THE CENTER TO COMBAT
CORRUPTION AND CRONYISM

Whistleblower Protection or Suppression?

A Decade of Section 203A of the Penal Code

THE CENTER TO COMBAT
CORRUPTION AND CRONYISM

Whistleblower Protection or Suppression? A Decade of Section 203A of the Penal Code

The Center to Combat Corruption and Cronyism (C4 Center)

Authors

Arief Hamizan

Jason Poh Hong Lee

Raja Nadhil Aqran

Editor

Pushpan Murugiah

Cover and Layout

Asyraf Abdul Samad

February 2025

C Four Consultancies Sdn Bhd

Unit A707, Pusat Dagangan Phileo Damansara 1,

No. 9, Jalan 16/11, Off Jalan Damansara,

46350 Petaling Jaya, Selangor, Malaysia.

www.c4center.org

Email: contact@c4center.org

Telephone: +603-7660 5140

Whistleblower Protection or Suppression?

A Decade of Section 203A of the Penal Code

The Center to Combat Corruption and Cronyism

TABLE OF CONTENTS

Executive Summary

Over the past decade, several multi-billion ringgit scandals have come to light in Malaysia, the most notable one being the 1Malaysia Development Berhad (1MDB) scandal. What many of these cases have in common is the misuse of public institutions and funds, highlighting the vulnerability of government to corruption and abuse of power. In this, whistleblowers – especially from the civil service – play a crucial role in anti-corruption efforts by sharing evidence of crime and cooperating with law enforcement. Unfortunately, the existing legal framework for whistleblower protection in Malaysia – governed by the Whistleblower Protection Act 2010 (WPA 2010) – is severely inadequate. The threat faced by civil service whistleblowers is particularly acute due to the introduction of s. 203A of the Penal Code (s. 203A), which came into force in 2014. Essentially, this law criminalises the disclosure of information obtained in the performance of public duty. The broad scope of this law deters would-be whistleblowers in the civil service from coming forward and revealing first-hand knowledge of government corruption and abuse of power.

This report explores the difficult relationship between s. 203A and the WPA 2010. As will be explored fully in the case studies in this report, it is argued that s. 203A effectively creates legal and practical barriers for whistleblowers to access the protections afforded under the WPA 2010. S. 203A is frequently used by law enforcement agencies as an intimidation tactic to inculcate a culture of secrecy and instil fear within the civil service and even private sector individuals, casting doubt on the enforcement of anti-corruption laws in Malaysia. The vague wording of the section makes potential whistleblowers uncertain of their entitlement to legal protection, which further deters them from disclosing instances of corruption.

A comparative study of similar laws from different jurisdictions reveal that mitigating factors are absent in confining the application of s. 203A to its specific purpose. In huge contrast with our Commonwealth counterparts, Malaysia has a lack of legislative commitment in striking a fair balance between withholding information to protect legitimate interests and encouraging disclosure of information to fight corruption and uphold the public's right to know.

To address these challenges, this report recommends the following:

- **Repeal s. 203A of the Penal Code**
- **Amend the Whistleblower Protection Act 2010**
- **Enact a Right to Information Law**
- **Amend the Official Secrets Act 1972**

When viewed against the backdrop that corruption in Malaysia is endemic, the significance of the whistleblower's role in exposing corruption and assisting law enforcement agencies only becomes more obvious. After ten years of s. 203A, it is high time for Parliament and the government to take initiatives to enhance whistleblower protections as a crucial step in fighting corruption at all levels of society in Malaysia.

CHAPTER ONE

Introduction

In 2014, s. 203A of the Penal Code was introduced into Chapter XI of the Penal Code through the Penal Code (Amendment) Act 2014, as follows:

> *S. 203A: Disclosure of information*
>
> *(1) **Whoever discloses any information** or matter which has been **obtained by him in the performance of his duties or the exercise of his functions under any written law shall be punished** with **fine** of **not more than one million ringgit**, **or** with **imprisonment** for a term **which may extend to one year**, **or** with **both**.*
>
> *(2) **Whoever has any information** or matter **which to his knowledge has been disclosed in contravention of subsection (1) who discloses that information** or matter **to any other person shall be punished** with **fine** of **not more than one million ringgit**, or with **imprisonment** for a term **which may extend to one year**, or with both.*[1]

[1]. Act 1471, section 10.

In other words:

- It is a criminal offence under s.203A(1) for any individual charged with legal duties or functions to disclose any information obtained by him during the performance of his duty or function;
- It is a criminal offence under s.203A(2) for any individual to disclose any information which he knows is obtained in violation of s.203A(1) i.e. information that is obtained during the performance of one's legal duties or functions; and
- The maximum punishment for both offences is a fine not more than RM1 million, or imprisonment for not more than 1 year, or both, which is considerably heavy to deter unauthorised disclosure.

In the parliamentary debates on the introduction of the section, the acting Minister in the Prime Minister's Department (Legal Affairs), Nancy Shukri, stated that the intention of the amendment was to fight organised crime by criminalising improper disclosure of information by public servants.[2] However – whether foreseen or not – the passing of the amendment has led to major negative implications for whistleblowers in Malaysia.

[2]. Hansard dated 22 October 2013, page 59: https://www.parlimen.gov.my/files/hindex/pdf/DR-22102013.pdf.

1.1 Background of whistleblower protection in Malaysia

In Malaysia, corruption scandals in the public sector have become a frequent and highly publicised occurrence, often dominating headlines and sparking public outrage. Among the most notable cases is the 1Malaysia Development Berhad (1MDB) scandal, which not only highlighted the embedded nature of corruption within the public sector, but also illustrated the huge impact whistleblowers can have in anti-corruption efforts. The 1MDB scandal involved the misappropriation of billions of ringgit in public money, which was then spent on luxury items such as yachts, jewellery, real estate, and even funding for Hollywood films. This scandal led to the fall of the Barisan Nasional coalition government after 61 years of uninterrupted rule, and the conviction of former Prime Minister Najib Razak for his role in the affair. Pivotal to uncovering the scandal were the efforts of numerous whistleblowers. One example was Xavier Gusto, who leaked 90GB of data including 227,000 emails from his former employer, PetroSaudi, which had signed the first major deal with 1MDB.[3] Separately, government auditor Nor Salwani Muhammad became a key witness for the prosecution after she secretly made voice recordings of a 2016 meeting where changes to the Auditor-General's audit report on 1MDB were ordered. She also retained a draft copy of the original 1MDB audit report which had been ordered to be destroyed by her superiors.

The subsequent efforts of the media, civil society organisations, political actors, and the general public to hold the corrupt actors accountable would not have been possible without the extreme risks

[3]. The Guardian's comprehensive reporting of the 1MDB whistleblower's story: https://www.theguardian.com/world/2016/jul/28/1mdb-inside-story-worlds-biggest-financial-scandal-malaysia.

taken by the whistleblowers. Thus, ensuring the provision of strong protections for whistleblowers – that can ensure their safety and encourage them to come forward – is critical for combatting corruption.

Against this context, it must be recognised that whistleblowers play an essential role in exposing corruption, serious wrongdoings and mismanagement of public funds, which ultimately affects the overall welfare of citizens, financial integrity of the nation, democratic values, human rights and the rule of law.[4] It cannot be overstated that whistleblowing itself is an inherently dangerous task, as whistleblowers are subjected to the risk of being dismissed from their employment, arrested, harassed with death threats, or killed.[5] Furthermore, proving corruption is not a straightforward task, as it often involves sophisticated transactions that conceal illicit activity, voluminous documents, and the movement of assets in and out of jurisdictions. Evidence is difficult, if not impossible, for enforcement agencies to retrieve or trace without the help of whistleblowers who have first-hand knowledge or proximity to incriminating matters.[6]

UNCAC and the Whistleblower Protection Act 2010

Articles 33 and 37 of the United Nations Convention Against Corruption (UNCAC) – which has been signed and/or ratified by 190

[4]. Resolutions and decisions adopted by the Conference of State Parties to the United Nations Convention against Corruption at its tenth session, CAC/COSP/2023/10/8: Protection of reporting persons, https://www.unodc.org/documents/treaties/UNCAC/COSP/session10/resolutions/L-documents/2325382E_L.12_Rev.1.pdf

[5]. Transparency International: *Whistleblowing*: https://www.transparency.org/en/our-priorities/whistleblowing.

[6]. National Whistleblower Center: *Why Whistleblowing Works*. See also Transparency International Policy Position #01/2010, *Whistleblowing: an effective tool in the fight against corruption*, https://images.transparencycdn.org/images/2010_1_PP_Whistleblowing_EN.pdf

States Parties – obliges a State Party to consider incorporating within their domestic laws appropriate measures for the protection of whistleblowers against unjustified treatment and immunities from prosecution.

Malaysia signed the UNCAC on December 2003 and ratified it on September 2008. To fulfil Malaysia's obligations under the UNCAC, the then Barisan Nasional Government enacted the Whistleblower Protection Act 2010 (WPA 2010).

According to the Preamble of the WPA 2010, this law was introduced as:

> *An Act **to combat corruption** and other wrongdoing **by encouraging and facilitating disclosure of improper conduct** in the public and private sector, **to protect persons making those disclosures**... to provide for the matters disclosed to be investigated and dealt with.*

Prior to the enactment of the WPA 2010, legal protection for 'informers' existed in a patchwork mode across different laws.[7] These laws provided no clear assurances regarding protection of anonymity, protection against detrimental action and of the obligations for enforcement agencies or corporate entities to take appropriate action upon receiving complaints of wrongdoing.[8]

Hence, the introduction of the WPA 2010 was potentially a step in the right direction. For example, section 7 affords three types of protection to a whistleblower, namely:

---

[7]. In the context of corruption, see s. 65 of the Malaysian Anti-Corruption Commission Act 2009. In the corporate sector, see s. 587 of the Companies Act 2016. In respect of money laundering, see ss. 5 and 24 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

[8]. Tan Keat Siang, *Whistle-blowing as an Anti-Corruption Tool - An Overview* (Journal of Public Security and Safety, Volume 10, No 1/2020): https://www.moha.gov.my/images/maklumat_bahagian/ipsom/jurnal/volume10/no6_volume_10_2020.pdf.

a. Protection of confidential information;
b. Immunity from civil and criminal action; and
c. Protection against detrimental action.

However, the legislation has several shortcomings. Section 7(1) only confers whistleblower protection to an individual who makes disclosure to enforcement agencies, such as the police or the Malaysian Anti-Corruption Commission (MACC). In many other jurisdictions, protection is also granted if disclosure is made to other parties, such as the media, civil society organisations, and parliamentarians.[9] Even worse, section 8(1) of the WPA 2010 expressly prohibits a whistleblower from disclosing the information to a third party once an investigation has begun. Read together with section 11, this can lead to revocation of the whistleblower's protections entirely. C4 Center has previously published a report on the weaknesses of the WPA 2010 which included several recommendations for reform.[10]

1.2 Legal implications of S. 203A for whistleblowers

For the purposes of this paper, section 6(1) WPA 2010 is of particular importance:

6. (1) A person may make a disclosure of improper conduct to any enforcement agency based on his reasonable belief that any person has engaged, is engaging or is preparing to engage in improper conduct:

[9]. For example, the Australian Public Interest Disclosure Act 2013 provides multiple channels of disclosure for whistleblowers, such as internal and external disclosures to the public, emergency disclosures and legal practitioner disclosures.

[10]. C4 Center, *Gaps in the Act: A Legal Analysis of Malaysia's Current Whistleblower Laws* (2021): https://c4center.org/gaps-in-the-act-a-legal-analysis-of-malaysias-current-whistleblower-protection-laws/. See also C4 Center's press statements on whistleblower reform: https://c4center.org/new-paradigm-shift-needed-protect-whistleblowers-fight-against-corruption-0/

Provided that such disclosure is not specifically prohibited by any written law.

S. 203A specifically prohibits disclosure of a broad scope of information for public officials. As such, the section significantly cuts access to any form of whistleblower protection for potential whistleblowers in the public service. This is of particular concern in Malaysia when considering the frequency and scale of public sector corruption. While the 1MDB corruption scandal rightly made global headlines, there has been a noticeable lack of accountability for numerous other public sector corruption cases that have been exposed, such as the Scorpene scandal,[11] the littoral combat ship (LCS) scandal,[12] helicopter procurement scandals,[13] Taman Rimba Kiara land deal scandal,[14] and the Private Finance Initiative (PFI) scandal.[15]

Without the first-hand evidence that is often only accessible to public officials, bringing justice to those involved in high-level corruption can be a near impossible task. Recognising the inadequacies of the current legal framework for whistleblower protection in Ma-

[11]. Malaysiakini dated 23 July 2017: https://www.malaysiakini.com/news/389497. See also https://c4center.org/msian-authorities-urged-to-act-on-scorpene-deal-after-french-charge/.

[12]. https://c4center.org/the-littoral-combat-ship-lcs-scandal-the-crooks-and-villains-behind-malaysias-defence-procurement-laid-bare/.

[13]. The Ministry of Defence spent more than RM 300 million for six lightweight combat helicopters which were never delivered to the Royal Malaysian Army. The Edge Malaysia dated 20 May 2019: https://theedgemalaysia.com/article/report-rm300m-paid-usmade-helicopters-were-never-delivered. No further actions were taken after the MACC had completed its investigations, see Free Malaysia Today dated 28 July 2022: https://www.freemalaysiatoday.com/category/nation/2022/07/28/no-further-action-over-purchase-of-helicopters-says-minister/.

[14]. C4 Center's press statement dated 22 January 2019: https://c4center.org/press-statement-tengku-adnan-should-be-investigated-dubious-land-deal-relating-taman-rimba-kiara/.

[15]. The Edge Malaysia dated 26 July 2018: https://theedgemalaysia.com/article/cover-story-secret-government-debt-has-ballooned-rm50-billion. See also C4 Center's PFI report: https://c4center.org/wp-content/uploads/PFI-Report.pdf .

laysia, this report examines the impact of s. 203A of the Penal Code on whistleblower protection in Malaysia since its introduction over ten years ago.

1.3 Methodology

The primary objective of this report is to explore the legal and practical implications of s. 203A, especially on whistleblowing and the overall effort to combat corruption in Malaysia. This report first analyses the background and context surrounding s. 203A. This includes discussions within Parliament between the Minister and Members of Parliament (MPs) and also outside of Parliament by grassroot activists, civil society organisations and legal practitioners. Then, this report analyses the law itself, examining its ambiguous nature and issues of proportionality by exploring the language used and the context of its placement within the Penal Code. After identifying the issues with the law itself, the report then explores the potential ramifications of s. 203A. These include how s. 203A enables the Executive – through various law enforcement agencies and the Attorney-General – to silence whistleblowers and whether the judiciary is able to 'fill the gaps' of s. 203A through ordinary principles of statutory interpretation.

For the purposes of analysing s. 203A, this report reviews laws which prohibit disclosures of information from different Commonwealth jurisdictions such as Canada, United Kingdom, New Zealand, Australia and Singapore, highlighting the similarities and differences between s. 203A and these laws. This is particularly significant in drawing attention to the potential issues that might arise in enforcing s. 203A. Furthermore, the comparative study also reveals and provides persuasive justifications for the recommended reforms to

s. 203A.

In order to illustrate the urgent need to reform s. 203A and to demonstrate how the section is susceptible to abuse, this report incorporates real life instances in which law enforcement agencies have employed s. 203A. This also includes multiple statements made by the police, which show the varying interpretations regarding s. 203A.

The sources for this report include the Hansard, online news reports and press, journal articles and academic opinions on whistleblowing laws, Malaysian and foreign legislation, as well as case judgments.

The next chapter provides a detailed background of s. 203A, including the arguments for and against its introduction as it was being tabled in Parliament. Chapter 3 examines the weaknesses of s. 203A from a legal standpoint, while Chapter 4 provides a comparative legal analysis with similar provisions in other jurisdictions. Chapter 5 highlights several cases involving s. 203A which illustrate how it has been employed over the past decade. Finally, recommendations and conclusions are outlined in Chapters 6 and 7 respectively.

CHAPTER TWO

S. 203A of the Penal Code

2.1 The introduction of s. 203A

The Penal Code (Amendment) Bill 2013 - which included the new s. 203A – was tabled in 2013.[16] During Parliamentary Readings to introduce the section, the acting Minister in the Prime Minister's Department (Legal Affairs), Nancy Shukri, stated that the purpose of s. 203A was to fight organised crime by criminalising improper disclosure of information by public servants.[17] The section purportedly addresses collusion between enforcement officers and criminals.

When it comes to the design of s. 203A, it was the Cabinet's deliberate intention to enact s. 203A in very broad language. The rationale was to establish s. 203A as an "enabling clause", envisioned

[16]. D.R. 9/2013: https://www.parlimen.gov.my/files/billindex/pdf/2013/DR%209_2013%20EN.pdf

[17]. Hansard dated 22 October 2013, page 59: https://www.parlimen.gov.my/files/hindex/pdf/DR-22102013.pdf.

to fortify existing anti-corruption frameworks under the Malaysian Anti-Corruption Commission Act 2009 and the Anti Money Laundering and Anti-Terrorism Financing Act 2001 (as it was known at the time).[18] [19] The Cabinet believed that this would significantly increase the prospects of prosecuting criminal groups and rogue enforcement officials, ultimately leading to a substantial reduction in corruption-related crimes. Furthermore, the severe punishment advanced by Cabinet was intended to deter public officials from communicating with and receiving bribes from criminals.

Thus, to summarise, the stated objectives of introducing s. 203A were:

- To combat organised crime (and, by extension, corruption) by criminalising communication between enforcement officers and criminals;
- To safeguard national security by reducing leakage of information, which mirrors the ethos of the Official Secrets Act 1972; and
- To uphold proper administration of justice and maintaining public order through effective prosecution of crimes.[20]

[18]. After the Anti-Money Laundering and Anti-Terrorism Financing (Amendment) Act 2014 was passed, the Act came to be known as the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001, as it is known today: see section 77 of the Anti-Money Laundering and Anti-Terrorism Financing (Amendment) Act 2014.

[19]. Hansard dated 22 October 2013, pages 59 and 62

[20]. Hansard dated 22 October 2013, page 59.

2.2 Opposition to the law

The introduction of the Penal Code (Amendment) Bill 2013 was not welcomed by stakeholders not aligned with the government. Despite concerns about the far-reaching implications of the provision, there was little time provided for constructive parliamentary debates. The Bill was rushed through for voting,[21] despite being vehemently criticised by Opposition MPs as being "poorly drafted" and amidst calls that it should be "withdrawn" for further careful deliberation.[22]

One of the most damning critics of s. 203A was then Padang Serai MP N. Surendran Nadarajah, who commented, amongst other things, that the ambiguity associated with the wide language used in drafting s. 203A would result in an entrenched culture of secrecy within the civil service, further stretching the legal reach of the OSA 1972.[23] Most importantly, he stressed that due to the lack of mitigating factors, s. 203A risked being abused by law enforcement agencies to obstruct (instead of advancing) the proper administration of justice and compromising the public's right to information.

This criticism was echoed by current Damansara MP Gobind Singh Deo, who stated that in the absence of mitigating factors such as a list clearly illustrating the circumstances in which s. 203A ought to apply, the purpose of the section is easily obscured. The result would be a deviation of its objective, from eliminating corruption and collusion between law enforcement agencies and criminal syndicates to instead silencing civil servants and potential whistleblowers. As he

[21]. The debates for s. 203A only took one day and it proceeded to Committee Stage and Third Reading within the same day – Hansard dated 22 October 2013. See also Syahredzan Johan's comments to The Star dated 4 November 2013: https://www.malaysianbar.org.my/article/news/legal-and-general-news/members-opinions/goodbye-to-whistleblowers.

[22]. Hansard dated 22 October 2013, page 68.

[23]. Hansard dated 21 October 2013, page 31.

described it, the law was one "which takes us ten steps backwards".[24]

However, the Minister disregarded these criticisms and justified the enactment of s. 203A on the basis that there was a "compelling and immediate need to uphold national security" – a bare assertion which was not substantiated through empirical data or statistics.[25] She further stated that the better option is to "enact s. 203A first and amend it later in the future."[26] It is notable that there have been no amendments since its legislation.

When addressing the concerns of MPs regarding the potential conflict between s. 203A and the WPA 2010, the Minister stated that the enactment of s. 203A would ensure all disclosures of information involving corruption are made to relevant law enforcement agencies tasked to investigate the disclosed matters, and no one else. She said it is only reasonable for those who make disclosures through proper channels to enjoy the legal protection provided by the WPA 2010.[27]

However, this statement does not reflect the legal and practical realities of whistleblowing. Whistleblowers often have to overcome difficult obstacles to be granted legal protection, such as making exclusive disclosures to relevant enforcement agencies,[28] and ensuring that there is cogent supporting evidence before making the disclo-

[24]. Hansard dated 21 October 2013, page 68-69.

[25]. Hansard dated 22 October 2013, page 59.

[26]. Ibid.

[27]. Hansard dated 22 October 2013, page 64.

[28]. Section 6(1) of the Whistleblower Protection Act 2010, as interpreted by the Court of Appeal's decision in *Rokiah bt Mhd Noor v Menteri Perdagangan Dalam Negeri Koperasi & Kepenggunaan Malaysia* [2016] MLJU 1765.

sure.[29] It also ignores the fact that enforcement agencies have no discretion at all in deciding whether to revoke whistleblower protection if any one of the circumstances laid out by s. 11(1)(a) – (f) of the WPA 2010 is present.[30]

Outside of Parliament, activists also strongly opposed the legislation of s. 203A. Lawyers for Liberty described s. 203A as akin to "North Korean" laws and a "license for corruption cover-up" by the government.[31] Current Bangi MP, Syahredzan Johan, speaking to The Star on behalf of the Malaysian Bar Council, highlighted that the proposed section "would mean that no civil servant can ever be accorded protection under the WPA 2010, even if he/she made disclosure pursuant to the Act".[32] ARTICLE 19 stated that s. 203A severely undermines the public's freedom of expression under Article 10 of the Federal Constitution and the public's right to information.[33]

[29]. The High Court in *Rokiah bt Mhd Noor v Menteri Perdagangan Dalam Negeri Koperasi & Kepenggunaan Malaysia* [2015] MLJU 238 held that disclosures based on the reasonable belief of the whistleblower does not automatically entitle them to legal protections under the WPA 2010; the whistleblower must produce cogent evidence to the enforcement agencies to substantiate the disclosure. C4 Center argues that this interpretation is erroneous because it is contrary to the essence of s. 6(1) WPA 2010. The effect of this interpretation is to set an impossible standard for whistleblowing. See C4 Center, *Gaps in the Act: A Legal Analysis of Malaysia's Current Whistleblower Laws*, page 16-17.

[30]. Section 11(1) of the WPA 2010 uses the word "shall", which generally creates a legal obligation and leaves no room for discretion.

[31]. Hansard dated 22 October 2013, page 59.

[32]. Malaysian Bar, *Goodbye to* whistleblowers, November 4, 2013: https://www.malaysianbar.org.my/article/news/legal-and-general-news/members-opinions/goodbye-to-whistleblowers

[33]. ARTICLE 19, *Malaysia: Repeal Section 203A of the Penal Code*, February 16, 2015: https://www.article19.org/resources/malaysia-repeal-section-203a-penal-code/

2.3 Passing of the law

Despite the fierce opposition to the law, on 22 October 2014, the Penal Code (Amendment) Bill 2013 – including s. 203A – was passed by Parliament.

The amendment was legislated just four years after the WPA 2010 came into force. As will be discussed in the next chapter, the section essentially rendered the protections under the WPA 2010 inaccessible to public officials wanting to expose corruption by sharing information to enforcement agencies. S. 203A took away the most powerful "proper channel" available to public officials to fight corruption.

A key reflection is that the attitude of the government and the timing of the amendment cast serious doubts as to the true intent of the law. Firstly, despite opposition MPs and public leaders raising critical concerns with the law – many of which have now come true – the government response was dismissive and the issues were left unaddressed. Secondly, in the drafting of the law, it is highly unlikely that the detrimental effect of the provision on the WPA 2010 was not known. This was, after all, a law intending to combat corruption, and the government would necessarily have considered the wider implications for the anti-corruption framework.

Most notably, the section was tabled by the Najib Razak administration at a time when several high-profile controversies were causing public furore. These include the alleged abuse of BERNAS's dominant position in the rice industry[34] and criminal proceedings in France involving the Scorpene submarine scandal.[35] Importantly, these corruption scandals involved major public figures, including

[34]. Malaysia Today, November 13 2013: https://www.malaysia-today.net/2013/11/13/the-bernas-story-revisited/. See also The Edge dated 28 September 2023: https://theedgemalaysia.com/node/683067.

[35]. Malaysiakini, 23 July 2017: https://www.malaysiakini.com/news/389497.

Najib Razak himself.

Against this context, it is difficult not to view the section, with all its consequent effects, as anything but the introduction of yet another draconian law to quell dissent and silence opposition. As will be discussed in the next sections, this is primarily how the law has been used since its introduction.

CHAPTER THREE

Weaknesses of S. 203A of the Penal Code

This chapter discusses two major issues with s. 203A – how it limits access to whistleblower protection, and how the ambiguous wording of the section enables misuse of the law.

For ease of reference, s. 203A of the Penal Code reads as follows:

S. 203A: Disclosure of information

(1) ***Whoever discloses any information*** *or matter which has been* ***obtained by him in the performance of his duties or the exercise of his functions under any written law shall be punished*** *with* ***fine*** *of* ***not more than one million ringgit****,* ***or*** *with* ***imprisonment*** *for a term* ***which may extend to one year****,* ***or*** *with* ***both****.*

(2) ***Whoever has any information*** *or matter* ***which to his knowledge has been disclosed in contravention of subsection (1) who discloses that information*** *or matter* ***to any other person shall be punished*** *with* ***fine*** *of* ***not more than one million ringgit****, or with* ***imprisonment*** *for a term* ***which may extend to one year****, or with both.*

3.1 S. 203A severely limits access to whistleblower protection

The WPA 2010 stands as the governing legislation for whistleblower protection in Malaysia. The Act confers three types of protection to a whistleblower, namely:

a. Protection of confidential information;
b. Immunity from civil and criminal action; and
c. Protection against detrimental action.

To obtain these protections, an individual must make a disclosure of "improper conduct" to an enforcement agency. Improper conduct refers to any conduct which, if proven, would constitute a disciplinary or criminal offence. Generally, an enforcement agency is a Federal or State body that has both investigation and enforcement powers. This includes the Royal Malaysian Police, the Malaysian Anti-Corruption Commission, and the Immigration Department, among others.

Notably, protection is only afforded if the disclosure is not specifically prohibited by any written law. It is here that s. 203A has the most detrimental effect on whistleblowing in Malaysia.

S. 203A(1) prohibits disclosure of any information obtained in the performance of an individual's duties or functions under any written law. This brings the section into direct conflict with the WPA 2010. As a result, an individual will not receive whistleblower protection under the law if they disclose information obtained in the course of performing their legal duties. Even worse, such disclosure – even to an enforcement agency – would be considered an offence and the individual could be prosecuted instead.

S. 203A(2) extends criminal liability to an individual who discloses such information to other persons if they knew that the information was disclosed in a manner which contravenes s. 203A(1). This subsection prohibits any third parties, such as the media and the public, from disseminating the information received from an individual whom they know was obtained in the performance of his/her legal duties. Consequently, s. 203A(2) ensures that even those who receive information from first-hand parties – those caught under s. 203A(1) – are not entitled to whistleblower protection, should they disclose such information to an enforcement agency.

3.2 How ambiguities of s. 203A enable its misuse

Even beyond the severely limiting effect that s. 203A has on obtaining whistleblower protection, it is also problematic as a standalone section. Laws must be precisely elaborated and clear enough for an individual to regulate their behaviours in accordance with that law – this is especially crucial for laws that restrict fundamental liberties. However, as will be elaborated below, s. 203A is worded so ambiguously that it leads to absurdities and enables its misuse.

For any criminal matter, in order to find the accused guilty of the offence charged against him, the prosecution must prove, beyond reasonable doubt, everything in issue of the case, namely: the identity of the accused, the nature of the act (*actus reus*), and criminal intent (*mens rea*). The prosecution must also rebut any defence available to the accused.[36] Against this context, there are several ambiguities in the wording of s. 203A which lead to detrimental effects:

- Wide *actus reus* that leads to a near limitless scope of application
- No definition of "disclosure"

[36]. *Public Prosecutor v Ang An An* [1970] 1 MLJ 217, per Raja Azlan Shah J at 219.

- No definition of "information"
- No clear threshold for criminal liability
- The insertion of s. 203A into Chapter XI of the Penal Code

3.2.1 Near limitless scope of application

From a plain reading of the section, it is difficult to discern which class of people this section seeks to regulate, especially as there are no statutory exceptions, explanations, and illustrations for guidance.

The words "**Whoever** discloses any information or matter which has been obtained by him **in the performance of his duties or the exercise of his functions under any written law**" in s. 203A(1) do not appear to restrict the offence to public servants *per se*. It is arguable that this section also covers officers of private bodies, so long as they obtained such information in the performance of their duties or exercise of their functions under a written law. However, this leads to a broad scope of application that far exceeds the stated intent of the legislation. For example, could it be argued that a director of a company has contravened s. 203A(1) if he disclosed information which he obtained in the exercise of his duties under the Companies Act 2016?

On the other hand, s. 203A(2) is focused on those who disseminate such information knowing that its disclosure was unauthorised. This is not necessarily limited to public servants only and is wide enough to include journalists, the general public and private sector employees. In its plain and ordinary meaning, s. 203A(2) could literally punish anyone who knowingly shares information obtained in the performance of one's legal duties.

3.2.2 No definition of "disclosure"

The provision is silent on what amounts to "disclosure". Essentially, the omission of a statutory definition makes the law blind to the purpose of the disclosure, enabling s. 203A to impose criminal liability on any individual who discloses information obtained in the performance of his legal duties without reference to the context in which the disclosure was made. The section makes no practical distinction between an innocent whistleblower who makes reasonable disclosures to expose corruption and a rogue enforcement officer who, in return of a bribe, leaks information to help criminal syndicates from being caught. For instance, if a public servant in one Ministry obtains information in the performance of his duties, and communicates that information to his immediate superior, would he have committed an offence? Who is deserving of prosecution under s. 203A ultimately depends on the interpretation and implementation of relevant law enforcement agencies.

3.2.3 No definition of "information"

S. 203A does not define the term "information". Without any legal clarification, it would be appear that the section considers all possible forms of information as prohibited from disclosure. Again, this near limitless scope could lead to absurdities in application. Would this cover a situation where a public servant discloses information about the people they work with, such as their names?

Upon closer inspection, it appears that s. 203A complements the extensive scope of the OSA 1972 in preventing public access to government information. The OSA 1972 sets out a certification process which classifies certain information as "official secrets":

> ... ***any document specified in the Schedule*** *and any information and*

material relating thereto ***and includes any other official document, information and material as may be classified as "Top Secret", "Secret", "Confidential" or "Restricted"****, as the case may be,* ***by a Minister****, the Menteri Besar or Chief Minister of a State or such public officer appointed under section 2B.*[37]

Moreover, the Schedule to the OSA 1972 provides for three categories of documents that are automatically deemed "official secrets":

1. Cabinet documents, records of decisions and deliberations.
2. State Executive Council documents, records of decisions and deliberations.
3. Documents concerning national security, defence and international relations.

Any person who wrongfully communicates information classified as "official secrets" to any unauthorised person will be liable for an offence under s. 8(1) of the OSA 1972. While the application of OSA 1972 is still broad,[38] there is a theoretical limit to its application by virtue of the classification framework under the statute.

In contrast, s. 203A does not have a proper legal framework to regulate its enforcement. The immediate consequence is that s. 203A effectively extends the repressive application of OSA 1972 far beyond classified "official information" to any information obtained during the performance of one's legal duties. In other words, s. 203A appears to fill in the theoretical gaps of the OSA 1972 by censuring the disclo-

[37]. Section 2 of the OSA 1972.

[38]. Section 2A of the OSA 1972 expressly confers power to the Minister to add, delete and amend the Schedule by order published in the Gazette. Furthermore, section 30A of the same Act allows the Minister to prescribe the manner of classifying information, documents and other material as "official secrets". Exercise of executive discretion on matters of national security and public policy are generally not reviewable by the judiciary due to the concept of separation of powers. See Council for Civil Service Unions v Minister for the Civil Service (The GCHQ case) [1985] AC 374.

sure of any information that falls outside the ambit of s. 2 of the OSA 1972 read together with its Schedule, so long as it is obtained in the performance of one's legal duties.

This potentially entrenches the culture of secrecy and subservience not only within the civil service, but also private sector entities that perform public functions, such as government-linked companies (GLCs), government-linked investment companies (GLICs) and statutory bodies like the Ministry of Finance Incorporated (MOF Inc.). This is particularly significant when viewed against the backdrop of the intricate nexus between business and Malaysian politics and the numerous corruption scandals involving GLCs and GLICs.[39] The ecosystem of GLCs and GLICs has long been abused by politicians as a tool for money politics and patronage, especially through appointments to lucrative leadership positions in exchange for political loyalty.[40] The conflict of interests within this sector pose huge corruption risks – unfortunately, whistleblowers in these high-risk GLCs and GLICs are similarly caught under the detrimental effects of s. 203A.

3.2.4 No clear threshold for *criminal liability*

Mens rea refers to the question of 'moral fault' or culpability on the part of the wrongdoer in committing the act in question, and this requires the fact-finder (i.e. the judge) to examine the mental state of the wrongdoer. It is a cardinal element of a criminal offence because it acts as a filter to sieve out innocent individuals from those who truly deserve to be punished under the relevant penal law. The

[39]. C4 Center, *State of Corruption: Power, Politics and Policies in Malaysia*, Part III – Business in Politics: Seeking Control of Malaysia's Political System.

[40]. C4 Center, *Conflict of Interest: Preventing Political Patronage and Corruption in Malaysia*, https://c4center.org/conflict-of-interest-preventing-political-patronage-and-corruption-in-malaysia/.

common types of *mens rea* are intention, recklessness, knowledge and negligence.

S. 203A(1) is silent on the standard and requirement of *mens rea*. The absence of *mens rea* means that there is no apparent legal constraint as to the scope of s. 203A. Thus, the message that s.203A(1) sends to the public is that any form of disclosure of information is prohibited and illegal. The act of disclosure alone is sufficient to attract criminal responsibility.

On the other hand, s. 203A(2) requires *mens rea*, that is, the subsequent discloser has "knowledge" that the information he discloses was obtained in contravention of s. 203A(1) i.e. in the performance of one's legal duties. S. 203A(2) is however silent as to the standard of the *mens rea* required, thus creating more confusion and ambiguity as to its application. Knowledge in the case of s. 203A(2) can be: (1) subjective (whether the accused actually knows), (2) objective (whether the accused ought to have known), or (3) partially subjective and objective (whether a reasonable person in the accused's position would have known). The distinction between these standards may be technical, but the consequences are drastic, as it effectively decides the scope of criminal liability and the class of persons who will eventually be found guilty under s. 203A(2).

3.2.5 The insertion of s. 203A into Chapter XI of the Penal Code

The peculiar insertion of s. 203A into Chapter XI of the Penal Code (Chapter XI) – titled "False Evidence and Offences against Public Justice" – contradicts the Cabinet's purported intent. According to the then Minister, the rationale of inserting s. 203A in Chapter XI, particularly in between sections 203[41] and 204,[42] is because improper communication of information to criminals is *equivalent* (in terms of blameworthiness) to giving false evidence or obstructing judicial process, hence a true threat to public justice.[43]

Regrettably, s. 203A has no direct correlation or relevance with ss. 203-204 and Chapter XI as a whole. The act of enforcement officials leaking information to criminals differs significantly from giving false information in court (s. 203) or destroying documentary evidence (s. 204). It is difficult to reconcile the assertion that the disclosure of information constitutes an offence involving "false evidence" or one that is "against public justice". It is important to recall that s. 203A was introduced to combat organised crime by criminalising communications between public officials and criminal syndicates. Placing s. 203A within Chapter XI only emphasises its ambiguity, disconnecting it from its stated role in safeguarding national security and maintaining confidence in public administration.

[41]. Giving false information respecting an offence committed.

[42]. Destruction of document to prevent its production as evidence.

[43]. Hansard dated 22 October 2013, page 103.

3.3 Practical concerns in applying s. 203A

3.3.1 Openness to political abuse and arbitrary application

A major concern with the vagueness of s. 203A is the potential lack of prosecutorial fairness under this provision. The application of this law is further complicated by the lack of separation between the offices of the Attorney-General (AG) and the Public Prosecutor (PP).[44]

In addressing the concerns of the opposition MPs as to the disproportionate nature of s. 203A, the then Minister defended the Cabinet's decision by asserting the responsibility of the PP and the judiciary to exercise "maximum valuation" in a criminal proceeding.[45] This involves a careful assessment of the intent behind disclosure of information and all the available evidence, ensuring punishment only for deserving individuals.[46] In doing so, she reiterated that the PP and the judiciary are duty-bound to consider essential factors such as the imperative to uphold public justice, safeguard the integrity of the criminal justice system, national security reasons and the country's commitment in tackling corruption.

However, the concerns raised continue to be justifiable. The primary function of the office of the AG is to advise the government on legal matters,[47] whereas a major power of the office of the PP is the discretion to institute, conduct or discontinue any proceedings for an offence.[48] The fact that both roles are held by a single individual

[44]. Article 145(3) of the Federal Constitution read together with section 376(1) of the Criminal Procedure Code, which states that "*The Attorney-General shall be the Public Prosecutor…*"

[45]. Hansard dated 22 October 2013 at page 103.

[46]. Ibid.

[47]. Art. 145(2) of the Federal Constitution.

[48]. Art. 145(3) of the Federal Constitution.

means that the AG/PP cannot be free from political influence – this is especially so as the AG/PP is appointed by the Yang di-Pertuan Agong on the binding advice of the Prime Minister.[49] Consequently, offence-creating laws with broad scopes – such as s. 203A – are highly susceptible to abuse by governments, especially when the AG/PP generally cannot be held accountable for the exercise of his/her powers.[50]

The vague and broad character of s. 203A enables the AG/PP to suppress dissent among 'disloyal' public servants by instituting criminal proceedings at their discretion. Ultimately, this renders the stated anti-corruption objectives of the section illusory and unattainable, as s. 203A can be utilised to penalise genuine whistleblowers who pose a threat to the government of the day.

An example of a similar law abused despite government assurances is the now-repealed Internal Security Act 1960 (ISA 1960). During Parliamentary debates, Tun Abdul Razak emphasised[51] that the ISA 1960 was not intended to be used against political members.[52] Despite this, the ISA 1960 famously became one of the government's most draconian weapons, used numerous times against politicians, journalists, and activists until its repeal in 2012. One of the most controversial uses of the ISA 1960 was the 1987 "Operation Lalang" – the second largest mass arrest in Malaysian history following the May 13

[49]. Art. 145(1) read with Art. 40(1A) of the Federal Constitution.

[50]. *Karpal Singh & Anor v Public Prosecutor* [1991] 2 MLJ 544; *Johnson Tan Han Seng v Public Prosecutor* [1977] 2 MLJ 66; *Long bin Samat v Public Prosecutor* [1974] 2 MLJ 152; but very recently, the Federal Court confirmed that the AG/PP's discretion is amenable to judicial review under very exceptional circumstances, see *Sundra Rajoo Nadarajah v Menteri Luar Negeri, Malaysia & Ors* [2021] 6 CLJ 199.

[51]. Dewan Rakyat Parliamentary Debates dated 22 June 1960: https://www.parlimen.gov.my/files/hindex/pdf/DR-22061960.pdf

[52]. The original draftsman of ISA 1960 commented in his book: ".... I must hope that the practice of imprisonment without trial, charge or conviction admitted by the Act 1960 will not be regarded as a permanent feature of the legal and political landscape of Malaya or for that matter of Asia generally." See Hickling, H. (1983). *The First Five Years of the Federation of Malaya Constitution.* Mal. L.R, 183.

riots in 1969. Under the alleged justification of preventing racial riots, the police arrested 106 to 119 people under s. 73 of the ISA 1960, including prominent opposition leaders Lim Kit Siang and Karpal Singh, social activists like SUARAM's advisor, Kua Kia Soong, intellectuals, and university students.[53]

3.3.2 The judiciary cannot remedy an intrinsically defective s. 203A

During parliamentary debates on the section, the Minister sidelined concerns by expressing confidence in the judiciary's ability do justice in every case, and that the judiciary would be capable of mitigating all of the potential concerns associated with s. 203A in line with established judicial principles.

Even if there were to be genuine cases of prosecution under s. 203A, the inherent ambiguity would likely require judicial interpretation to resolve. While courts often apply a purposive approach to interpreting legislation, this method is not always straightforward. In many cases, courts have declined to read additional words into a legislation as that would be considered encroaching upon the legislative powers of Parliament.

This underscores a fundamental challenge in statutory interpretation: the balance between separation of powers and judicial deference. The purposive approach – in which the courts consider the purpose of a provision instead of only relying on its literal meaning - only applies where there are doubts or ambiguities on the terms or words employed by the Legislature. Indeed, the general rule is that where the words are precise and unambiguous, the literal rule of

[53]. Kua Kia Soong's letter to Free Malaysia Today, '*34 years after Ops Lalang, still no sincere apology by Dr M*', dated 27 October 2021: https://www.freemalaysiatoday.com/category/opinion/2021/10/27/34-years-after-ops-lalang-still-no-sincere-apology-by-dr-m/

construction should be adopted. If Parliament's intention is clearly embodied through the language used in the statute, the court has a duty to enforce its plain meaning even if it is "inconvenient, impolite or improbable".[54]

In fact, the Federal Court has restricted the use of Hansards in statutory interpretation to situations where the literal construction of the statute would lead to an "absurdity".[55] What constitutes an absurdity is ultimately an open-ended question, which varies differently according to the views and attitudes of the particular bench hearing the case.[56] This element of unpredictability creates another layer of ambiguity laden in s. 203A, further strengthening the claim that s. 203A is disproportionate in meeting its intended legislative objective.

Moreover, the fact that there are still no reported case judgments in the past ten years of its enactment to provide clarity on the interpretation of s. 203A only proves the same. The Minister's argument that the judiciary would be relied upon to resolve the section's well-known flaws and dangers was irresponsible as an elected lawmaker, as the judiciary cannot be expected to inject clarity into an inherently unclear statutory provision on a case-to-case basis.

[54]. Manokaram a/l Subramaniam v Ranjit Kaur a/p Nata Singh [2009] 1 MLJ 21.

[55]. Chin Choy & Ors v Collector of Stamp Duties [1979] 1 MLJ 69.

[56]. Noor 'Ashikin binti Hamid' and Rusniah Ahmad, Judicial Interpretation: A Conceptual Analysis, Proceedings of International Conference on Public Policy and Social Science, UiTM Melaka Malaysia, November 2012.

CHAPTER FOUR

Comparisons with Other Jurisdictions

Numerous jurisdictions have also enacted laws prohibiting disclosure of information obtained in the performance of legal duties or functions. However, in contrast with s. 203A, these laws provide comprehensive guidelines, thorough explanations, and well-defined exceptions serving to clearly delineate the legal limitations on disclosing information. Upon examining these laws, certain features have been identified as follows. Disclosure of information is restricted to very specific situations where:

1. The offender is strictly a public official.
2. The offender must disclose information either in the execution of his/her public duties or the information disclosed must be obtained in the capacity of a public official.
3. There is a serious breach of public trust by the public official, or

the conduct is beyond acceptable standards of conduct.

4. The disclosure must be prejudicial to social order, public safety, and national security.
5. There is a clear distinction between permissible and impermissible disclosure.
6. There is a legitimate attempt to strike a fair balance between upholding freedom of information and protecting public interest considerations in providing robust defences and exceptions.

4.1 United Kingdom

4.1.1 Misconduct in Public Office

In the UK, there is no statute or written law prohibiting the disclosure of information obtained in the performance of one's legal duties or functions. Instead, a common law offence exists derived from the development of case law. The common law offence of misconduct in public office regulates wrongful or improper communication by public officials to others. This ancient common law offence has a broad scope which encompasses a diverse range of conducts that are 'calculated to injure public interest so as to call for condemnation and punishment'.[57]

In *Attorney General's Reference No. 3 of 2003*,[58] the Court of Appeal stated that there are 4 essential elements to this offence:

1. The suspect must be a public official acting as such i.e. in the discharge of duties of the office;[59]
2. They must have wilfully breached their public duties;

[57]. *R v Dytham* [1979] 1 QB 723, as per Lord Widgery CJ. His Lordship has noted that this includes, but not limited to, acts of dishonesty and corruption.

[58]. [2004] EWCA Crim 868, para 54-64.

[59]. *R v Collins; R v Lewis and another* [2022] EWCA Crim 742.

3. The breach must have been such a serious departure from acceptable standards as to constitute a criminal offence; and to such a degree as to amount to an abuse of the public's trust in the public official;[60] and
4. There must have been no reasonable excuse or justification.

4.1.2 Crown Prosecution Service guidelines

The guideline issued by the Crown Prosecution Service (CPS) on this common law offence is important to note.[61] The CPS states that it is generally prohibited for public servants to misuse their privileged access to confidential information and subsequently disclose them to the media without justifiable reason. Moreover, the scope of criminality extends to journalists who publish such privileged information.

The rationale behind the common law offence lies in the paramount public interest of upholding the integrity and incorruptibility of public officer holders, especially those serving in enforcement and investigative agencies. It is imperative that public officials refrain from compromising public interest by divulging information in exchange for payments or any other improper considerations. Such actions are a fundamental breach of their duty of loyalty and undermines the trust relationship between the civil servants and the country. Public officials are cognisant of the sensitive nature of information they have obtained in the performance of their functions and should recognise the critical importance of maintaining public

[60]. The misconduct normally would normally have to amount to an affront to the standing of the public office held which fell so far below the standards accepted as to amount to an abuse of the public's trust in the office holder: *R v Dytham* [1979] 1 QB 723.

[61]. CPS, *Media: Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists*. https://www.cps.gov.uk/legal-guidance/media-prosecuting-cases-where-public-servants-have-disclosed-confidential

confidence.

However, the CPS strongly emphasises that UK citizens have the right to access information under Article 10 of the European Convention of Human Rights.[62] It is for the court to meticulously analyse the merits and facts of each case, engaging judiciously in the balancing act between conflicting public interests and the proportionality of legitimate aims. Furthermore, the CPS emphasised that not all misconduct will be caught by the common law offence. Prosecution is only for conducts of serious nature, and severity must be determined through close examination of the following factors:

1. The need for maintenance of public standard and confidence in the public office;
2. The disclosure of information must have caused harm to public interest to attract culpability;[63]
3. Severity of the harm caused to public interest must be considered in relation to the responsibility of the public officer and its office-holder, the importance of public objects they serve and the nature and extent of the departure from those responsibilities;[64]
4. The test of evaluating of harm to public interest is objective and cannot be considered in 'a vacuum'.[65]

[62]. This Article provides for the freedom of expression. The ECHR is incorporated into UK law through section 2 of the Human Rights Act 1998.

[63]. *R v Chapman and others; R v Sabey* [2016] 1 All ER 1065.

[64]. *Shum Kwok Sher v Hong Kong Special Administrative Region* [2002] 5 HKCSAR 381, p.409 as per Sir Anthony Mason NPJ delivering the judgment for the Final Court of Appeal, referred by the UK Court of Appeal in *AG's Reference No.3 of 2003* [2004] EWCA Crim 868.

[65]. [2004] EWCA Crim 868, para 45 and 58-59.

4.1.3 Comparison with s. 203A

Similarly broad in scope

Both the common law offence and s. 203A exhibit extremely broad scopes: s. 203A can prohibit any information obtained while performing legal duties, whereas the common law offence can encompass any conduct done by a public official calculated to harm public interest. Similarly, prosecutions under the common law offence consist of a principal offender (i.e. the corrupt public official disclosing information) and the accomplice who aids and abets the principal offender.

Specific to Public Officials

When examining the differences, the common law offence distinctly pertains to the actions of public officials in the discharge of public duties. This important qualification is absent in s. 203A.

Clear Mens Rea

The common law offence clearly outlines the requisite mens rea, that is ‘wilfulness’ in breaching public duties, which is inherently subjective. Conversely, s. 203A lacks this explicit mens rea element and relies, at best, on presumptions established by case law.

Consideration of Public Interest

Under the common law offence, disclosure of information is punishable only if it is actually detrimental to public interest, judged against acceptable standards and the levels of public trust placed in the public official. This condition emphasises the importance of proportionality in pursuing the legitimate aim of safeguarding public interest. The common law offence seeks to condemn only serious misconduct that is objectively prejudicial to the public. This is drastically different from the wording of s. 203A, which lacks distinctions based on severity, sensitivity of the information disclosed or public interest considerations.

Existence of a legal defence

Finally, the common law offence offers a legal defence to any accused public officials, enabling them to exonerate themselves upon proving a reasonable excuse or justification for their disclosure. Again, there are no such defences for s. 203A, leaving no legal avenue for any accused persons to excuse a *bona fide* disclosure of information.

4.2 Canada

4.2.1 Canadian Foreign Interference and Security of Information Act 1985

The Canadian Foreign Interference and Security of Information Act 1985 (FISIA 1985) generally prohibits wrongful communication, use, reception, retention, and failure to take reasonable care of certain government information. At the outset, it is necessary to mention that in the case of *O'Neill et al v The Attorney General of Canada [O'Neill v Canada (Attorney General)]*,[66] the Supreme Court of Ontario declared sections 4(1)(a), 4(3) and 4(4)(b) of the FISIA 1985 unconstitu-

[66]. 82 OR (3d) 241, 82 OR (3d) 241.

tional on the grounds of being so vague that it endangers life, liberty, and security of a person contrary to section 7 of the Canadian Charter of Rights and Freedom. In other words, these subsections are legally unenforceable in Canada.[67]

Currently, even without the subsections that were struck down, the legal framework under section 4 of the FISIA 1985 continues to prohibit any wrongful communications of secret information for the purposes of prejudicing national interest and public safety of the Canadian people and government.[68]

Although sections 4(1)(a), 4(3) and 4(4)(b) of the FISIA 1985 are legally unenforceable in Canada, a discussion and comparison of the sections with s. 203A is still pertinent to illustrate that the presence of mitigating factors alone will not stamp out all the apparent dangers of a disproportionate law being used in harsh and oppressive ways. This strengthens the recommendation to repeal s. 203A altogether, which will be discussed in full in Chapter 6 below.

4.2.2 Comparison with s. 203A

Definition of Information

A major distinguishing feature of the FISIA 1985 from s. 203A is that it defines what qualifies as 'information'. Section 4 of the FISIA 1985 generally prohibits the disclosure of two types of confidential in-

[67]. The Attorney-General of Canada subsequently decided not to appeal against the decision, see: https://www.ourcommons.ca/DocumentViewer/en/39-1/SECU/report-7/response-8512-391-198?page=33. The subsequent amendments to the FISIA 1985 did not amend or repeal the subsections which were declared unconstitutional by the Canadian courts.

[68]. It is still an offence under s. 4(1)(b) – (d) FISIA 1985 to use secret information for the benefit of any foreign power in any other manner prejudicial to the safety or interests of the State. Additionally, it is an offence under s. 4(4)(a) of the FISIA 1985 for public officials to retain secret information without lawful authority to do so or fails to restore to the person of authority so as to endanger safety of the secret information in his possession.

formation:

1. Exhaustive category: any secret official code word, password, sketch, plan, model, article, note, or document.
2. Non-exhaustive category: any secret information that relates to, used or obtained in a prohibited place, obtained or accessed in the course of employment or holding of a public office under the Canadian Government.

Types of Punishable Disclosures

Another difference from s. 203A is that not all disclosures of information are punishable under s. 4(1) FISIA 1985. It is only an offence if the person who possesses or has control over any secret information commits one of the following acts:

1. Communicates the secret information to an unauthorised person or to whom it is not in the interest of the country to communicate with;
2. Uses the secret information they have possession over for the benefit of any foreign power or in a manner prejudicial to the safety or interests of the country;
3. Retains the secret information when they have no right, or it is contrary to their duty, to do so, or where it fails to comply entirely with all directions issued by a lawful authority directing the disposal or return of the secret information;
4. Fails to take reasonable care or acts in a way which endangers the safety of the secret information.

Section 4(1) of the FISIA 1985 specifically criminalises the unauthorised disclosure of confidential information where it is contrary or prejudicial to national interest. This provision provides a list of legal considerations for the Canadian judiciary to assess when determining the guilt of the discloser and the necessity of criminal prosecution. These considerations include public interest factors and national security concerns. Additionally, section 4(1) is to be read together with section 3(1) and (2) of the FISIA 1985, which exhaustively provides for the circumstances in which the purpose of disclosing secret information is prejudicial to the safety and interests of the State.[69] This is in stark contrast to s. 203A which gives no guidance to the law enforcement agencies, the judiciary and the AG/PP.

Existence of legal defences

Section 4(3) of the FISIA 1985 makes it an offence for any person who knows or ought to have known that by receiving any secret information, they are in breach of the FISIA 1985. Up to this point, s. 4(3) of the FISIA 1985 is similar to s. 203A(2). However, it is a complete defence for the recipient of secret information if they can prove that the communication was not voluntary. This defence is absent in s. 203A.

In addition, s. 4(4) of the FISIA 1985 makes it an offence for any person who retains secret information for the purposes of injuring national interests or public safety, without lawful authority or excuse, or unreasonably fails to restore the secret information to any authorised person or a police officer.

Notably, s. 4(4)(b) provides a defence to both the discloser and

[69]. This includes, *inter alia*, causing an urgent and critical situation in Canada that endangers lives, health and safety of Canadians or threatens the ability of the Government of Canada to preserve the sovereignty, security and territorial integrity of Canada, and interfering with a service or computer programme, whether public or private, or its operation in a manner that has a significant adverse impact on the health, safety, security or economic or financial well-being of the people of Canada or the functioning of any government in Canada.

recipient of any secret information. They may exonerate themselves from criminal liability if they are able to prove, on a balance of probabilities,[70] that they had no intention to cause harm to the State, had lawful excuse or valid reasons for retaining the secret information or not restoring the information to any competent law enforcement agencies. The burden then lies on the prosecution to disprove the defences raised beyond reasonable doubt[71] (a higher threshold than the balance of probabilities).

4.2.3 Judicial criticism of defences provided by FISIA 1985

Comparatively, s. 4 of the FISIA 1985 appears to be more robust than s. 203A in terms of providing mitigating factors such as proper legal defences to any accused persons, indicating an attempt by the Legislature to draw legitimate boundaries of its applicability. Even then, after a thorough and comprehensive analysis of the potential impacts, the Supreme Court of Ontario had criticised the adequacy of these provisions from a constitutional law perspective. Subsequently, the Canadian court deemed sections 4(1)(a), 4(3) and 4(4)(b) of the FISIA 1985 as unconstitutional on the basis that the inherent ambiguity of the sections constituted a real risk of draconian application by the Executive so as to encroach on the Canadian citizens' fundamental right to life, liberty, and security of persons.

Here are some of the salient points made by the Supreme Court of Ontario which are all directly relevant to the legality of s. 203A:[72]

1. The sections were 'standardless', giving the State 'unfettered

[70]. In simpler terms, that it is more probable than not. But if it is of equal probability, then the standard of proof is not satisfied.

[71]. This requires the prosecution to bring enough evidence for the court to believe, without uncertainty, that something is true or untrue.

[72]. Ibid, para 39, 59 and 70-71.

ability to arbitrary protect whatever information it chooses to classify as secret information or unauthorised disclosure' allowing the State to punish anyone who fall within the scope of FISIA 1985, whether or not they are bound by any governmental policies or codes of conduct;

2. The sections endanger the rights of 'those outside the government who are in receipt of government information', punishing them regardless of the circumstances. It does not draw appropriate distinction between those who receive the secret information deliberately and inadvertently, nor pay any regard as to whether the disclosure of the information actually harms national interest;
3. The FISIA 1985 does not provide 'any guidance to the public as to what amounts to the prohibited conduct prescribed by these sections', depriving them the fair opportunity to 'make a considered evaluation of whether their conduct is likely to be criminal or not';
4. It is 'too late' for the Legislature to expect the prosecution or the judiciary to clarify the vagueness and ambiguity revolving the impugned sections of the FISIA 1985, and 'judicious use of prosecutorial discretion cannot cure constitutionally overbroad legislation';
5. The impugned sections provide 'no guidance to law enforcement officials' on whether a crime has been committed, and consequently there are 'no controls on the exercise of their discretion and there is the danger of arbitrary and ad hoc law enforcement', violating the tenet of rule of law.

These judicial pronouncements bear significant relevance to the assertions made by the former Law Minister during debates surrounding the enactment of s. 203A. Analogously, they persuasively expose the weaknesses and draconian implications of s. 203A. If the comparatively more favourable law (s. 4 of the FISIA 1985) was struck down by the Canadian courts for being disproportionate and unjustifiable, there arises a genuine and serious concern regarding the possibility of s. 203A infringing upon Article 5 of the Federal Constitution. It also cast doubts on the effectiveness of recommendations to amend s. 203A by introducing mitigating factors to restrict its application, as opposed to completely repealing the section.

4.3 Australia

4.3.1 S. 122.4 Australian Criminal Code Act 1995

S. 122.4 of the Australian Criminal Code Act 1995 (CCA 1995) prohibits unauthorised disclosure of information[73] by current or former Commonwealth officers[74] if all the following conditions are satisfied:

1. Communicates information obtained by reason of their holding the position of a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity;
2. They are bound by a duty not to disclose that information;[75] and
3. The duty arises under a law of the Commonwealth.

[73]. Section 90.1 of the CCA 1995 defines "Information" as information of any kind, whether true or false and whether in a material form or not, and includes:(a) an opinion; and (b) a report of a conversation.

[74]. Section 121.1 of the Australian Criminal Code Act 1995 defines a "Commonwealth officer" as (a) an Australian Public Service employee; (b) an individual appointed or employed by the Commonwealth otherwise than under the *Public Service Act 1999*; (c) a member of the Australian Defence Force; (d) a member or special member of the Australian Federal Police; (e) an officer or employee of a Commonwealth authority; (f) an individual who is a contracted service provider for a Commonwealth contract; (g) an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract.

[75]. For example, see Regulation 7 of the Australian Public Service Regulations 2023 read together with section 13(13) of the Australian Public Service Act 1999.

4.3.2 Comparison with s. 203A

Existence of a legal duty to not disclose information

The primary distinction with s. 122.4 of the CCA 1995 is the imposition of a legal duty upon the Commonwealth officer to not disclose information obtained while holding the Commonwealth office. This forms the prerequisite for determining guilt under this provision. Under s. 203A, the mere act of disclosing information obtained in the performance of any legal duty or function alone is sufficient to attract criminal liability. Put simply, s. 203A criminalises disclosure of information without first creating a duty not to do so in relation to the individual's legal function.

Disclosure of information to non-Commonwealth officers

Section 122.4A prohibits the act of communicating and dealing with information by non-Commonwealth officers i.e. those who are not current or former Commonwealth officers. It essentially mirrors section 122.4 with one additional condition of satisfying any one of the following factors:

1. The information communicated by a Commonwealth officer to non-Commonwealth officer must bear a security classification of secret or top secret;
2. The communication of the information damages the security or defence of Australia, interferes with or prejudices the administration of criminal justice, or harms or prejudices the health or safety of the Australian public.

The contrast of this section with s. 203A(2) is striking. Section

122.4A of the CCA 1995 exclusively punishes the recipient of classified information prejudicial to national security, administration of public justice and endangers public safety. This threshold indicates a legislative effort to strike a fair balance between protecting public interest and upholding Australian citizens' right to information. However, this is clearly absent in the language used in s. 203A.

Existence of statutory defences

Notably, section 122.5 of the CCA 1995 provides a list of defences for offences under sections 122.4 and 122.4A:

1. The information was done in accordance with powers, functions, and duties in a public officer's lawful capacity;
2. The information communicated is already public at the material time or has been previously communicated;
3. The information is communicated to an integrity agency, a competent court or tribunal, or to persons engaged in the business of reporting news;
4. The communication of information is permitted by the Public Interest Disclosure Act 2013 or the Freedom of Information Act 1982;
5. The information is communicated for the purposes of reporting any offence or maladministration;
6. The information communicated relates to a person.

The defences available under Australian criminal legislation are notable examples of how disclosure can be permitted where public interest considerations are involved. S. 122.5 confines restrictions on disclosure of information to circumstances of strict necessity. As has been discussed, this is not the case under s. 203A.

4.4 New Zealand

4.4.1 S. 78A(1) New Zealand Crimes Act 1961

S. 78A(1) of the New Zealand Crimes Act 1961 (CA 1961) prohibits wrongful communication, retention or copying of official information.[76] It makes it an offence for a person who owes allegiance to the New Zealand Government (i.e. public or statutory officer) if they commit any of the following:

1. Knowingly or recklessly, and **with knowledge that they are acting without lawful authority**, communicate any official information to any other person knowing that doing so is prejudicial to the security or defence of New Zealand;
2. Retains or copies any official document **with the intent of prejudicing the security or defence of New Zealand with knowledge** that **retention or replication is without lawful authority**, the official document is related to the security or defence of New Zealand and that undisclosed disclosure thereof is likely to be prejudicial to the security or defence of New Zealand; or
3. Knowingly fails to comply with any directions ordered by a lawful authority for the return of any official document which is in their possession, the official document is related to the security or defence of New Zealand and that undisclosed disclosure thereof is

[76]. Section 78A(2) defines "official information" as (a) means any information held by — (i) a department; or (ii) a Minister of the Crown in his or her official capacity; or (iii) an organisation; or (iv) an officer or employee of any department or organisation in his or her capacity as such an officer or employee or in his or her capacity as a statutory officer; or (v) an independent contractor engaged by any department or Minister of the Crown or organisation in his or her capacity as such contractor; and (b) includes any information held outside New Zealand by any branch or post of (i) a department; or (ii) an organisation; and (c) includes any information held by an unincorporated body (being a board, council, committee, subcommittee, or other body) (i) which is established for the purpose of assisting or advising, or performing functions connected with, any department or Minister of the Crown or organisation; and (ii) which is so established in accordance with the provisions of any enactment or by any department or Minister of the Crown or organization.

likely to be prejudicial to the security or defence of New Zealand.

4.4.2 Comparison with s. 203A

Consistent with the legal frameworks discussed above, the objectives of s. 78A(1) of the CA 1961 are clearly defined. **Firstly**, this provision is limited to public or statutory officers working for the New Zealand Government. **Secondly**, the disclosure of the official information must be intentional in causing prejudice to national security. **Thirdly**, any use, retention or release of the official information must be done without proper or lawful authority. **Fourthly**, the official information must relate to national security.

Although relatively shorter and less complex than other laws prohibiting disclosure of information, the language of s. 78A(1) of the CA 1961 is clear enough to inform governmental and non-governmental persons on whether their conduct of disclosing certain information is criminal or not. The language used in this section is straightforward, allowing laypersons to easily comprehend the prescribed standard of conduct set by the Legislature. Further, the provision clearly outlines the requisite *mens rea* (in bold above for emphasis), which is absent in s. 203A.

4.5 Singapore

4.5.1 S. 7 Public Sector (Governance) Act 2018

S. 7(1) of the Public Sector (Governance) Act 2018 (PSGA 2018) prohibits unauthorised disclosure by making it an offence if an individual:

1. Discloses or causes to be disclosed any information[77] under the control of a Singaporean public sector agency to another person;
2. The disclosure is not authorised by any data sharing direction issued to the Singaporean public sector agency;
3. Is a relevant public official of the Singaporean public sector agency; and
4. Either knows that the disclosure is unauthorised or is reckless as to whether the disclosure is authorised.

Section 7(3) PSGA 2018 prohibits improper use of information by making it an offence if an individual:

1. Makes use of the information under the control of a Singaporean public sector agency;
2. The use is not authorised by any data sharing direction issued to the Singaporean public sector agency;
3. Is, at the material time, a relevant public official in the Singaporean public sector agency;
4. Knows that the disclosure is unauthorised or is reckless as to whether the disclosure is authorised.
5. As a result of the disclosure, obtains a gain for themselves or any other person, or causes harm to another individual or person.

S. 7(2) and (5) respectively provide defences to s.7(1) and (3) if the offender is able to prove, on a balance of probabilities, either one of the following conditions:

1. The information under control of the Singaporean public agency at the material time is generally accessible or available; or

[77]. Section 2 of the PSGA 2018 defines "Information" as to include (a) any facts, statistics, instructions, concepts or other data in a form that is capable of being communicated, analysed or processed (whether by an individual or a computer or other automated methods); and (b) data sets.

2. The disclosure of the information was permitted by any other written law, a court order or in any other circumstances which disclosure is prescribed.

4.5.2 Comparison with s. 203A

This is another relatively straightforward and simple legal framework providing general prohibition against unauthorised disclosure or improper use of official information, yet providing applicable defences to offenders if the disclosure is legally permissible or *bona fide* in nature. Sections 7(1) and (3) are specifically aimed at Singaporean public officials, the disclosure must be unauthorised and the *mens rea* element must be recklessness or subjective intention.

4.6 Summary

The above comparisons reveal that in other similar jurisdictions, the prohibition on disclosure of information by public officials includes the following features:

1. The offender is strictly a public official.
2. The offender must disclose information either in the execution of his/her public duties or the information disclosed must be obtained in the capacity of a public official.
3. There is a serious breach of public trust by the public official or beyond acceptable standards of conduct.
4. The disclosure must be prejudicial to social order, public safety, and national security.
5. There is a clear distinction between permissible and impermissible disclosure.
6. There is a legitimate attempt to strike a fair balance between up-

holding freedom of information and protecting public interest considerations in providing robust defences and exceptions.

These features are critical in providing clarity to law enforcement agencies and potential whistleblowers. They demonstrate how, in other jurisdictions, there exists a legislative commitment to upholding the public's right to information against the backdrop of legitimate national security needs. However, as noted several times above, these aspects are absent from s. 203A.

It is also crucial to note that unlike Malaysia, countries discussed in this chapter did not enact laws prohibiting the disclosure of information by public servants in a vacuum. These laws were enacted (or later revised) within the wider context of laws that permit public interest disclosures, acting as mechanisms for public scrutiny to buttress open accountability in the civil service and government sector.[78] In other words, laws that restrict disclosures of information in these countries are not in conflict with laws that enable whistleblowing and access to government-held information; they exist in harmony to ensure that information on public interest matters are always openly accessible by the public, and prohibition should only be allowed in exceptional situations where there is a real legitimate threat to public safety and national interest (this will be discussed in depth in Chapter 6 below). This holistic approach and careful attention to context were absent in the then Minister's arguments and basis for introducing s. 203A in Parliament, and this is likely one of the contributing factors for the current state of confusion due to the overlap between

[78]. For example, in the UK, the legal framework under Official Secrets Act 1989 are complemented by the Freedom of Information Act 2000 and the Public Interest Disclosure Act 1998 which allows the public to make requests for information from the Government departments and protects whistleblowers who disclose information about malpractice at their workplace respectively: https://researchbriefings.files.parliament.uk/documents/CBP-7422/CBP-7422.pdf.

s. 203A and OSA 1972.

As argued, the lack of clarity and broad scope of s. 203A leave it open to misuse by government. The next chapter discusses several cases over the past decade which illustrate how this can take place.

	Malaysia	UK	Canada	Australia	New Zealand	Singapore
Law that prohibits disclosure of information obtained in the performance of legal duties/function	Penal Code, section 203A (s. 203A)	Common law offence of misconduct in public office.	Foreign Interference and Security of Information Act 1985 (FISIA 1985), section 4(1)(a), 4(3) and 4(4)(b). Note: these sections were declared unconstitutional and legally unenforceable by the Supreme Court of Ontario in O'Neill v Canada (Attorney General) [2006].	Criminal Code Act 1995 (CCA 1995), section 122.4 and 122.4A.	New Zealand Crimes Act 1961 (CA 1961), section 78A.	Public Sector (Governance) Act 2018 (PSGA 2018), section 7
What is the purpose of the law?	1. To fight organised crime. 2. To prevent collusion and communication between public officials and criminal syndicates.	1. To prevent public officials from misusing their privileged access to confidential information and disclosing them without justification. 2. To generally prohibit conducts calculated to injure public interests which are deserving of criminal punishment. 3. To uphold the integrity of public officeholders and to maintain trust and confidence in the civil service.	1. To address national security concerns. 2. To protect public safety by preventing harmful disclosure of official information. 3. To uphold Canada's sovereignty by protecting it from foreign interference.	1. Prohibit unauthorised disclosure of information which is inherently harmful to Australia's interests and safety. 2. Prohibit the disclosure of security classified information. 3. To modernise and replace its predecessor in order to address current environment of threats to national interest.	To protect the national interests and public safety of New Zealand by prohibiting the wrongful disclosure, retention and replication of official information obtained in the performance of legal duties.	1. To provide for a consistent governance framework across public bodies in Singapore and to support a whole of government approach to the delivery of services in the Singapore public sector. 2. To set a high standard of conduct for public official to maintain public trust and confidence in the Singaporean government and civil service.
Are parameters provided as to what 'information' entails?	No.	Yes. The information must have some element of confidentiality or privilege associated with it, and thus should not ordinarily be disclosed unless there are good reasons otherwise.	Yes. Section 4(1) FISIA 1985 provides that: 1. The information must have an element of secrecy. 2. It relates to or is used in prohibited places. 3. It is entrusted to him/her by the State because of his position in public office.	No for Commonwealth officers. Yes for non-Commonwealth officers. Section 122.4A CCA 1995 provides that: 1. The information must bear a security classification of secret or top secret. 2. The disclosure of the information is capable of injuring national interests or public safety.	Yes. Section 78A(2) of the CA 1961 defines "official information" as any information held by: 1. A department. 2. A Minister acting in his/her official capacity. 3. An officer, employee or organisation acting in the capacity of a public or statutory officer. 4. Independent contractor engaged by a Minister, public or statutory officer or an organisation acting on behalf of the New Zealand government.	Yes. Section 2 PSGA 2018 defines "information" to include: 1. Any facts, statistics, instructions, concepts or other data in a form that is capable of being communicated, analysed or processed (whether by an individual or a computer or other automated methods); and 2. Data sets.

	Malaysia	UK	Canada	Australia	New Zealand	Singapore
What is the impugned act i.e. actus reus?	Disclosure of any information obtained in the performance of one's legal duties/ functions.	1. There must be a public official discharging his/her public duties. 2. The breach is such a serious departure from acceptable standards and an abuse of public trust that it deserves criminal punishment. 3. There is no reasonable excuse or justification for the breach. 4. The test is objective, judged on reasonable standards expected of a similar officeholder.	For s. 4(1) FISIA 1985: 1. Communicating secret information to an unauthorised person. 2. Using the secret information to benefit any foreign power or in a prejudicial manner to the country's safety and interest. 3. Retains the secret information without lawful authority, and fails to comply with any directions to return or dispose the information. 4. Failed to take reasonable care in handling the secret information so as to endanger its safety. For s.4(3) FISIA 1985, it is an offence if any person is committing an offence if he/ she receives secret information knowing or ought to have known that he/she had no lawful authority in doing so. For s.4(4) FISIA 1985, it is an offence to retain and use secret information so as to endanger national interests and public safety, and failing to surrender the information to the police or authorised officer.	For s. 122.4 CCA 1995, the public official must be subjected to the legal duty to not disclose information obtained while holding the Commonwealth office. For s. 122.4A CCA 1995: 1. The information communicated by a Commonwealth officer to a non-Commonwealth officer. 2. The information must bear a security classification of secret or top secret. 3. The information must be capable of injuring national interest, public safety, defence of Australia, or interferes with the administration of criminal justice.	Communicates, retains, copies or fails to comply with directions to return official information or documents which is prejudicial to the security or defence of New Zealand.	For s. 7(1) PSGA 2018: 1. Disclose or causes the disclosure of information held by a Singaporean public sector agency. 2. The disclosure is not authorised by any data sharing direction issued by a Singaporean public sector agency before or at the material time. 3. The public official is working in the relevant Singaporean public sector agency. For s. 7(3) PSGA 2018: 1. Uses the information under the control of a Singaporean public sector agency. 2. The use is not authorised by any data sharing direction issued by a Singaporean public sector agency before or at the material time. 3. The public official who discloses the information was working in the relevant Singaporean public sector agency at the time of disclosure. 4. Obtains a benefit or causes harm to another individual as a result of the disclosure or use of the information.
Who is the law regulating?	Unclear. 1. S. 203A(1): Whoever that discloses any information obtained in the performance of his/her legal duties/ functions – this would mean that s. 203A(1) applies to, but is not limited to, public officials. 2. S. 203A(2): Whoever knowingly discloses information obtained by someone in the performance of their legal functions/ duties.	The common law offence regulates both: 1. Public officials acting in their official capacity. 2. Any third parties that publish the privileged information.	Section 4(1), 4(3) and 4(4) FISIA 1985 regulate both: 1. Public officials acting in their official capacity. 2. Any third parties that retains, discloses and/or fails to restore the secret information	Section 122.4 CCA 1995 regulates Commonwealth officers i.e. public officials subjected to a legal duty to not disclose information. Section 122.4A CCA 1995 regulates any third parties that receives security information that is classified as a secret or top secret.	Section 78A(1) of the CA 1961 only applies to a person who owes allegiance to the New Zealand government i.e. a public or statutory officer acting in his/her official capacity.	Section 7(1) PSGA 2018 regulates current and former Singaporean public officials. Section 7(3) PSGA 2018 regulates both: 1. Current and former Singaporean public officials. 2. Any person who uses the information disclosed by a current and former Singaporean public official.

	Malaysia	UK	Canada	Australia	New Zealand	Singapore
What is the standard for criminal liability i.e. mens rea?	For s. 203A(1), it is unclear or strict liability. For s. 203A(2), the standard is knowledge that the information was obtained in the course of performing one's legal duties/ functions.	The disclosure of privileged information/breach of public duty must be wilful and deliberate.	For s. 4(1) FISIA 1985, it is unclear or strict liability. For s. 4(3) FISIA 1985, it is knowledge or fallen below the reasonable standard of a recipient of secret information. For s. 4(4) FISIA 1985, it is the intention to harm or injure public interests, or otherwise failure to prove lawful reasons for retention of the secret information.	For s. 122.4 CCA 1995, it is strict liability. For s. 122.4A CCA 1995, it is also strict liability.	1. Knowledge that the public/statutory officer is acting without lawful authority in communicating, retaining, copying the official information. 2. Reckless (i.e. unreasonably as to whether the public/ statutory officer had lawful authority to disclose, retain, copy official information. 3. Intention to injure and prejudice the security or defence of New Zealand.	For both s.7(1) and (3) PSGA 2018, it is either: 1. Knowledge that the disclosure is unauthorised by ant data sharing directives issued by the relevant Singaporean public sector agency. 2. Reckless as to whether the disclosure is authorised.
Are there any express mitigating factors?	No.	Yes. The Crown Prosecution Service (CPS) guidelines.	Yes. Section 3 of the FISIA 1985 itself.	Yes. Section 122.5 CCA 1995 itself.	Yes. Section 78A of the CA1961 itself.	Yes. Section 7(2) and (5) of the PSGA 2018.
What are the express mitigating factors?	The Hansard provides some guidance to the interpretation of s. 203A, but this does not override the clear and wide language of the section. Furthermore, the Hansard is only useful if the interpretation of the s. 203A leads to some 'absurdity'.	1. UK citizen's right to access information under Article 10 of the European Convention of Human Rights (ECHR), incorporated by section 2 of the Human Rights Act 1998. 2. Prosecutions under this common law offence must be of serious nature and appropriate for criminal punishment. 3. The impugned conduct must have fallen below the ordinary standard of a similar officeholder. 4. A context-specific approach is important: the prosecution must consider the importance of the public object which the public officer serves and the nature and extent of the departure from his/her responsibilities.	Section 3(1) and (2) of the FISIA 1985 provides for circumstances in which disclosure of secret information will be treated as prejudicial to the safety and interests of Canada.	1. Section 122.5 CCA 1995 provides for a wide range of legal defences. 2. The Australian Attorney-General Department reviews the secrecy laws annually and provide recommendations to the Federal Government. 3. A statutory agency called the Independent National Security Legislation Monitor regularly reviews and conduct consultations as to the necessity, effectiveness and provide recommendations to secrecy laws in Australia.	1. The section only punishes public/ statutory officers. 2. Intention to injure national interest and public safety is the paramount element of criminal culpability, which is relatively the highest threshold of mens rea. 3. Existence of lawful authority is a complete defence available. 4. The official information must relate to national security.	Section 7(2) PSGA 2018 provides legal defences for offences under s. 7(1) PSGA 2018. Section 7(5) PSGA 2018 provides legal defences for offences under s. 7(3) PSGA 2018.

	Malaysia	UK	Canada	Australia	New Zealand	Singapore
Are there any express legal defences?	No.	Yes. The common law offence provides a full defence of justification or lawful excuse for the disclosure.	No for s. 4(1) FISIA 1985. Yes for s. 4(3) and (4) FISIA 1985. 1. S. 4(3): A complete defence is available if he/she can prove that the communication of the secret information is not voluntary. 2. S. 4(4)(b): A complete defence if he/she can prove lack of intention to cause harm to public interest or existence of lawful excuse in retaining or failing to restore the secret information.	S. 122.5 CCA 1995 provides for the following available defences: 1. The Commonwealth officer had lawful authority to disclose the information. 2. Information is already public when it was communicated. 3. The information was disclosed to a competent authority such as the integrity agency, competent court or tribunal, or to the media. 4. The information is an act of whistleblowing under the Public Interest Disclosure Act 2013. 5. The information communicated relates to a person.	It is a complete defence if the public/ statutory officer can prove existence of lawful authority in disclosing the information.	It is a complete defence under the sections 7(2) and (5) PSGA 2018 if the offender can prove any of the following circumstances: 1. The information in question is generally accessible or available to the public at the material time of its disclosure. 2. The disclosure of the information was permitted by any other written law, a court order or in any other circumstances which disclosure is permitted (e.g. whistleblowing).
Are there any Freedom of Information (FOI)/ Right to Information (RTI) legislation?	No.	Yes. The UK Freedom of Information Act 2000.	Yes. Access to Information Act 1985.	Yes. Freedom of Information Act 1982.	Yes. The Official Information Act 1982.	No. However, Singaporeans can access public data via websites of government agencies and public bodies. For information not available on these websites, Singaporeans may make a formal request for such information, and the relevant government agency or public body will have the discretion to disclose the information or refuse it.
Is this law enacted in tandem with secrecy laws i.e. laws that regulate official secrets?	No. Therefore there is a potential overlap with the Official Secrets Act 1972.	No. But this common law offence will not overlap with the UK Official Secrets Act 1989 since the statute takes precedence over case law due to the supremacy of the UK Parliament.	Yes. These laws are enacted as part and parcel of the FISIA 1985 framework regulating official secrets in Canada.	Yes. These laws are the only all-encompassing legislation regulating the disclosure of official secrets in Australia.	Yes. Since the Official Secrets Act 1951 was repealed by the Official Information Act 1982, the law that regulates official information is the Crimes Act 1961.	No. This law is wider than the Singaporean Official Secrets Act 1935 as it prohibits disclosure of any information held by the Singaporean public sector agency.

CHAPTER FIVE

Case Studies

Since its legislation, there has not been a single reported conviction under s. 203A. In fact, criminal charges based solely on s. 203A have been rare. However, s. 203A is frequently used in police investigations on the dissemination of sensitive public information along with other similar offences such as s. 8 of the OSA 1972 and s. 233 of the Communications and Multimedia Act 1998 (CMA 1998).

The case studies in this chapter reveal that law enforcement agencies do not actually use s. 203A to prevent leakages of information for the purpose of curbing corruption and collusion between public officials and criminals, but as a general tactic to intimidate those who possess information of public interest.

5.1 Charges under s. 203A

5.1.1 2018: Datuk R. Sri Sanjeevan, the Chairman of Malaysian Crime Watch Task Force

In 2018, Datuk R. Sri Sanjeevan was charged under s. 203A(1) and (2) for disclosing the contents of a police report on his blog in 2015. According to the then acting director of the Federal Police Commercial Crimes Investigation Department (CCID), DCP Datuk Saiful Azly Kamaruddin, the reason the charge was brought against him was because he did not obtain the consent of the complainant before publishing the contents of the police report.[79] He notably stated that a police report is a "confidential document of the complainant", and "anyone in possession of a police report and *publishes it without permission* from the complainant is committing an *offence* and action can be taken against him".[80] In 2020, Datuk R. Sri Sanjeevan was acquitted and discharged as the prosecution had failed to establish a *prima facie* case against him.[81] The prosecution did not appeal against his acquittal.

Here, s. 203A was utilised (unsuccessfully) to punish disclosure of information. The issue here is two-fold. Firstly, the charge against Datuk R. Sri Sanjeevan was only brought three years after the contents of the police report were posted in his blog.

Secondly, the fact that a full criminal trial was conducted when the elements of s. 203A were clearly not fulfilled demonstrate the broad potential for misuse of the section. Strictly speaking, Datuk R.

[79]. New Straits Times dated 17 December 2018: https://www.nst.com.my/news/crime-courts/2018/12/441525/sri-sanjeevan-charged-revealing-content-police-report.

[80]. The Sun dated 17 December 2018: https://thesun.my/local_news/illegal-to-share-police-report-without-the-consent-of-the-complainant-XJ281088.

[81]. Free Malaysia Today dated 8 January 2020: https://www.freemalaysiatoday.com/category/bahasa/2020/01/08/pengerusi-mywatch-bebas-kes-dedah-kandungan-laporan-polis/.

Sri Sanjeevan did not obtain the contents of the police report during the performance of a legal duty or function under any written law. Without this, an offence under s. 203A(1) cannot stand at all. Furthermore, a complainant is under no legal duty to make a police report under s. 107 of the Criminal Procedure Code (CPC).[82] Since the complainant, being the maker of the police report, did not receive any information in the performance of any legal duty or function prescribed by the law, the question of whether Datuk R. Sri Sanjeevan had knowledge that such information was disclosed in contravention of s. 203A(1) becomes academic. Thus, the charge under s. 203A(2) must fall as well.

It is likely that these two points rightly influenced the Sessions Court Judge to acquit and discharge Datuk R. Sri Sanjeevan at the end of the prosecution's case. However, the question still remains as to why the charge was brought against him in the first place, despite such a clear lack of legal basis.

5.1.2 2022: Leakage and circulation of the 'modified' Federal Court judgment on the final SRC appeal

In August 2022, the police commenced investigations under s. 203A, s. 8 of the OSA 1972, and s. 233 of the CMA 1998 after receiving reports on a leaked draft judgment in relation to the former Prime Minister Najib Razak's SRC final appeal. The leaked draft judgment was allegedly uploaded on the Malaysia Today website first, and went viral in many WhatsApp groups and social media right before the final judgment was delivered in open court later in the same day.[83]

[82]. In fact, it is the police that is under a legal duty to receive information from the maker of a first information report or a police report – s. 107(4) of the CPC.

[83]. The Rakyat Post dated 24 August 2022: https://www.therakyatpost.com/news/2022/08/24/leaked-altered-najib-judgment-draft-court-confirms-lodges-police-report/

The Chief Registrar Office of the Federal Court subsequently issued an official statement confirming the leak but insisted that the draft judgment being circulated was modified, condemning this as an intentional act to undermine the administration of justice and the integrity of the judicial system.[84] There are no media reports regarding any follow-ups by the police after their investigations and whether any suspects were arrested or further questioned.

The police conducted investigations under s. 203A to identify the culprit who leaked the draft judgment and for the act of disseminating false information. While it could be argued that the leaked document was sensitive information, the use of s. 203A illustrates how the section can be applied to scopes far broader than its original ambit of eliminating corruption and collusion between public officials (especially law enforcement officers), cartels and criminal syndicates.

This raises serious questions about the actual significance of s. 203A in the current legal landscape and public governance. When it comes to the protection of classified information, s. 8 of the OSA 1972 is more than adequate. Similarly, when it comes to ensuring responsible use of network facilities, s. 233 of the CMA 1998 is wide enough to prohibit and punish dissemination of false information intended to annoy, abuse, threaten or harass another. To extend the application of s. 203A beyond the object of fighting organised crimes (and anti-corruption) is to run afoul of Parliament's intention. Notwithstanding this comparison, both the OSA 1972 and CMA 1998 remain extremely problematic in how they criminalise certain forms of expression.

[84]. BERNAMA dated 24 August 2022: https://www.bernama.com/en/news.php?id=2114226.

5.1.3 2024: Badrul Hisham Shaharin (Che'gu Bard), a member of the political party BERSATU

In July 2024, Badrul Hisham Shaharin (more commonly known as 'Che'gu Bard') was arrested and remanded for 2 days following police investigations under s. 203A(2) of the Penal Code for giving false information, as well as s. 8 of the OSA 1972 for disclosing classified information and s. 233 of the CMA 1998 for disseminating false information. He was investigated for exposing alleged corruption by a senior naval officer.[85] The Kuala Lumpur police chief, Datuk Rusdi Mohd Isa, stated that it is a "normal procedure" to arrest Che'gu Bard and remand him for the purposes of assisting police investigations over his allegation of corruption. Furthermore, he stated that after evaluating Che'gu Bard's act of disclosure, there is "*indeed a need for him to be arrested*" as the police needed to access the incriminating documents to investigate "where [Che'gu Bard] got the documents from because he is not an employee [of the Royal Malaysian Navy]". There are no media reports as to whether the exposed senior navy officer was arrested or questioned by the police and/or the MACC for further investigations.

Again, s. 203A appeared to be used by law enforcement agencies to intimidate whistleblowers and punish public interest disclosures, contrary to the stated object of s. 203A. As seen in this case, the police decided to investigate Che'gu Bard instead of the named official. Moreover, the incident would set a bad precedent in making it a prerequisite for the whistleblower to disclose his source of the information and to prove his accusations true before any proper investigations can be taken against the wrongdoer he accuses. The effect of this 'standard of procedure' would create even more obstacles

[85]. BERNAMA dated 29 July 2024: https://www.bernama.com/en/news.php?id=2323085.

to the legal protections provided by the WPA 2010.

It is important here to highlight the comments made by the presiding Magistrate who heard the remand application against Che'gu Bard. After hearing the submissions from both the DPP and Che'gu Bard's lawyer, the presiding Magistrate classified Che'gu Bard as a whistleblower pursuant to the provisions of the WPA 2010 and directed that he "should be accorded legal protection from any civil and criminal action".[86] It is concerning that the police – an enforcement agency by virtue of s. 2 of the WPA 2010 - needed a reminder from the judiciary to fulfil its statutory obligations to protect whistleblowers. This illustrates further the deep incongruency between the use of s. 203A and the whistleblower protection framework.

5.2 Key statements by enforcement figures on s. 203A

What is especially notable about the section is how it has been referred to by members of government. The varying interpretations of s. 203A by law enforcement agencies, mainly the police, clearly demonstrates the broad and unclear scope of the section.

5.2.1 2015: Attorney General used s. 203A to 'preserve the integrity of criminal investigation'

In 2015, at the peak of the 1MDB scandal allegations, documents allegedly implicating Najib Razak were disclosed in the Wall Street Journal article titled "Malaysia Orders Freeze of Accounts Tied to Probe of Alleged Transfers to Prime Minister Najib". The then AG, Tan Sri Abdul Gani Patail, expressed in a media statement that he "would

[86]. Berita Harian dated 28 July 2024: https://www.bharian.com.my/berita/kes/2024/07/1277725/chegu-bard-direman-2-hari-isu-dakwaan-rasuah-pegawai-tinggi-tldm

not hesitate to prosecute any person found to have leaked confidential investigation-related information" to preserve the integrity of criminal investigations and public trust in the inter-agency Special Task Force to investigate the alleged subject-matter. He then stressed that this disclosure was "not a question of whistle-blowing" because the matter is undergoing investigation.[87] He was instead concerned that the documents were leaked from within the investigation itself. The statement was endorsed by key leaders of enforcement institutions such as the Governor of Bank Negara, Inspector-General of Police, and the Chief Commissioner of the MACC.

Nonetheless, the information concerned was not classified official information under the definition of the OSA 1972. Furthermore, it is not entirely clear how the leakage of information could undermine or obstruct their operations. This is an obvious example of how s. 203A(1) is used to prohibit disclosure of information not classified as official secrets under the OSA 1972. This interpretation does not appear to address the objective of s. 203A i.e. fighting organised crime, but instead, the unclear objective of preserving the integrity of police investigation.

5.2.2 2019: PDRM used s. 203A to create 'standard of procedures' for investigating leakages of information

In 2019, the PDRM Corporate Communications Head Datuk Asmawati Ahmad made the following statements regarding s. 203A:[88]

[87]. Media statement released by Bank Negara Malaysia dated 8 July 2015. Accessed on 9 January 2024: https://www.bnm.gov.my/-/special-task-force-investigation-relating-to-allegations-of-funds-transmitted-to-the-accounts-of-the-prime-minister

[88]. Malay Mail dated 21 August 2019: https://www.malaymail.com/news/malaysia/2019/08/21/cops-warn-against-spreading-classified-info-after-directive-against-zakir-n/1782799

- S. 203A creates an offence for circulating and **exposing** official information classified as secrets;
- The primary use of s. 203A by the police is to identify the source of the leakage of classified information;
- Individuals investigated under s. 203A are required to "assist the police to identify the source" of leakage;
- S. 203A prohibits any person who has in their possession of classified information **obtained from any parties through any means** from disclosing or sharing it to other individuals;
- Any person in possession of classified information "cannot share or spread it", otherwise they will be criminally liable under s. 203A(2);
- The police will always conduct investigations under both s. 203A(1) and (2) at the same time.

This statement, albeit clarifying the standard operating procedures of the police, is wholly detrimental to anti-corruption efforts as it fails to mention the laws protecting whistleblowers during investigations. This is clear proof that s. 203A(2) is interpreted by law enforcement agencies to cover situations where the OSA 1972 does not theoretically apply i.e. prohibiting the disclosure of classified information by individuals who are not civil servants and did not obtain the classified information in the performance of any public duties.

However, even this interpretation is misleading because s. 203A does not only regulate classified information – such as information classified under the OSA 1972 – but an undefined scope of information that, as explained above, can be read as limitless.

Regardless of whether the omission to address the WPA 2010 is deliberate or innocent, the statement sends a concerning message to potential whistleblowers and limiting their access to legal protections under the WPA 2010. Another question to be raised here is whether a whistleblower is caught by s. 203A(2) if they make a police report under s. 107 of the CPC and, in doing so, disclose information obtained by them in the discharge of their legal duties or functions under the written law.

5.2.3 2021 & 2024: PDRM used s. 203A to 'prevent obstruction' of ongoing investigations and criminal proceedings

In April 2021, the Johor police chief Datuk Ayob Khan Mydin Pitchay made a public statement threatening to arrest individuals who shared via WhatsApp the confidential list of 12 law enforcement officers (including police officers and a deputy public prosecutor) who were arrested for allegedly assisting fugitive businessman Nicky Liow Soon Hee.[89] The focus of s. 203A was strangely towards those who disseminated the list of arrested persons that was deemed 'sensitive' by the police, rather than the captured individuals themselves who were allegedly colluding with sophisticated human trafficking syndicates.

A similar incident happened recently in June 2024, where the Federal Classified Crime Investigation Unit collaborated with the Malaysian Communications and Multimedia Commission (MCMC) to investigate the leaked investigation details linked to the murder of Zayn Rayyan Matiin on social media platforms. The Selangor police chief Datuk Hussein Omar Khan held that the investigations were carried out under s. 203A, section 8 of the OSA 1972 and section

[89]. Free Malaysia Today dated 27 April 2021: https://www.freemalaysiatoday.com/category/nation/2021/04/27/stop-sharing-names-of-cops-nabbed-over-nicky-leow-links-warns-ayob/

233 of the CMA 1998 to prevent obstruction of court proceedings.[90] Although there was a good reason here to investigate the leakage, it must be stressed once again that the use of s. 203A had no relation whatsoever to fighting organised crime.

5.3 Summary

The fact that there are no recorded cases judgments or successful prosecutions under s. 203A highlights its practical insignificance in terms of prosecution of crimes. This is especially so when considering that it is rare for s. 203A to be used as a standalone charge. Instead, it appears to need the 'support' of other similarly draconian laws in its application.

It is concerning that law enforcement agencies such as the police appear ready to use the section to prohibit the public from spreading information used in ongoing investigations that are deemed 'sensitive'. The section is commonly used in ways that clearly deviate from the objective of fighting organised crime to what the law enforcement agencies think is necessary to preserve the integrity of criminal investigations and court proceedings. This echoes the arguments raised in Chapter 3, whereby the wide language and ambiguous scope of the section allows law enforcement agencies to bend its application to their whims.

What is clear from the case studies above is that s. 203A is commonly resorted to by law enforcement agencies to create an atmosphere of fear and a hostile environment for any persons who wish to disclose information on improper conduct and potential wrongdoing within their knowledge. The retention of the section for

[90]. New Straits Times dated June 15 2024: https://www.nst.com.my/news/crime-courts/2024/06/1063888/investigations-zayn-rayyan-probe-leak-being-done-under-official

ten years despite its lack of use in prosecuting rogue enforcement officials and organised criminal syndicates speaks to the fact that s. 203A is useful not to prevent collusion and corruption, but as a tool for fearmongering.

CHAPTER SIX

Recommendations

The analysis of the previous chapters has shown that s. 203A is problematic in several ways. Due to the conflict between s. 203A and the WPA 2010, many whistleblowers are unable to access legal protections. Law enforcement agencies have also regularly taken advantage of the wide language of s. 203A to protect information unilaterally deemed sensitive. To overcome these issues, C4 Center proposes the following recommendations.

6.1 Repeal s. 203A of the Penal Code

The above analysis has identified the following:

- Numerous criticisms were levelled against the law during its tabling in Parliament. Despite this, the Minister argued that it would be best to "introduce the law first and amend it later." [91]

[91]. Hansard dated 22 October 2013, page 59.

S. 203A has not been amended since its introduction.
- The lack of a single reported conviction under s. 203A in ten years indicates that the section is too vague to be enforced successfully.
- Cases where s. 203A has formed part of a charge are completely unrelated to the government's stated objective of fighting organised crime. Instead, these cases are directly related to punishing whistleblowers.
- Statements by parties connected to the government in relation to s. 203A illustrate a complete divergence from the objective of fighting organised crime. Instead, the statements show the use of s. 203A as tool to silence those not aligned with government interests.
- In comparison to similar laws from other jurisdictions, s. 203A is extremely regressive in nature due its lack of clarity in scope and application.

It can also be argued that the existence of s. 203A has had a negative effect on:

- **Whistleblowers who wish to report improper conduct.** As whistleblower protection is only available to disclosures of improper conduct not prohibited by law, it is highly probable that s. 203A has discouraged whistleblowers from reporting improper conduct due to fear of being caught by this provision.
- **The development of a transparent and accountable culture within the civil service.** It has long been argued that eradicating a culture of secrecy within the civil service is crucial to improving governance and combatting corruption in the public sector. The continued existence of s. 203A creates an uncertain and fearful environment for public officials and how they handle informa-

tion. As long as this law exists, it would be rational for a public official to err on the side of caution and treat information in a secretive manner, stymieing the development of more open government.

Therefore, C4 Center urges the immediate repeal of s. 203A.

Though an argument could be made that s. 203A could be amended to overcome its inherent weaknesses – taking cues from other jurisdictions – this would only create more confusion as to the purpose of the law. As it stands, the negative impact, proven misuse, and regular misinterpretation of the section necessitate its immediate repeal. If a law is necessary for fighting organised crime or punishing disclosures of information detrimental to public interest, one can be tabled separately and passed after seriously taking into account criticisms and opposing views.

6.2 Actively enhance the WPA 2010 to supersede s. 203A and any other laws prohibiting disclosure of information

The various conflicts with s. 203A underscore the inherent weakness of the WPA 2010 framework. Currently, the scope, accessibility, and protections afforded under the WPA 2010 are highly inadequate to effectively protect whistleblowers.

Consequently, repealing s. 203A alone is not enough. Instead, the WPA 2010 must also be comprehensively revamped to better fulfil its intended objective of fighting corruption through fostering a culture of whistleblowing. Thus, the WPA 2010 should be amended as follows:

- **Remove the proviso to s. 6(1) WPA 2010** to enable whistleblowers to receive prima facie protection from enforcement agencies so long as there are reasonable grounds to believe that the information reported is true.[92]
- **Introduce a "notwithstanding clause"** into the WPA 2010 that expressly stipulates that provisions under the WPA 2010 shall unequivocally prevail over any written laws prohibiting disclosure of any information involving matters of public interest or improper conduct.
- **Introduce a public interest defence** to restrict revocation of whistleblower protection only to cases where the specific harm to some identifiable legitimate national interest far outweighs the public's right to know the information disclosed.
- **Amend ss. 6 and 8 of the WPA 2010 to include internal and external disclosure to the public**. This includes the media, MPs, civil society organisations, lawyers, and other parties not defined as an "enforcement agency" under section 2 of the WPA 2010.
- **Amend the WPA 2010 to include a statutory presumption that disclosure of certain categories of information**, such as corruption, environmental harm, abuse of public office, human rights violations, **shall always be in the public interest**. The burden shall lie on the government to prove otherwise and justify non-disclosure.
- **Amend s. 11 WPA 2010** to **give discretion to enforcement agencies**, enabling them the flexibility to weigh all the factors involved when deciding **on the revocation** of whistleblower protection.
- Require law enforcement agencies and regulatory bodies to **regu-**

[92]. In line with the UNCAC CoSP 2023 Resolution 10/8 (CAC/COSP/2023/L.12/Rev.1), which prefers the "reasonable belief/grounds" interpretation over "good faith" standards for disclosures.

larly educate the public about whistleblowing.

- **Amend s. 26 WPA 2010 to clarify the purpose of the reward system** and the kinds of reward. The purpose of the reward system must be aimed at encouraging motivation for the public to collectively fight corruption and to fairly compensate the whistleblower for the labour and risk involved.

6.3 Enact a Right to Information Act

The culture of secrecy is embedded and institutionalised under the OSA 1972 and s. 203A. The OSA 1972 and s. 203A should be reformed and repealed respectively as these laws disproportionately prohibit the act of disclosing information of public importance. However, these reforms alone may not be sufficient to uproot the existing secrecy regime and barriers to whistleblowing. Holistic reforms that promote a culture of open accountability must be effected in order to resolve the possibility of conflicts between laws that prohibit and permit disclosure of information, such as s. 203A and the WPA 2010. To this end, **the government should first legislate a Right to Information (RTI) Act**. This law would include the following:

- The overriding presumption that all information held by governments and public institutions are in principle subject to disclosure and openly accessible to the public upon request. This is known as the **principle of maximum disclosure** which recognises the public's right, including whistleblowers, to receive and access in a timely and easily accessible manner.
- Disclosure of information should **only be refused if there are legitimate grounds** recognised in line with international standards and best practice, such as national security or personal privacy.

- Governments are subjected to an overriding legal obligation to publish information, which is known as the **obligation of proactive disclosure**. Essentially, governments should publish all information through the relevant channels and ensure that it is routinely updated and easily accessible by the public.
- **Establish an independent administrative oversight body** to ensure that government agencies and public institutions have appropriate processes and procedures in place to guarantee and facilitate access to information. The core purpose is to ensure that governments do not act as gatekeepers who have full and decisive discretion on what the public should or should not know.

6.3.1 How will RTI laws help whistleblowers?

RTI laws and whistleblower protection laws are closely connected to each other in preventing corruption. RTI laws ensure that the public is able to access information on processes and decisions made by the government, allowing the public to hold the government accountable for any fraud, corruption, mismanagement, abuse of authority or incompetence. This parallels the purpose of whistleblower protection laws, that is to encourage whistleblowers to come forth and disclose crucial information regarding instances of corruption and wrongdoing otherwise unknown to the general public, thus assisting law enforcement agencies in investigating and combatting corruption.

The RTI framework would essentially supplement the existing legal framework under the WPA 2010, allowing whistleblowers to retrieve necessary information to bolster their formal complaints on any improper conduct to law enforcement agencies and overcome difficult evidential thresholds imposed on whistleblowing. RTI laws would also enable whistleblowers to conduct research and obtain information on their own regarding all the necessary procedures they must comply with in order to be entitled to the legal protections accorded under the WPA 2010, which is currently unavailable to whistleblowers who would otherwise lose their legal protection on the grounds of disclosure to entities that are not enforcement agencies. RTI laws would also require relevant enforcement agencies to publicly disseminate their whistleblower policies and guidelines, thus streamlining the whistleblowing process and allowing whistleblowers to direct their complaints to the proper channels of disclosure.

6.3.2 The universal adoption of RTI laws and its impact on public institutions and civil service worldwide

According to UNESCO, 138 UN Member States have adopted access to information (ATI) laws as of 2023,[93] and ARTICLE 19 has stated that at least 91% of the global population is currently located in a country or territory that allows them to make a formal request for information from a state and/or a local authority.[94] Public ATI is also recognised as an element of the Sustainable Development Goals (SDGs) under Target 16.10, emphasising the essential nature of information transparency and accessibility in improving public governance.

UNESCO's *2022 Report on Public Access to Information* includes a section on the State of New South Wales in Australia, where it was found that mandated proactive disclosure of information was an

[93]. United Nations Educational, Scientific and Cultural Organization, *The need to accelerate worldwide progress: UNESCO 2023 Report on Public Access to Information (SDG 16.10.2)*, Paris, p. 13, available at <https://www.unesco.org/en/articles/need-accelerate-worldwide-progress?hub=776>.

[94]. ARTICLE 19, *Sustainable Development Goals: On or off track? Assessing the progress through freedom of expression and information*, July 2023, p. 7, available at <https://www.article19.org/wp-content/uploads/2023/07/SDGs-Briefing-July-2023.pdf>.

important tool for informing the public, increasing participation in community life and trust and confidence in public institutions, and improving decision-making.

> *The proactive disclosure of government information ensures transparency, accountability and provides a necessary assurance that elected officials and other publicly funded senior decision makers, place the public interest above their private interests as demanded by, and expected of, public office. Importantly, disclosure of interests minimizes the risk of fraud and corruption.*
>
> *...*
>
> *In particular, under the Government Information (Public Access) Act 2009, local councils must publish information about the returns of pecuniary interests lodged councilors and designated persons. Upon becoming aware of non-compliance with these requirements the New South Wales Information Commissioner undertook a compliance audit. The resultant education and governance recommendations have secured greater levels of transparency and accountability.*
>
> *...*
>
> *When the New South Wales Information Commissioner became aware of possible non-compliance with contract disclosure requirements by the New South Wales Government's insurance and care scheme provider [it] undertook compliance audits. The agency's implementation of the Information Commissioner's recommendations has resulted in systemic improvements in accountability and transparency.*[95]

The First Global Report on the Implementation of Access to Information Laws (2020) by the Intergovernmental Council of the International Programme for the Development of Communication

[95]. United Nations Educational, Scientific and Cultural Organization, *A Steady Path Forward: UNESCO 2022 Report on Public Access to Information (SDG 16.10.2)*, Paris, p. 33-34, available at <https://www.unesco.org/en/articles/steady-path-forward?hub=776>.

similarly explains the benefits brought about by the implementation of Sri Lanka's RTI Act, No. 12 of 2016:

> *During the first three years of its implementation, the RTI Act has made inroads into rendering governance open and transparent, "significantly altering the relationship between the citizen and the State" and, to some extent, giving ways to increased transparency and accountability.*
>
> ...
>
> *[T]he study concluded that the RTI regime has cultivated a culture of pro-transparency in Sri Lanka. Information disclosure has not only led to the mere release of information but has also shaped the public's attitude in asserting accountability in governance. The CSOs, whose role also facilitated citizens to file RTI requests, have acknowledged that development projects have become more transparent and corrupt practices have reduced due to the RTI Act. ATI has therefore become a form of activism that deepens democratic participation, transparency, accountability and combating corruption. Working towards achieving the SDGs and monitoring country progress on that basis has also supported and encouraged pro-transparency advocates in their efforts of ensuring more transparency and sustainable development.*[96]

[96]. Intergovernmental Council of the International Programme for the Development of Communication, *Access to Information for Sustainable Development: From Promise to Practice – Report on the Monitoring and Reporting of SDG Indicator 16.10.2 (Public Access to Information)*, CI-20/COUNCIL.32/5, Paris, 28 September 2020, pp. 22-26, available at <https://unesdoc.unesco.org/ark:/48223/pf0000374637>.

6.4 Amend the OSA 1972 and harmonise it with the RTI framework

In tandem with the introduction of an RTI legislation, the legal framework under the OSA 1972 needs to be amended to align consistently with the RTI framework and the principles of open governance in general. It is worth reiterating that the OSA 1972 may not need to be repealed completely (as it still bears considerable importance in protecting certain information for legitimate purposes), but it should be fundamentally revamped and revised in harmony with the ethos of the RTI legislation. In any event of conflict, the RTI legislation should prevail over the OSA 1972.

The introduction of a RTI legislation and amending the OSA 1972 in line with RTI laws is to essentially create two separate systems of law – the former creating a holistic system to facilitate public access to government-held information, and the latter governing classification and secrecy. For an example of how this could function, guidance may be drawn from the federal level Australian model established by the Freedom of Information Act 1983 (FOIA 1983) and the Australian Government Protective Security Policy (AGPSP).[97]

Under the Australian model, the fact that information or a document is classified as an official secret according to the AGPSP does not automatically confer upon it the status of secrecy. Rather, classification is only for internal administrative processes such as document access and storage. Classification is not conclusive as to whether a document or information may subsequently be disclosed under the FOIA 1983. Upon receipt of an FOI request, the FOI team in the relevant government agency or public institution collects all the relevant

[97]. Australian Government Protective Security Policy Framework Release 2024, page 38-53: https://www.protectivesecurity.gov.au/system/files/2024-11/pspf-release-2024.pdf .

documents and reviews the “harm posed” to determine whether any statutory exemption to prohibit disclosure would apply. Otherwise, the information must be disclosed. It is also crucial to mention that disclosure itself **does not** cause the original document to lose its classification. The disclosed copy of the information or document is merely an authorised copy for the purposes of disclosure, and some parts of the information may be blocked or redacted, if necessary.

If this model is accepted, the necessary amendments to the OSA 1972 would include the following:

- **Amend the definition of “official secrets”** under section 2 of the OSA 1972 by deleting the phrase “any document specified in the Schedule and any material and material relating thereto and”.
- **Delete sections 2A and 2B of the OSA 1972** that confers wide powers to the Minister to amend the Schedule to the OSA 1972 and for public officials to be appointed to classify official documents.
- **Delete the Schedule to the OSA 1972** which contains the list of classes of information that are presumptively “official secrets”.
- **Delete section 16A of the OSA 1972** which immunises the exercise of the power under section 2B from judicial review.
- **Introduce a new section to confine the power of the Minister to classify information to a harm or public interest test.** This will require the Minister to consider whether there is a legitimate aim to classify the information (legality), there is a real harm to the legitimate aim if the information is disclosed (necessity) and the harm in disclosing the information far outweighs the public interest (proportionality). This section must be harmonised with the RTI legislation to allow all information to be accessed unless there is a specific legitimate interest justifying its non-disclosure. Instances of corruption, *inter alia*, should be presumed to

be in the public interest to be disclosed even if it concerns official secrets; the burden lies on the government to prove why the harm in disclosing the official secret far outweighs the benefit and the public's right to know.

- **Introduce a new section for the right to appeal** against the Minister's decision to classify information under the RTI legislation. In other words, the decision of the Minister to classify information as an official secrets should not be conclusive, and it shall be amenable to judicial review and scrutiny by an independent oversight body established to oversee the implementation of the RTI legislation. Whistleblowers must be deemed to have prima facie legal standing (or *locus standi*) to file for an appeal against the Minister's decision for the purposes of his disclosure, so long as he is able to show reasonable grounds for believing that the disclosure is true.
- **Insert a new section into the OSA 1972 to introduce a public interest defence** where any impugned act of unauthorised disclosure that was made under a reasonable belief in public interest, wrongdoing or improper conduct, the person shall not be held liable under the OSA 1972 and shall be afforded prima facie protections under the WPA 2010. In order words, the WPA 2010 shall prevail in an event of conflict with the penal provisions under the OSA 1972.

6.4.1 How will amending the OSA 1972 help whistleblowers?

If the OSA 1972 is amended, the positive impacts on anti-corruption efforts are two-fold. Firstly, the apparent conflict between the WPA 2010 and the OSA 1972 would be resolved in favour of whistleblowers and efforts to combatting corruption. Public officials who have first-hand knowledge of information that are classified as official secrets under the OSA 1972 should nevertheless have the option to disclose them if they have reasons to believe that the classified information forms the subject matter of any improper conduct or wrongdoing. In such a case, the whistleblower must be given legal protection under the WPA 2010 to assist law enforcement agencies in investigating the formal complaint. Without the necessary amendments to the WPA 2010 and the OSA 1972 (and without s. 203A repealed), a public official who possesses information about corruption, abuse of power and criminal misappropriation of public funds by their colleagues or superiors are practically unable to disclose them at all. This culture of secrecy would allow corruption to thrive in the civil service unchecked and uncontrolled.

Secondly, the amendments to the OSA 1972 and the enactment of a RTI legislation would result in a paradigm shift of social attitude from an entrenched culture of secrecy to a culture of openness and transparency. These reforms will create a new social norm where reasonable disclosures on corruption, fraud, mismanagement and incompetencies on the part of the government are widely encouraged and the informed public will have freer access to information to hold the government publicly accountable for their actions or failures. Whistleblowers within the public sector will be more daring in holding their colleagues and superiors accountable for their wrongdoings, thus restoring trust and confidence in public institutions by sending the message that not all civil servants are unethical and complicit in corrupt practices. This also minimises instances of corruption in the public sector as the risks for being exposed and caught by fellow civil servants are high.

CHAPTER SEVEN

Conclusion

After ten years in force with problematic results, it is now the right time to repeal the redundant s. 203A. The fact that there were no reported successful prosecutions or recorded judgments involving the section speaks of the provision's own ineffectiveness in fighting organised crimes and corruption. Yet the pernicious impact of s. 203A on whistleblower protection laws and the anti-corruption movement cannot be easily ignored. This section has inculcated a lived reality of constant fear amongst civil servants, enforcement officers, GLC employees and many more, which will persist until clarified by the apex court or through legislative amendment.

Its alarmingly broad scope and vague application manifests draconian tendencies, granting almost unchecked powers to law enforcement agencies. S. 203A effectively has no discernible limit to its application, allowing law enforcement agencies to read into the language and arbitrarily apply the section to their liking. Today, law enforcement agencies may use the section to uphold public justice. Tomorrow with the same breath, the police can use it to silence and punish whistleblowers. The element of unpredictability, uncertainty and absurdity associated with the application of s. 203A is exactly what deters whistleblowers from exposing corruption. Another draconian aspect of s. 203A is its ability to expand the theoretical scope of its controversial and repressive counterpart, the OSA 1972. In the absence of a certification process or a viable framework to regulate its enforcement, s. 203A effectively prohibits the disclosure of information that falls outside the ambit of the OSA 1972. If s. 203A and the OSA 1972 are read together, it would mean that no information obtained in the performance of one's legal duties, whether in the public or private sector, could ever be disclosed. This makes section 203A no different from a gag order on potential whistleblowers, normalising a culture of secrecy and subservience in all aspects of Malaysian society.

After comparing s. 203A with similar laws in the UK, Canada, Australia, New Zealand and Singapore, one apparent shortcoming of s. 203A is the absence of statutory defences, illustrations, or explanations which provide particularity to the scope of application and the purpose of the respective legislations in prohibiting the disclosure of certain information. These mitigating factors are crucial to restrict the disclosure of certain information in cases where it is strictly necessary to protect legitimate interests. The laws in other jurisdictions account for intersections with laws crucial for open governance and transparency, such as whistleblower protection laws and the right to information. In short, they represent *bona fide* attempts by the respective Legislatures to strike a fair balance between the competing interests of safeguarding national interest and upholding the public's right to know. None of these were present in the wording of the s. 203A nor the Hansards.

In conclusion, immediate reforms are desperately needed to bolster whistleblower protection. The failure of the WPA 2010 and s. 203A to curb corruption underscores the need for comprehensive reforms. The government must acknowledge the urgency in repealing s. 203A and amending the WPA 2010 and OSA 1972. In line with these reforms, the government must enact a robust RTI legislation to cultivate an active culture of open transparency and uphold the right to information. With information being widely accessible to the public and public interest disclosures being normalised, instances of corruption will be more effectively prevented and easily exposed. Most importantly, the upheaval of the secrecy regime would lead to the removal of obstacles for whistleblowers, who are instrumental in uncovering corruption. Immediate government action is needed to enhance accessibility of legal protections to this brave class of persons, as delaying the overhaul of these laws will only serve to further entrench corruption in Malaysian institutions, undermining democracy, human rights, and public welfare.