, mass media and NGOs, it may be possible to raise questions and sense of social responsibility in the minds of regulators, system designers, data users and data subjects. This dissemination of knowledge could also have the potential of mobilizing social movements by individuals and groups who are directly affected by state and corporate surveillance practices. In this endeavor, critical scholars may find it useful to focus on certain groups who will be strategic to future mobilization for social change in the areas of surveillance and privacy, for instance, civil liberties groups, consumer associations, the media, NGOs focusing on information technology and on democratic development, and HIV-positive persons.

The future is uncertain and I dare not make predictions how the surveillance/privacy scenario in Thailand will unfold. Whether there is a potential for an anti-surveillance movement, which may not be limited to a politics of privacy, in this unique social context will depend on how much critical scholarship can advance the issue and the process of public learning. This is indeed an important role and I am proud to have played my small part.

APPENDIX 1

Case Study as Methodology for Analysis
of State Surveillance Systems

In seeking information about the development of computerization at the Registration Administration Bureau (in chapter 4) and the criminal records division (chapter 5) and its significance for social control, I decide to use "case study" as a research strategy. Case study is "an empirical enquiry that investigates a contemporary phenomenon within its real-life contextl when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidences are used."[1] The two case studies were carried out mainly through arranged site visits to both organizations. I estimated that about eight to ten on-site visits would be sufficient. To gain field experience, I conducted an experimental study in January 1996, visiting the Office of Central Registration in Bangkok. Based on this visit, in which I was assigned to speak with an official who oversees the development of the PIN project, I drew up a checklist of topics to be investigated at this site and others in the future visits. This served as a format for interviews with selected members of the staff later. The headings from this checklist indicate the kinds of information I sought at the site:

1) the organization visited: history, function, style, environment;

2) data held about individuals and groups, in manual and automated forms;

3) description of the present record-keeping system;

4) comparison of the operation of computerized system with prior manual systems;

5) the decision to computerize: why and how made, and by whom;

6) transitions from initial computerization to the present;

7) management perceptions of information needs and data usage;

8) data confidentiality and data access: rules, practices, cases, and issues;

9) management attitudes towards a balance between information needs and personal privacy;

10) impacts on subjects of data collection;

11) future plans for computerization of files containing sensitive personal information, and establishment of inter-organization data-sharing networks through advanced computer systems.[2]

---

[1] R.K. Yin, *Case Study Research: Design and Methods* (Newbury Park: Sage, 1989), 23.
[2] Some of the topics in this checklist are borrowed from a checklist drawn up by Alan Westin and Michael A. Baker in *Databanks in a Free Society* (NY:Quadrangle /New York Times Book Co, 1972), 23-24.

From April 1996 onwards, I began to conduct the actual site visits to both organizations. The entire period of site visits lasted for a little more than four months as I visited both sites concurrently. The site visits were arranged by a letter generally describing my research project -- to study the management of databases of personal information at the organization -- and expressing the hope that the organization would be willing to co-operate (see appendix 2). As it is customary for government organizations to be cooperative with academic institutions, I asked my senior supervisor at Simon Fraser University and the dean at the Faculty of Communication Arts, Chulalongkorn University to each write a letter to request cooperation and to certify my status as a graduate student and a university faculty member respectively. Owing largely to these letters, both organizations were willing to cooperate.

At most sites, the early visits proved to be very important in providing background about the organization and its record-keeping systems. Since published materials about their computerization projects were scarce except as internal, and thereby, confidential documents, I had to rely mainly on oral accounts from middle-level staff who were usually assigned to brief me about the projects. As a result, during the first few visits to the first site -- the Registration Administration Bureau, most of the time was spent in interviewing these designated staff -- usually managers of the data-processing unit, and heads of principal "user departments" in the organization -- using the checklist above as a guideline. At the criminal records division, however, the top executive -- the director of the division -- was the first to grant me an interview. This was in order to establish a courtesy of approval by the top authority in the division and to suggest to the other staff that proper cooperation be rendered.[3] Wherever possible, however, I would secure additional written materials from the organization's files to document the accounts of practice and policy given orally.

After having obtained sufficient background data about the computerization projects, I requested permission to sit in and observe the actual data-handling practices of professional and clerical staffs in data entry and processing. Whenever possible, I also conducted interviews with these staff, trying to be as unobtrusive and non-disruptive of their work as possible. Important anecdotal evidence was collected through this part of the site-visits. In the meantime, I also arranged for more interviews with higher-ranking executives of the organizations whose timeline was less flexible. After four months, I also did some more

---

[3] It must be noted, with appreciation, that Maj. Gen. Chatri Sunthornsorn, director of the criminal records division, was exceptionally kind to me. Although we had had no prior connection with each other, he facilitated my convenient access to personnel and data-areas during the site visits.

follow-up visits and had extensive telephone conversations to complete any remaining inquiries or necessary updating of my files.

In addition to materials drawn directly from each organization, I also searched national newspapers and other media sources for information or commentary on the organization and their computerization projects. While there were a few articles published in the press on these issues, they were primarily descriptive and lacked analytical insights. Most seemed to derive from press releases that echoed directly the message disseminated by the organizations visited.

One of the main problems encountered during the site visits to the Registration Administration Bureau was getting an appointment with key officials who were in a position to affect decision-making at the organization. These officials were mostly unavailable -- either too preoccupied with their work schedule or away on official trips. There were a few times when I was stood up for an appointment because the official "had an urgent task to attend to." To get a thirty-minute interview with one of the senior officials who has played a leading role in the development of the PIN project, I had to wait for more than five months. Nevertheless, the middle-level officials there were very cooperative and provided me with the needed information and facilitation of access.

As for the criminal records division, there was less problem in getting appointments and interview with senior personnel. However, when asked about the use of the AFIS for employment screening in the private sector, some of the middle-level staff seemed defensive and reluctant in volunteering information. In many ways, the heavy reliance on oral accounts is a major limitation of my method. It is particularly difficult to triangulate the evidence from the oral accounts with other sources since the topic at hand is not well-known or well-publicized. I generally coped with this limitation by asking as many people on the same topic as possible. When there is an obvious contradiction in the stories, then it is presumed to be less reliable, and vice versa.

APPENDIX 2

Example of Letter Seeking Cooperation

from Record-Keeping Organizations

4 May 1996

To (name of director/or authority in charge of the organization)
re: seeking your organization's cooperation for the research of Ms. Pirongrong Ramasoota

My name is Pirongrong Ramasoota. I am a Ph.D. candidate in Communication at Simon Fraser University in Canada, as well as a full-time (currently on-leave) lecturer at the Faculty of Communication Arts, Chulalongkorn University. I am presently doing research in Thailand for my doctoral dissertation on the topic of "The Management of Government Databases of Personal Information in Thailand." I think this is a very important subject for the economic and social development of the country, and hope you will agree with me.

The research I am undertaking requires that I examine data-handling practices at public record-keeping organizations that have major computerization programs. Since your organization fits this criteria, I would like to request for site-visits to your organization at the convenient time so that observation of the practices and interviews with the responsible staff can be carried out.

I will be very grateful for the assistance you can offer to me in the course of conducting this research. I will be contacting you again by telephone to follow up on the letter and to make further arrangements.

Sincerely yours,

(Ms. Pirongrong Ramasoota)

APPENDIX 3

Focus Group as Methodology

for Examining Perception of Information Privacy

From a "communication perspective," it is assumed here that people develop their attitudes and perceptions relating to concepts in part by interaction and communication with other people. In this light, the various types of survey research -- mail, telephone and face-to-face -- are quite deficient. This is because research subjects in surveys usually form opinions in isolation and the researchers assume the subjects really do know how they feel about the topic being asked. As far as privacy is concerned, survey research may be an appropriate tool in the West where privacy is a deeply rooted concept and widely understood. Even so, in several cross-sectional surveys on privacy, in particular computers and privacy, results confirmed that attitudes and opinions about privacy still vary from context to context and that it is not possible to predict from one context to another.[1] To relate this finding to the Thai setting, it is reasonable to assume that people in different social classes are likely to utilize quite different cognitive frames when they think about the presence or absence of privacy. While the more modernized upper socio-economic strata may see privacy in a manner similar to their western counterparts, many among the poorer classes may not have a genuine opinion about privacy at all. In order to understand the distinct schema that people utilize when thinking about privacy, survey research can be too restrictive as the pre-designed questions would undoubtedly reflect the biases and predisposition of the researcher.

On the other hand, focus groups as defined and described below, are more suitable for this research for several reasons.

> A focus group is a carefully planned discussion designed to obtain perceptions on a defined area of interest in a permissive, non-threatening environment. It is conducted with approximately 7 to 10 people by a skilled interviewer. The discussion is comfortable and often enjoyable for participants as they share their ideas and perceptions. Group members

---

[1] See for example Louis Harris & Associates, Inc. and Alan F. Westin, *The Dimensions of Privacy: a National Opinion Research Survey of Attitudes Toward Privacy* (New York: Garland Publishing, 1981); James Katz and Annette Tassone, "Public Opinion Trends: Privacy and Information Technology," *Public Opinion Quarterly* 4 (1990): 125-143; and Oscar Gandy, *The Panoptic Sort.*

influence each other by responding to ideas and comments in the discussion.[2]

First, and foremost, focus groups are less confining than survey research. which tends to be superficial and rigid in framing the subject of investigation. Rather than relying on standardized questionnaires, focus group results are solicited through open-ended questions where the respondents are able to choose the manner in which they respond and develop their thoughts based on the observations of others collaborating in the group discussion. Focus groups thus present a natural environment where participants are influencing and influenced by others — just as they do in real life. The researcher can then go beyond addressing the participants' perceptions and attitudes to probe into their actual behaviors and experiences.

Secondly, with the limited timeframe and financial resources that were available for this research, focus groups were all the more the reasonable choice as they are relatively low in cost and provide quite speedy results. If survey research had been selected as a method for this inquiry, it would have involved a much lengthier process and a greater expense. To begin with, it would take a considerable amount of time and effort to secure a minimally adequate sample size that can ensure the representativeness of the population of Thai individuals qualified to speak on "privacy." The parent population in this case is not only extremely large in size but also highly heterogenous. Suppose the population were to be limited to Bangkok residents alone, the only possible way to determine samples from this population would be to use telephone directories of the Bangkok Metropolitan Area (BMA) as a sampling frame.[3] This would, however, distort the representativeness of the sample significantly since only fifteen percent of registered Bangkok residents own a telephone. The socio-economic disparity among different social groups, which is characteristic of the Bangkok population, would be absent in the sample. Therefore, larger samples derived from a different sampling frame would be required to reflect the characteristics of the larger and more heterogeneous social groups. This, as mentioned, would be impossible to achieve given the time and financial constraints of this study.

Last but not least, the intent of this research is not to arrive at some quantitative data that would, for instance, capture the participants' level of agreement or disagreement with

---

[2]Richard A. Krueger, *Focus Groups: a Practical Guide for Applied Research* (Thousand Oaks, Calif: Sage, 1994), 6.
[3]The registered population of Bangkok is approximately five million, not including possibly another few million migrant laborers who also reside in the city and the metropolitan area.

certain pre-designed statements about privacy. Instead, it aims at exploring and probing into the unchartered terrain of "privacy" as experienced by selected subsets of Thai individuals from different socio-economic backgrounds. Focus groups appropriately produce the qualitative data that is needed. The information generated from the various focus group sessions not only provide insights into the participants' attitudes, perceptions, opinions, and experiences about privacy but also expose, to some degree, their concepts of self and control over their own environments. These latter two points are particularly important in shedding light on the changing spatial relationship between the state and its citizens which forms the larger question of this study.

Despite their many advantages, focus groups also have their limitations. First, as aforementioned, the obvious inability to secure representative samples would make it impossible to use focus group data to generalize to the population as a whole. While the views of participants in the five focus groups carried out in this study may be illustrative of what certain social groups think about privacy, these views are by no means an exhaustive representation of Thai society in general. Secondly, focus groups also leave the researcher less control in the group interview sessions. As I have personally experienced from moderating certain sessions, the group discussion often deviated from the question raised to issues that most reflected the priority concerns of particular participants who tended to dominate the discussion. Even with a considerable amount of preparation, it became clear later on that the actual conducting of a group interview required a lot of skills and adeptness in handling unexpected circumstances. Furthermore, groups were very difficult to assemble. It was impossible to recruit a perfect stranger in Bangkok to participate in the session which would take up at least two hours of his or her time.[4] Finally, I was left with the option to recruit participants through the means of peer-referral and personal connection. While this recruiting approach enabled me to achieve a reasonable homogeneity in certain attributes of the group participants, it was not always possible to maintain a sense of unfamiliarity among them. In a couple of sessions where people in lower socio-economic groups were recruited, one group was dominated by a few restaurant employees who work closely together, while the other was populated by a group of construction workers who worked at the same construction site. In the last session where HIV positive patients and health professionals were present, the participants had all known and worked with each other before.

---

[4]This is particularly difficult in Bangkok where the chronic traffic congestion would discourage people from even considering the invitation to join the group session.

APPENDIX 4

Introductory Remark to the Focus Group Discussion

Good morning and welcome to our session today. Thank you for taking the time to join our discussion on information privacy. My name is Pirongrong Ramasoota and I am presently a Ph.D. candidate at Simon Fraser University, Canada. I am also a faculty member in the department of Journalism here. Assisting me is Ms. Nana Kom-amnajsakul who is a master's student in Journalism. We are attempting to gain information about the public perception and awareness of information privacy particularly computerized information which are held in databases of public and private organizations. Today we have invited people who we feel may be involved with the issue of information privacy in one way of another to share their ideas on the issue.

We will be discussing information privacy in computerized data maintained by private organizations such as banks, credit card issuers, direct mail and marketing companies and the like. There are no right or wrong answers but rather differing points of view. Please feel free to share your point of view even if it differs from what others have said.

Before we begin, let me remind you of some ground rules. This is strictly a research project and your comments will not be reproduced for other reasons. Please speak up and only one person should talk at a time. We are tape-recording the session because we don't want to miss any of your comments. If several are talking at the same time, the tape will get garbled and we will miss your comments. Please be assured of complete anonymity as your names will not be attached to your comments in our later reports nor will the tape be released for any other purpose but data analysis. Please keep in mind that we are just as interested in negative comments as positive comments, and at times the negative comments are the most helpful.

Our session will last about an hour and a half, and we will not be taking a formal break. The rest rooms are one flight of stairs up, and you will see the spiral stairs as soon as you walk out of this conference room. Refreshments are over near the wall. Feel free to leave the table for either of these or if you wish to stretch, but please do so quietly.

Well, let's begin. We've placed name tents on the table in front of you to help remember each other's names. Let's find out some more about each other by going around

301

the room one at a time. Please tell us first how you would define "privacy" and whether any of you has ever personally been the victim of what you felt was an improper invasion of privacy.

REFERENCES

Adorno, Theodor. 1969. Scientific Experiences of a European Scholar in America. In The Intellectual Migration: Europe and America 1930-1960, ed. D. Fleming and B. Bailyn. Cambridge, Mass: Harvard University Press.

Aeusrivongse, Nithi. 1995. *ratthathammanun chabab watthanatham* (Constitution: the Cultural Tradition). In *chat thai muang thai baeb rian lae anusawaree* (Thai Nation, Thailand, Textbooks and Monuments), ed. Nithi Aeusrivongse. Bangkok: Matichon Press.

Aglietta, Michel. 1979. A Theory of Capitalist Regulation. London: New Left Books.

Anderson, Benedict R. O'G and Ruchira Mendiones. 1985. In the Mirror: Literature and Politics in Siam in the American Era. Bangkok: Duangkamol.

Anderson, Perry. 1984. Lineages of the Absolutist State. London: Verso.

Apornsuwan, Thanes. 1996. *sitthi khon thai nai ratthai* (The Rights of Thais in the Thai State). In *Jintanakam su pi songphan navakam cheung krabuanthat dam thaisuksa* (New Paradigms in Thai Studies in the Year 2000), ed. Chaiwat Satha-Anand. Bangkok: Thailand Research Fund.

Banuri, Tariq. 1990. Development and the Politics of Knowledge: a Critical Interpretation of the Social Role of Modernization. In Dominating Knowledge: Development, Culture, and Resistance, ed. Frederique Apffel Marglin and Stephen Marglin. Oxford: Clarendon.

Battye, Noel Alfred. 1974. The Military, Government, and Society in Siam, 1868-1910: Politics and Military Reform during the Reign of King Chulalongkorn. Ph.D. diss., Cornell University.

Bell, Daniel. 1973. The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York: Basic Books.

Bell, Daniel. 1979. The Social Framework of the Information Society. In The Computer Age: a Twenty-Year View, ed. Michael L. Dertouzos and Joel Moses. Cambridge, MA: MIT Press.

Beniger, James A. 1992. The Control Revolution: Technological and Economic Origins of the Information Society. Cambridge, Mass: Harvard University Press.

Bennett, Colin J. 1991a. Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s. Science, Technology & Human Values 16 (1): 51-69.

Bennett, Colin J. 1991b. Review Article: What is Policy Convergence and What Causes It? British Journal of Political Science 21: 215-233.

Bennett, Colin J. 1992. Regulating Privacy. Ithaca, NY: Cornell University Press.

Bennett, Colin J. 1998. Convergence Revisited: Toward a Global Policy for the Protection of Personal Data. In Technology and Privacy: the New Landscape, ed. Phil E. Agre and Marc Rotenberg. Cambridge, Mass: MIT Press.

Bloustein, Edward J. 1984. Privacy as an Aspect of Human Dignity -- an Answer to Dean Prosser. In Philosophical Dimensions of Privacy, ed. Ferdinand David Schoeman. Cambridge: Cambridge University Press.

Boonnoon, Jirapan. 1998. NECTEC plans public hearings on smart card standard. The Nation, 10 November 1998, F 3.

Boonnoon, Jirapan. 1999. Slight growth predicted for IT market in Thailand this year. The Nation, 2 March 1999, F 2.

Boxer, C. R., ed. 1971. A True Description of the Mighty Kingdom of Japan and Siam. Amsterdam: N. Israel.

Registration Administration Bureau. 1996a. khormun samnak boriharn karn thabian krom karn pok krong khwampenma khrongsarng annart nathee khwamrabphidchob lae khrongkarn samkan (Information on the Registration Administration Bureau, Department of Local Administration: Origin, Structure, Authority, Responsibility and Important Projects). Bangkok: Department of Local Administration.

Registration Administration Bureau. 1996b. khu meu karn patibat ngan thabian rasadorn (Manual for the Operation of Civil Registration). Bangkok: Department of Local Administration.

Science Council of Canada. 1982. Planning Now for an Information Society: Tomorrow is Too Late. Ottawa: Science Council of Canada.

Carnoy, Martin, Manuel Castells, Stephen S. Cohen, and Fernando Henrique Cardoso. 1993. The New Global Economy in the Information Age: Reflections on Our Changing World. University Park, PA: Pennsylvania State University Press.

Castells, Manuel. 1993. The Informational Economy and the New International Division of Labor. In The New Global Economy in the Information Age, ed. Martin Carnoy, Manuel Castells, Stephen S. Cohen, and Fernando Henrique Cardoso. University Park, PA: Pennsylvania State University Press.

Chalermchuang, Tiang. 1965. karn khuap khum ponla muang kab khwam mankhong khong chat (Citizen Control and National Security). Special degree thesis, National Defence College.

Chamarik, Sanek. 1995. karn muang thai lae phattanakoarn ratthathammanun (Thai Politics and the Development of the Constitution). Bangkok: Thai Studies Institute, Thammasart University.

Christensen, Scott. R. 1993. Democracy without Equity?: Institutions and Political Consequences of Bangkok-based Development. In Who Gets What and How?: Challenges for the Future, TDRI Year-End Conference, ed. Scott R. Christensen and Ammar Siamwalla. Chon Buri, Thailand: Thailand Development Research Institute (TDRI).

Christensen, Scott R. and Ammar Siamwalla. 1994. Muddling toward a Miracle: Thailand and East Asian Growth. TDRI Quarterly Review 12 (April): 14-22.

Chuvichian, Somnuk. 1967. Karn thabian rasadorn nai khwam rabpidchob khong krasuang mahatthai (Civil Registration under the Responsibility of the Ministry of Interior), The National Institute for Development Administration (NIDA).

Clarke, Roger. 1994. The Digital Persona and its Application to Data Surveillance. The Information Society 13 (2): 77-92.

Cohen, Jean L. and Andrew Arato. 1992. Civil Society and Political Theory. Cambridge, Mass: MIT Press.

Privacy Protection Study Commission. 1977b. Technology and Privacy: the Report of the Privacy Protection Study Commission. Washington DC: US Government Printing Office.

Office of Official Information Committee. 1998. *rai ngam prajam pi samnam ngan khana kammakam khor mun khao sam khong ratchakam* (Annual Report of the Committee on Government Information (1997-1998)). Bangkok: Ministry of PM's Office.

Department of Corrections. 1996. History of Penal System in Thailand. Bangkok: Department of Corrections.

Crawford, John. 1967. Journal of an Embassy to the Courts of Siam and Cochin China. Kuala Lumpur: Oxford University Press.

Dandeker, Christopher. 1990. Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day. New York: St. Martins' Press.

Davies, Simon G. 1996. Surveying Surveillance: an Approach to Measuring the Extent of Surveillance. In Computers, Surveillance and Privacy, ed. David Lyon and Elia Zureik. Minneapolis: University of Minnesota Press.

Davies, Simon G. 1998. Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. In Technology and Privacy: the New Landscape, ed. Phil E. Agre and Marc Rotenberg. Cambridge, Mass: MIT Press.

de la Loubère, Simon. 1969. The Kingdom of Siam. Translated by A.P. Geun R.S.S. Kuala Lumpur: Oxford University Press.

Department of Local Administration, Ministry of Interior. 1983. *khu meu patibat ngan tambrongkam chat tham lekprachamtua prachachon pi 2526* (A Manual for the Operation of the Project to Issue Identification Numbers to Citizens, 2526 B.E.). Bangkok: Agriculture Cooperatives Union of Thailand Press.

Dheeravegin, Likit, ed. 1989. Thai Politics: Selected Aspects. Bangkok: Tri-Sciences Publishing House.

Dheeravegin, Likit. 1992. Semi-Democracy: the Evolution of the Thai Political System. New York: Times Academic Press.

Criminal Records Division. 1991. *Kam suksa khwam pen paidai khong krongkam pramuan phon lai new meu doi attanomat* (Feasibility Study for the Automatic Fingerprints Identification System Project). Bangkok: Department of Police.

Dizard, W.P. 1982. The Coming Information Age. New York: Longman.

Dreyfus, Hubert L. and Paul Rabinow. 1982. Michel Foucault: Beyond Structuralism and Hermeneutics. Chicago: University of Chicago Press.

Flaherty, David. 1989. Protecting Privacy in Surveillance Societies: the Federal Republic of Germany, Sweden, France, and the United States. Chapel Hill: University of North Carolina Press.

Flaherty, David H. 1986. Government Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies. Science, Technology & Human Values 11 (1): 7-18.

Flaherty, David H. 1998. Controlling Surveillance: Can Privacy Be Made More Effective? In Technology and Privacy: the New Landscape, ed. Phil E. Agre and Marc Rotenberg. Cambridge: MIT Press.

Fortner, Robert S. 1986. Physics and Metaphysics in an Information Age. Communication 9: 151-172.

Foucault, Michel. 1977. Discipline and Punish: the Birth of the Prison. New York: Vintage Books.

Foucault, Michel. 1980. Power/Knowledge: Selected Interview and other Writings. New York: Pantheon Books.

Friedrich, Carl J. 1971. Secrecy versus Privacy: the Democratic Dilemma. In Privacy, Nomose Series 13 Yearbook of the American Society for Political and Legal Philosophy, ed. J. Roland Pennock and John W. Chapman. New York: Atherton Press.

Gandy, Oscar. 1993. The Panoptic Sort: a Political Economy of Personal Information. Boulder: Westview Press.

Giddens, Anthony. 1979. Central Problems in Social Theory: Action, Structure, and Contradiction in Social Analysis. Berkeley: University of California Press.

Giddens, Anthony. 1981. A Contemporary Critique of Historical Materialism: Vol. I Power, Property and the State. Berkeley: University of California Press.

Giddens, Anthony. 1982. Profiles and Critiques in Social Theory. London: Macmillan.

Giddens, Anthony. 1987. The Nation-State and Violence: Volume Two of a Contemporary Critique of Historical Materialism. Berkeley: University of California Press.

Giddens, Anthony. 1990. The Consequences of Modernity. Cambridge: Polity Press.

Gohlert, Ernst W. 1991. Power and Culture: the Struggle against Poverty in Thailand. Bangkok: White Lotus.

Gordon, Diana. 1987. The Electronic Panopticon: a Case Study of the Development of the National Criminal Records System. Politics and Society 15: 483-511.

Graham, Peter. 1993. The Australian Card: a Burden rather than a Relief?. The Australian Quarterly 58 (1): 4-14.

Hanna, Nagy, Sandy Boyson, and Shakuntala Gunaratne. 1996. The East Asian Miracle and Information Technology: Strategic Management of Technological Learning. Washington DC.: World Bank.

Hardt, Hanno. 1992. Critical Communication Studies: Communication, History, and Theory in America. New York: Routledge.

Harvey, David. 1989. The Condition of Postmodernity: an Inquiry into the Origins of Cultural Change. Oxford: Blackwell.

Hayeesalah, Phochana and Thaneeya Peerapong. 1996. Computerized ID Cards: Critics Fret Over Loss of Privacy and Human Rights Issues. The Nation, 13 February 1996, C 2.

Held, David. 1980. Introduction to Critical Theory: Horkheimer to Habermas. Berkeley: University of California Press.

Held, David. 1989. Political Theory and the State. Stanford: Stanford University Press.

Hewison, Kevin. 1989. Bankers and Bureaucrats: Capital and the Role of the State in Thailand. Yale University: Center for Southeast Asian Studies.

Hiramatsu, Tsuyoshi. 1993. Protecting Telecommunications Privacy in Japan. Communications of the ACM 36 (8 (August)): 74-77.

Hon, Wong Seng. 1992. Exploiting Information Technology: A Case Study of Singapore. World Development 20 (12): 1817-1818.

Hong, Lysa. 1981. The Evolution of the Thai Economy in the Early Bangkok Period and its Historiography. Ph.D. dissertation, University of Sydney.

Iamtham, Pompirom. 1987. The Student-led Democratic Movement after the 14 October 1973 Incident and its Relations with the Communist Party of Thailand. Asian Review 1: pp. 9-24.

Ingram, J.C. 1955. Economic Change in Thailand since 1850. Stanford: Stanford University Press.

Innis, Harold. 1951. The Bias of Communication. Toronto: University of Toronto Press.

Ministry of Interior. 1995a. *khrongkam jattham rabob kam hai borikam prachachon thang darn kam thabian lae bat duay computer phram kam jad tham rabob khormun khaosam pheu kam boriham ngam* (Summary Report of the Project for the New Registration System to Service the Public by Using Computer and the Project to Establish a Management Information System for Administrative Purposes). Bangkok: Ministry of Interior.

Ministry of Interior. 1995b. (Summary Report of the Project for the New Registration System to Service the Public by Using Computer and the Project to Establish a Management Information System for Administrative Purposes).

Kaiyuravongse, Sayamol. 1993. *sitthi prachachon nai kam rab ru khor mun khao sam khong ratchakam* (People's Freedom of Access to Government Information). Bangkok: Association of Rights and Freedom of the People.

Kanwanich, Supradit. 1996. Vote-buying in all Bangkok constituencies. The Bangkok Post, 24 November 1996, 5.

Katz, James E. 1987. Telecommunications and Computers: Whiter Privacy Policy? Social Science and Public Policy 25 (1 (November/December)): 81-86.

Keane, John. 1988. Remembering the Dead: Civil Society and the State from Hobbes to Marx and Beyond. In Democracy and Civil Society: on the Predicaments of European Socialism, the Prospects for Democracy and the Problem of Controlling Social and Political Power, ed. John Keane. London: Verso.

Kiatsunthorn, Kittiphan. 1995. *mattra kam thang aya nai kam khum khrong kor mun suan bukkhon* (Criminal Measures for the Protection of Personal Data). Master's thesis, Chulalongkorn University.

Kiattananan, Paisal, Pichet Durongkaveroj, Thaweesak Koanantakool, and Adshiriya Agsom-intara. 1996. National Information Infrastructure in Thailand. Seoul, South Korea: A paper presented at the International Forum for APII Testbed.

Kilger, Max. 1994. The Digital Individual. The Information Society 10 (March 1994): 93-99.

Koananthakool, Thaweesak. 1998. The Roles of the National Electronics and Computer Technology Center and the National Information Technology Secretariat on Electronic Commerce Development in Thailand. Bangkok: Ministry of Science, Technology, and Environment.

Koizumi, Junko. 1992. The Communication of *Suai* from Northeast Siam in the Middle of the Nineteenth Century. Journal of Southeast Asian Studies 13 (2): 282-294.

Kraemer, Kenneth L. and John Leslie King. 1977. Computers and Local Government, vo. 1, a Manager's Guide. New York: Praeger Publishers.

Laothamatas, Anek. 1992. Business Associations and the New Political Economy of Thailand: from Bureaucratic Polity to Liberal Corporatism. Oxford: Westview Press.

Laudon, Kenneth C. 1986. The Dossier Society: Value Choices in the Design of National Information Systems. New York: Columbia University Press.

Lyon, David. 1994. The Electronic Eye. Minneapolis: University of Minnesota Press.

Lyon, David and Elia Zureik, eds. 1996. Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

Macpherson, C.B. 1962. The Theory of Possessive Individualism: Hobbes to Locke. Oxford: Clarendon Press.

Macpherson, C.B. 1973. Democratic Theory: Essays in Retrieval. Oxford: Clarendon Press.

Maleesriprasert, Cheun-Arie. 1996. *karn khum khrong sitthi suan tua kab karn seu sarn sonted* (The Protection of Right to Privacy and the Communication of Information). Master's thesis, Chulalongkorn University.

Marshall, T. H. 1973. Class, Citizenship and Social Development. Westport, Conn: Greenwood Press.

Martin, James. 1978. The Wired Society. New Jersey: Prentice Hall.

Masuda, Yoneji. 1981. The Information Society as Post-Industrial Society. Washington DC.: World Future Society.

Masuda, Yoneji. 1982. The Global Information Society. In Information Technology: Impact on the Way of Life, ed. Liam Bannon, Ursula Barry, and Olay Holst. Dublin: Tycooly International.

Methakhunavudhi, Pateep. 1998. *naew thang nai karn ork kotmai khum khrong khor mun lae sarn son thet suan bukkhon nai prathed thai* (A Guideline for Data Protection Legislation in Thailand). Computes and Society 30 (September): 28-30.

Methakhunavudhi, Pateep and Apirat Petsiri. 1996. *naew thang nai karn ork kotmai khum khrong khor mun lae sarn song thed suan bukkhon nai prathet thaii* (A Guideline for Data Protection and Information Privacy Legislation in Thailand). Bangkok: National Research Council.

Miller, Arthur. 1971. The Assault on Privacy: Computers, Databanks, and Dossiers. Ann Arbor: University of Michigan Press.

Miller, Arthur. 1972. Computers, Data Banks, and Individual Privacy: an Overview. Columbia Human Rights Law Review 4 (1): 8-15.

Moore, Barrington. 1984. Privacy: Studies in Social and Cultural History. Armonk, NY: M.E. Sharpe.

Murphy, Robert F. 1984. Social Distance and the Veil. In Philosophical Dimensions of Privacy: an Anthology, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

Muscat, Robert J. 1994. The Fifth Tiger: a Study of Thai Development Policy. Helsinki: United Nations University Press.

Myrdal, Gunnar. 1968. The Beam in Our Eyes. In Asian Drama: an Inquiry into the Wealth of Nations, ed. Gunnar Myrdal. Harmondworth: Penguin Books.

Nakorn, Thienchai Na. 1992. *rang kot mai sitthi nai karn rab ru khor mun khao sarn khong ratchakarn* (Proposal for the Freedom of Official Information Act and Draft of the Act). Bangkok: Institute of Policy Studies and the Association of Social Sciences of Thailand.

Nartsupha, Chatthaip and Sompop Manarangsarn. 1984. *prawatsart settakit thai chontheung pho sor 2484* (The Economic History of Thailand Until 2484 B.E.). Bangkok: Thammasart University Press.

Nartsupha, Chatthip and Suthy Prasartsert. 1981. The Political Economy of Siam (1851-1910). Bangkok: The Social Science Association of Thailand.

Neher, Clark D. 1976. Modern Thai Politics: from Village to Nation. Cambridge: Schenkman.

Nora, SImon and Alain Minc. 1981. The Computerization of Society. Cambridge: MIT Press.

Oettinger, Anthony G. 1980. Information Resources: Knowledge and Power in the 21st Century. Science 209: 191-198.

Panananon, Chatchai. 1988. *Phrai,* Neither Free nor Bonded. Asian Review 2: 1-23.

Panich, Vicharn. 1997. Science and Technology in Thailand's Health Sector. In Science and Technology in Thailand: Lessons from a Developing Economy, ed. Yongyuth Yutthavong and Angela M. Wojcik. Bangkok: NSTDA/UNESCO.

Phongphaichit, Pasuk and Chris Baker. 1995. Thailand, Economy and Politics. Oxford: Oxford University Press.

Pongprasert, Suchalee. 1998. Multi-function Chip ID Cards in Five Years. The Nation, 20 April 1999, F 11.

Pongprasert, Suchalee. 1999. Alternative proposed to implement GiNET project. The Nation, 20 April 1999, F 4.

Pool, Ithiel de Sola. 1983. Technologies of Freedom. Cambridge: Harvard University Press.

Pool, Ithiel de Sola, Philip Stone, and Alexander Szalai. 1971. Communications, Computer, and Automation for Development. New York: United Nations.

Poonsawat, Chodok Veeratham. 1983. *khrongkarn chattham lek prachamtua prachachon kab khwam mankhong haeng chat* (The Project to Issue National Identification Numbers: National Security and the Right of Citizens). Special degree thesis, National College of Defense.

Porat, Marc Uri. 1978. Global Implications of the Information Society. Journal of Communication 28 (1): 70-80.

Pompong, Satchunij. 1995. Easy access to government information is vital in a democratic state. The Nation, 17 September 1995, B 3.

Poster, Mark. 1990. The Mode of Information: Poststructuralism and Social Context. Cambridge: Polity Press.

Poster, Mark. 1994. The Mode of Information and Postmodernity. In Communication Theory Today, ed. David Crowley and David Mitchell. Stanford: Stanford University Press.

Prasertkul, Seksan. 1989. The Transformation of the Thai State and Economic Change (1855-1945). Ph.D. dissertation, Cornell University.

Raab, Charles D. 1997. Privacy, Democracy and Information. In The Governance of Cyberspace: Politics, Technology, and Global Restructuring, ed. Brian D. Loader. London: Routledge.

Rabibhadana, Akin. 1976. The Organization of Thai society in the Early Bangkok Period (1782-1873). In Modern Thai Politics: from Village to Nation, ed. Clark D. Neher. Cambridge: Schenkman.

Rachanunphap, Prince Damrong. 1927. *Laksana Kam Pokkrong prathet siam tae boran (Ancient Administration of Siam)*. Bangkok.

Regan, Priscilla. 1993. The Globalization of Privacy: Implications of Recent Changes in Europe. The American Journal of Economics and Sociology 52 (3 (July)): 257-274.

Regan, Priscilla. 1995. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill: University of North Carolina Press.

Riggs, Frederick. 1966. Thailand: the Modernization of a Bureaucratic Polity. Honolulu: East-West Center.

Robins, Kevin and Frank Webster. 1988. Cybernetic Capitalism: Information Technology, Everyday Life. In The Political Economy of Information, ed. Vincent Mosco and Janet Wasko. Madison: University of Wisconsin Press.

Rotenberg, Marc. 1993. Communications Privacy: Implications for Network Design. Communications of the ACM 36 (8): 61-68.

Rule, James B. 1973. Private Lives and Public Surveillance. London: Allen Lane.

Rule, James B. 1980. The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York: Elsevier.

Sakkriengkrai, Sirilak. 1984. The Economic System in the Ayutthaya Period. In The Economic History of Thailand Until 2484 B.E., ed. Chatthip Nartsupha and Sompop Manarangsan. Bangkok: Thammasart University Press.

Samudavanij, Chai-anan. 1992. *roi pi haeng kampatirup rabob ratchakan thai* (The Co-Evolution of State and Political Power in Thailand). Bangkok: Chulalongkorn University Press.

Sarika, Khaen. 1988. *vara sutthai haeng chivit Jitr Phoumisak* (The Last Hours in the Life of Jitr Phoumisak). Bangkok: Sarika Press.

Satha-anand, Suwanna. 1990. *wa duay putta sassana kab sitthi manussayachon* (Regarding Buddhism and Human Rights). In *manussaya that nai pratchaya tawan ok* (Views in Eastern Philosophy), ed. Suwanna Satha-Anand. Bangkok: Chulalongkorn University Press.

Sawaengsak, Charnchai. 1997. *sara naroo phraratchabanyat khor mun khao sam khong ratchakam phor sor 2540* (The Freedom of Official Information Act B.E. 2540). Bangkok: Vinyuchon.

Schoeman, Ferdinand David. 1984a. Philosophical Dimensions of Privacy: an Anthology. Cambridge: Cambridge University Press.

Schoeman, Ferdinand D. 1984b. Privacy: Philosophical Dimensions of the Literature. In Philosophical Dimensions of Privacy: an Anthology, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

National Information Technology Committee Secretariat. 1995. Towards Social Equity and Prosperity: Thailand's Information Technology (IT) Policy into the 21st Century. Bangkok: National Electronics and Computer Technologies Center.

Siffin, William. 1966. The Thai Bureaucracy: Institutional Change and Development. Honolulu: East-West Center Press.

Krom Sinlapakorn. (Department of Fine Arts) 1962. *Khun Chang Khun Phaen* (Earl Chang, Earl Phaen). Bangkok: Khurusapha.

Slack, Jennifer Daryl and Martin Allor. 1983. The Political and Epistemological Constituents of Critical Communication Research. Journal of Communication 33 (3): 208-218.

Editorial staff. 1995. *waek maan pit tuaton samaphan prachathipatai: Prof. Dr. San Hattherat* (Lifting the Curtain of the Confederation of Thail Democracy: Prof. Dr. San Hattherat). Hi-Class Magazine, December 1995, 42-56.

Editorial staff. 1996. Committee rejects database access plan. The Nation, 13 July 1996, F 4.

Editorial staff. 1997. New identity cards offers ATM service exclusive to Siam Commercial Bank. The Bangkok Post, 29 October 1997, B 2.

Stifel, Laurence D. 1976. Technocrats and Modernization in Thailand. Asian Survey 15 (December): pp. 1-25.

Stonier, Tom. 1983. The Wealth of Information. London: Metheun.

Sukphanit, Kachorn. 1962. *Thanandon Phrai* (Status of Commoners). Bangkok.

Suphadiloke, Boonlert. 1984. *sitthi kam seusarn nai prathetthai* (The Right to Communicate in Thailand). Bangkok: Thammasart University Press.

Sussman, Gerald. 1991. The World Bank in the Philippines. In Transnational Communication: Wiring the Third World, ed. Gerald Sussman and John A. Lent. London: Sage.

Sussman, Gerald and John A. Lent, eds. 1991. Transnational Communication: Wiring the Third World. London: Sage.

Sutharoj, Pongpen. 1998. New ID cards likely to boast hi-tech features. The Nation, 8 December 1998, F 4.

Thompson, Judith Darvis. 1975. The Right to Privacy. Philosophy and Public Affairs 4 (4): 295-308.

Thompson, Virginia. 1941. Thailand: the New Siam. New York: Macmillan.

Toffler, Alvin. 1980. The Third Wave. New York: Morrow.

European Union. 1995. Directive 95/46/EC of the European Parliament and the Council of the 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free MOvement of Such Data. Official Journal of the European Communities L 281 (23 November 1995): 30-42.

Chula Unisearch. 1996. *khrongkam seuksa kot mai kam laek plian khor mun duany seu electronics nai prathet thai* (The Project to Study Laws Related to Electronic Data Interchange (EDI) in Thailand. Bangkok: NECTEC.

Uwanno, Borvornsak. 1993. *kot mai kab thang leuk sang khon thai* (Law and the Alternatives in Thai Society). Bangkok: Nititham Press.

Valaskakis, Simon. 1979. The Information Society: the Issue and the Choices. Montreal: Gamma.

Valdés, M. Isabel. 1987. Third World Countries and Conflicting Ideologies of the Information Age. In The Ideology of the Information Age, ed. Jennifer D. Slack and F. Fejes. Norwood, NJ: Ablex.

Vesaraj, Pratya. 1996. Bureaucratic Reform for the Future: Strategies for Development. In The Annual Seminar 1996 on Bureaucratic Reform for the Future of Thailand, ed. Chalongphob Susangkarakam and Apichai Phanthasane. Chon Buri, Thailand: Thailand Development Research Institute.

Warren, Samuel D. and Louis D. Brandeis. 1890. The Rights to Privacy. Harvard Law Review .

Weber, Max. 1930. The Protestant Ethic and the Spirit of Capitalism. Translated by Talcott Parsons. London: Allen and Unwin.

Weber, Max. 1978. Economy and Society, 2 vols. Berkeley: University of California Press.

Webster, Frank. 1995. Theories of the Information Society. London: Routledge.

Westin, Alan. 1967. Privacy and Freedom. New York: Atheneum.

Westin, Alan and Michael A. Baker. 1972. Databanks in a Free Society. New York: Times Book Co.

Whitaker, Reg. 1999. The End of Privacy: How Total Surveillance Is Becoming a Reality. New York: New Press.

Wilson, Kevin G. 1988. Technologies of Control. Madison: University of Wisconsin Press.

World Bank. 1990. World Development Report. Oxford: Oxford University Press.

World Bank. 1990. World Development Report. Oxford: Oxford University Press.

World Bank. 1993. The East Asian Miracle: Economic Growth and Public Policy. Oxford: Oxford University Press.

Wyatt, David K. 1969. The Politics of Reform in Thailand: Education in the Reign of King Chulalongkorn. Bangkok: Thai Wattana Panich.

Yin, R. K. 1989. Case Study Research: Design and Methods. Newbury Park: Sage.