Government Secrecy and Security Classifications in the Context of Integrity Management in Malaysia

Noreha Hashim
Faculty of Maritime Studies,
Universiti Malaysia Terengganu.

Corresponding author: noreha@umt.edu.my

ABSTRACT

Secrecy in government is almost always perceived as being antithetical to accountability and transparency in the conduct of democratic government. However, it is undisputable that government secrecy is practiced the world over because it is indispensable to state security, international relations, public and personal interests. Hence, democratic governments must perform a delicate balancing act between openness and confidentiality in the handling of official information. Indeed, effective governance requires various legal regimes that control government information through security classifications and impose punishments on offenders. This paper aims to address the dearth of research on government secrecy and security classifications in the context of integrity management in Malaysia. Integrity management encompasses not only the exercise of moral values by public institutions and officials but also the integrity of processes and procedures that uphold the integrity of governance. This exploratory research uses qualitative content analysis of data gathered from official government publications and websites, relevant documents and course notes, as well as interviews and correspondence with field experts. The inferences derived from themes and categories generated have resulted in several important findings. First, the 1972 Official Secrets Act (OSA) plays a significant role as part of a plethora of statutes and ethical codes that are indispensable to upholding government integrity. Second, weaknesses in balancing between openness and confidentiality when handling official information are attributed to organizational failure, public officials' lack of ethical values, comprehension and training. The challenge is to ensure that the OSA is not used for cover-ups of corruption, ethical misconducts and administrative transgressions while the proposed Freedom of Information Act does not lead to a culture of blaming and mistrust that could lead to the paralysis of government and governance.

Keywords: *Accountability, Governance, Secrecy, Transparency, Paralysis*

Received: 04/02/2020 **Revised**: 23/03/2020 **Accepted**: 13/06/2020 **Published**: 30/06/2020

INTRODUCTION

Malaysia has institutionalized means to ensure the accountability and responsiveness of government towards its citizens, e.g., democratic mechanisms of oversight in the forms of regular elections, channels for airing public opinions and public deliberations (Sagar, 2007). Moreover, these means are also supplemented by quite a comprehensive integrity management framework which includes conduct and ethical codes that are implemented by its civil service. It is important to note that integrity management encompasses not only the exercise of moral values by public institutions and officials but also the integrity of processes and procedures that uphold the integrity of governance. As such, security classifications of official documents form an integral part of integrity management because adequate protection of sensitive information is needed to ensure that the integrity of government is not compromised.

However, the astounding magnitude and number of incidences of abuses of power, criminal breach of trust, ethical misconducts, fraud, grand corruption and money laundering by top political leaders and civil servants under the administration of Dato' Seri Mohammad Najib bin Tun Abdul Razak (April 3, 2009 – May 10, 2018), have put to question the state of integrity of government and governance in Malaysia. For example, one of the world's worst public-corruption scandals involves a government-owned company, the 1Malaysia Development Berhad (1MDB); whereby a colossal amount of money purportedly raised for the country's development efforts was systematically appropriated, diverted and stolen by some of the country's top political leaders, civil servants, particular individuals, companies and financial institutions. The money was used not only for their personal consumption, glorification and profit, but also for buying and maintaining support from within and between the component parties of the then ruling Barisan Nasional (BN).

Indeed the country's descent into kleptocracy has also been facilitated by Najib administration's sacking of opposing cabinet members, replacement of key judicial and executive figures as well as thwarting enforcement agencies' investigative efforts, and abusing government secrecy and security classifications of official documents; all of which served to cover extensive corrupt and fraudulent activities (Gabriel, 2018). Hence it is disquieting to observe how institutionalized measures for government accountability and responsiveness have been turned on their heads, particularly from 2009 – 2018.

Indeed changes in the paradigm of the management of government secrecy in Malaysia can be attributed to the prevalence of exchanging and sharing of a vast amount of public, personal and organizational information on social media, the increased demand for greater government transparency by the people, e-government applications and transactions, as well as increasing threats of violations of government information technology systems. However, in spite of the above changes, one notes that inadequate academic attention has been paid to the roles of government secrecy and security classifications in the context of integrity management in the country. Hence, it is believed that a more thorough understanding of the nature and facets of government secrecy and security classifications can shed more light on how they can be used to promote and also thwart, the integrity of government. Therefore the objectives of this article are to: (i) examine the nature and facet of government secrecy and security classifications in general; (ii) identify how government secrecy and security classifications are incorporated in integrity management in the country; and (iii) discover the ways with which government secrecy and security classifications can be used to simultaneously promote and obstruct the integrity of government in Malaysia.

METHODS

A qualitative content analysis method is used for this exploratory research. This is because of the subjective nature and facets of secrecy, as well as the exacting demands for confidentiality and transparency in democratic government. Thus, it is believed that an in-depth understanding of the concept of secrecy and its operationalization in government are essential to the contextualization and understanding of the social reality of the phenomenon in question. Primary and secondary data are collected from official government publications and websites, relevant documents and course notes, as well as interviews and correspondence with field experts. The qualitative content analysis performed comprises the following steps. First, the elements to be coded are pinpointed and the codes that represent the themes of the study are formulated. These include “secrets”, “secrecy”, “government security classifications”, “ethics”, “integrity”, “government integrity management”, “conduct and ethics codes, Malaysia”, “legal instruments against corruption, Malaysia”, “transparency/openness”, “accountability” and “confidentiality” among others. Second, patterns, relationships and themes are identified by comparing primary with secondary data, as well as scanning for recurring phrases and words. This is followed by inductively devising a coding scheme that is tried on a selected sample and is rechecked for consistency. Finally, the coded data are interpreted according to patterns, relationships and themes discovered in relation to the objectives of the research.

RESULTS

In line with the research's objectives, the results are presented below in three sections. First, the nature and facet of government secrecy and security are discussed so as to illuminate their different facets and dimensions. The second section presents the ways and means of how government secrecy and security classifications are incorporated in the integrity management framework in Malaysia. Finally, the third section shows how government secrecy and security classifications can be a double-edged sword; whereby it can be used to simultaneously promote and obstruct government integrity.

The Nature and Facet of Government Secrecy and Security Classifications

Secrets originate from Latin *secretum,* and secrecy entails one's intentional decision on what to conceal and what to share with others (Birchall, 2016; Pozen, 2010). It has been argued that secrets and secrecy are social phenomena that are indispensable for social interactions, and are observable in the relationships between individuals, groups of people, governments and citizens, within governments, and between countries (Broeders, 2016; Simmel, 1906). Secrets are valuable because they can be traded for money, influence, prestige and power, as well as for maintaining and controlling relationships and social stratification (by selecting who would be privy to the types and contents of secrets shared, as well as those denied access to them) (Simmel/Wolff, 1950). Secrecy is also "slippery" in nature because of the different guises it assumes in accordance with the different contexts of activities within which it occurs (Benjamin, 2017).

Benjamin (2017) argues that in government, secrecy can either be "direct" or "indirect". Direct secrecy arises when the government affirmatively withhold information about its activities from the public (e.g., by classifying documents pertaining to those activities as "secret") (pp. 5-6). It prevents sensitive information from being shared with potential misfeasors' by justifying that this is done to protect public interests. Moreover, it grows proportionately to the number of documents with secret classification. Indirect secrecy occurs when the government intentionally does not take the required action, thus rendering applicable accountability and transparency mechanisms ineffective. It is also the result of government activities being outsourced to private parties, which exempt them from public law and scrutiny. In addition, it expands in size in proportion to the extent of government functions being outsourced to the private sector on the grounds that that the government is ineffective, incapable or too cumbersome to address public interests. Thus, the forms of direct and indirect secrecy identified reaffirm Warren's (1974) argument that secrecy enveloping the operations of governments and activities of civil servants provides a conducive breeding ground for corruption. Eventually secrecy can also lead to a situation of mistrust whereby citizens lose confidence in their government, and can only be reassured if government agrees to be more open.

Sissela Bok (1983), who is a prominent philosopher and ethicist, however, has argued against complete openness/transparency as the total revelation of secrecy would have disastrous consequences. According to Birchall (2016) the ethical, democratic, and social desirability of openness as espoused by a neoliberal and capitalistic stance can also be antithetical to the notions of "community and equality" (p.154). Moreover, the need for secrecy is protected by law in cases involving national security, citizens' rights to personal information and privacy concerns (e.g., individual legal, medical and taxation information), personal safety (for witnesses of crimes and criminal activities), as well as secret balloting in elections to deter vote buying, to name a few examples. Indeed, to exercise secrecy also means to exercise trust, whereby the government is entrusted by citizens to know the appropriate timing and circumstances within which direct and indirect secrecy are to be exercised without betraying the trust given.

A comparison of government security classifications (as means of direct secrecy) in various countries and parts of the world (e.g., United Kingdom, United States of America, Australia, and the European Union) shows that they share several fundamental characteristics. First, the government security classifications constitute administrative systems to enable the classification of information according to their level of sensitivity (e.g., top secret, secret, confidential, restricted, official, protected, etc.) as determined by the extent of damage that could occur if the information are compromised, misused or lost. Second, each security classification determines the degree of care and processes with which the information are to be collected, generated, handled, protected, shared, disclosed, unclassified and destroyed, as well as ensuring that the appropriate security controls are installed in proportion to the perceived level of threat. Third, the responsibility for safeguarding the confidentiality of accessed or entrusted government information, is shouldered by all civil servants as well as those who work with government. Hence, they must be provided with the required skills, training and awareness of the legal sanctions that can be imposed on them in the efforts to ensure that their actions do not compromise the integrity of contents and processes of classified information. Fourth, the number of people granted access to information is inversely correlated to the level of security classification (e.g., access to top secret information is limited to a selected few and vice versa). In addition, the sharing of information is also governed by the "need to know" principle (Cabinet Office, 2012; US Executive Order 13526, 2009; the Australian Government Security Classification System, 2011; European Union Council Decisions, 2013).

However, it is important to note that these government security classifications encompass not only "genuine national security secrecy", but also "bureaucratic secrecy" and "political secrecy" (Aftergood, 2008, pp. 402 – 404). Thus while "genuine national security secrecy" can be justified in the name of public interest, it has been argued that "bureaucratic secrecy" can be used by public bureaucracies to hoard information (Weber, 1946). It is also important to note that "political secrecy" happens when political leaders in power abuse the security classifications to "…advance a self-serving agenda, to evade controversy, or to thwart accountability….[as well as to conceal]… violations of law…" (Aftergood, 2008, p. 403). As the amount of information and types of activities that fall within the ambit of the government security classifications are extensive, it is difficult to ascertain whether information are classified in the name of "genuine political secrecy" or for the purposes of "bureaucratic secrecy" and "political secrecy". Thus, this explains the concerns over the huge number of documents that have been classified over the years, as well as the exorbitant costs of protecting classified information (Aftergood, 2008).

The Incorporation of Government Secrecy and Security Classifications in Integrity Management in Malaysia

Governance refers to the process of "…authoritative policy-making on collective problems and interests, and implementation of those policies" (Huberts, 2014, p.68) through the exercise of power involving governmental and/or non-governmental actors (Huberts, 2018). As such, integrity is an integral concept in government and governance. It originates from the Latin word *integra's* that encapsulates a state of perfect virtuousness, unblemished, uncorrupted, unimpaired, accountable, ethical, honest, having sound judgment and upstanding moral character (Dobel, 2016). In the context of government and governance, the scope of integrity and integrity management include ensuring and setting-up the required conduct and ethical codes for personal integrity, professional integrity and organizational integrity, as well the legal framework needed to enforce compliance and impose punishment.

According to Kidder (2005), personal integrity refers to the ability to remain steadfast in adhering and executing one's ethical principles despite the conflicts, pressures, or temptations for deviations. However, it is also argued that personal integrity also includes the ability to be empathetic and merciful given life's extenuating circumstances so as to avoid cruelty and inhumaneness (Koehn, 2005). In the case of public officials, professional integrity refers to the adherence to public service ethos that are translated into public service practices that are conducive to the pursuance of public interest (Rayner, Williams, Lawton & Allinson, 2010). Palazzo (2007) outlines the requirement for organizational integrity, namely (i) ethical leaders with exemplary conduct as role models, (ii) ensuring the existence of a conducive organizational climate for fostering ethical behaviors and resolving ethical dilemmas, (iii) training and education for appreciation of moral dimensions of actions taken, and implications of decisions made. Finally, the appropriate legal remits to enforce compliance and impose punishment must be instituted so that the seriousness of the need to uphold the integrity of government and governance is fully appreciated by those in government, as well as entities and individuals who work with government.

Government secrecy and security classifications are well incorporated in integrity management in Malaysia. For example, all government ministries, departments and agencies in Malaysia have their own codes of conducts and ethics that comprise elements of: (i) professional integrity, (ii) organizational integrity, (iii) the need for public officials to abide by laws, rules, regulations, circulars and directives as dictated by the Government of Malaysia (GoM), as well as (iv) to preserve and protect the safety and secrecy of government information by following the specific instructions given on accessing, classifying, handling, processing, storing, communicating, declassifying and destroying confidential information. Indeed, all public officials must obey the Government of Malaysia Security Orders or *Arahan Keselamatan Kerajaan Malaysia*, as well as the provisions of the 1972 Official Secrets Act (OSA)

(Enforcement Agencies Integrity Commission, 2016; Public Complaints Bureau, 2014).

The OSA (Act 88) contains provisions on: (i) security classifications of information, (ii) offences for disclosing official secrets and spying, (iii) obligations to provide information and report on suspected transgressions, as well as (iv) powers of enforcement accorded to the state. First, security classifications of information must be carried out according to the procedural mechanism specified by the OSA. This is supplemented by the Protection Security Orders which provide the detailed explanations needed for its operationalization. Government information are either official secrets that are included in the Schedule (s.2, OSA), official secrets that are not included in the Schedule (s.2, OSA), or official documents (ss. 9(2) and 2, OSA).

Information that fall under the Schedule are: (i) Cabinet documents, as well as minutes/records of Cabinet and Cabinet Committee meetings on decisions and discussions undertaken, (ii) documents, minutes and records of State Executive Council and State Executive Council Committees' meetings and deliberations, and (iii) documents on defense, international relations and national security. Information that fall outside of the Schedule are: (i) other official documents, communication, information and materials that Ministers, Chief Ministers or appointed public officers (whose letters of appointment are signed by the Prime Minister), choose to classify as "Top Secret", "Secret", "Confidential" or "Restricted". Official documents are documents that are in the possession of the civil service that can be physical, virtual, audio or photographic in nature.

It is important to note that the motto of the Chief Government Security Office (CGSO) of the Prime Minister's Department is "Preserving Secrecy Ensuring National Security" or *Kerahsiaan Terpelihara Menjamin Keselamatan Negara*. As such, its main functions are: (i) preparing and issuing protection security orders, (ii) providing protection security advice on the security of government buildings, documents, personnel and the use of Information and Communication Technology (ICT) by public organizations and officials, (iii) acts as the secretariat to all government ministries, departments and agencies' security committees and targets, and (iv) conducts inspection on the implementation of protecting government secrecy at all governmental levels (CGSO, 2019).

Other legal measures that are used to ensure government secrecy and compliance by public officials include the Sedition Act 1948 [Act 15], section 203A of the Penal Code 2015 [Act 574], the Communications and Multimedia Act 1998 [Act 588], as well as the Public Officers (Conduct and Discipline) 1993 Regulation 4 [P.U(A) 395/1993, whereby public officials who are found guilty of disclosing government secrets can be subjected to disciplinary actions, fired and/or face legal actions brought under the relevant acts for transgressions committed.

How Government Secrecy and Security Classifications can be used to Simultaneously Promote and Obstruct Government Integrity

According to expert informants, the current government secrecy and security classifications as provided by the OSA and supported by a plethora of Acts and Regulations, provide for excellent integrity management that promotes government integrity. However, inspectorate visits conducted reveal the different levels of organizational capacity among government ministries, departments and agencies at implementing protection security orders issued with regard to protecting government secrecy, and adhering to the required standard operating procedures (SOP) for security classifications. Moreover, some public officials' inadequate commitment to ethical values and codes of conduct, as well as lack of comprehension and appreciation for the need to safeguard government secrecy, are compounded by inadequate training that can/and do compromise government secrecy and security classifications as means of integrity management. Carelessness, inattention to details and lack of enforcement against transgressors for not following the SOP are also factors that weaken integrity management and compromise government integrity despite the existence of the laws and regulations. Hence these findings illustrate that government secrecy and security classifications as important elements of integrity management in Malaysia can be a double-edged sword. This characteristic makes it possible for government secrecy and security classifications to be simultaneously used to promote as well as obstruct government integrity.

It is important to note that the integrity of government depends on: (i) whether the government can be trusted to keep secrets, (ii) whether the secrets kept are really secrets worth keeping from the public, (iii) whether the government can provide assurances that it has genuine national security concern at heart and its actions are not influenced by bureaucratic secrecy or political secrecy, and (iv) whether the government can provide the appropriate level of mix between openness and secrecy demanded by the people. It is disconcerting to discover that these questions have not been debated or examined in-depth in Malaysia. Hence it is important that this exercise is conducted to halt government secrecy and security classifications from obstructing government integrity instead of promoting it.

Moreover, by lumping “genuine national security secrecy”, “bureaucratic secrecy” and “political secrecy” together under the OSA, one cannot help but wonder whether this arrangement provides more opportunities for abuses, corruptions and transgressions by politicians, civil servants and those who work with government. Indeed, those in the know are not able to provide accurate information as to the exact number of information that have been classified according to “genuine national security secrecy”, “bureaucratic secrecy” and “political secrecy” over the years. Information about the true financial costs associated with government secrecy and security classifications are also not known. A possible explanation for this situation is perhaps the respondents are not high enough in the hierarchy of power to be “in the know” of such information. Indeed, without this information it is impossible to know whether government secrecy and security classifications as important elements of integrity management, obstruct or promote government integrity.

CONCLUSION

The debate surrounding government secrecy and security classifications are mired in sticky issues fundamental to the conduct of democratic government. Indeed, in Malaysia extensive and in-depth reasoned discussions must be undertaken so that the nature and facets of government secrecy are understood, and responses devised according to needs of the Malaysian public. Indeed, changes in the paradigm of the management of government secrecy in Malaysia require that more adaptive and effective measures be introduced. This is to ensure that despite the prevalence of exchanging and sharing of a vast amount of public, personal and organizational information on social media, the increased demand for greater government transparency by the people, e-government applications and transactions, as well as increasing threats of violations of government information technology systems, the integrity of government and governance remain intact. It is also imperative that the OSA is not used for cover-ups of corruption, ethical misconducts and administrative transgressions. While more openness is required to prevent scandals such as the 1MDB and halt the descent of the country into kleptocracy, the panacea does not necessarily take the form of a Freedom of Information Act. Indeed, too much transparency can result in a culture of blaming and mistrust that could lead to the paralysis of government and governance. Thus, a more rational approach is to ensure that the OSA is repealed so that government secrecy and security classifications can really sort information into "genuine national security secrecy", "bureaucratic secrecy" and "political secrecy" categories. Only then can integrity management really promote government integrity in Malaysia.

ACKNOWLEDGEMENT

The author wishes to thank field experts for sharing their knowledge and experiences with her. Feedbacks have been used to improve the article.

REFERENCES

Aftergood, S. (2008). Reducing Government Secrecy: Finding What Works. *Yale Law and Policy Review*, 27(2), 399-416.

Australian Government. (2018). *Protective Security Policy Framework*. Retrieved from https://www.protectivesecurity.gov.au

Benjamin, A. B. (2017). The Many Facets of Secrecy. *William & Mary Policy Review*, 8(2), 1-49.

Birchall, C. (2016). Managing Secrecy. *International Journal of Communication*, 10, 152-163.

Bok, S. (1983). *Secrets: On the Ethics of Concealment and Revelation.* New York: Vintage Books.

Broeders, D. (2016). The Secret in the Information Society. *Philosophy & Technology*, 29(3), 293-305.

Cabinet Office. (2018). Government Security Classifications. Retrieved from https://assets.publishing.service.gov.uk

CGSO. (2019). *Fungsi CGSO*. Retrieved from http://www.cgso.gov.my

Dobel, J. P. (2016). Integrity in the Public Service. *Public Administration Review*, 50(3), 354-366.

Enforcement Agencies Integrity Commission. (2016). *Kod Etika dan Tatakelakuan*. Retrieved from http://www.eaic.gov.my

EU Council Decision of 23 September 2013 on the security rules for protecting EU classified information. Retrieved from http://data.europa.eu/eli/dec/2013/488/oj

Gabriel, C. (2018). The Rise of Kleptocracy: Malaysia's Missing Billions. *Journal of Democracy, 29(1), 69-75.* doi:10.1353/jod.2018.0005

Huberts, L.W. J. C. (2018). Integrity: What it is and Why it is important. *Public Integrity,* 20: sup 1, S18-S32. doi: 10.1080/10999922.2018.1477404.

Huberts, L.W. J. C. (2014). *The integrity of governance. What it is, what we know, what is done, and where to go.* Basingstoke, England: Palgrave Macmillan.

Kidder, R. M. (2005). *Moral Courage*. New York, NY: Harper Collins.

Koehn, D. (2005). Integrity as a Business Asset. *Journal of Business Ethics*, 58(1-3), 125-136.

Palazzo, G. (2007). Organizational Integrity – Understanding the Dimensions of Ethical and Unethical Behavior in Corporations. *Corporate Ethics and Corporate Governance,* 113-128.

Pozen, D. (2010). Deep Secrecy. *Stanford Law Review*, 62(2), 257-339.

Public Complaints Bureau. (2014). Panduan Pengurusan Keselamatan Dokumen Terperingkat. Retrieved from http://www.pcb.gov.my

Rayner, J., Williams, H., Lawton, A. & Allinson, C. (2010). Public Service Ethos: Developing a Generic Measure. *Journal of Public Administration Research and Theory,* 20(1), 27-51.

Sagar, R. (2007). On Combatting the Abuse of State Secrecy. *The Journal of Political Philosophy*, 15(4), 404-427.

Simmel, G. (1906): The Sociology of Secrecy and of Secret Societies. *American Journal of Sociology,* 11 (4), 441-498.

Simmel, G./Wolff, K. (1950). *The Sociology of Georg Simmel*. Translated, edited and with an Introduction by Kurt. H. Wolff. New York: The Free Press.

US Executive Order 13526 (2009). Retrieved from https: www.federalregister.gov

Warren, E. (1974). Governmental Secrecy: Corruption's Ally. *American Bar Association Journal*, 60(5), 550-552.

Weber, M. (1946). Bureaucracy. In *Essays in Sociology*. H. H. Gerth & C. Wright Mills (eds). Oxford: Oxford University Press.