(2020) 27 JUUM 20 - 24
https://doi.org./10.17576/juum-2020-27-02

Down the Cyber Rabbit Hole: Whistleblowing as a Means to Fulfilling Moral Obligations in Cyber Space

Hazlina Shaik Md Noor Alam

ABSTRACT

This paper discourses several issues stemming from whistleblowing. These include, but are not limited to, imposition of liability for inaction in the face of wrongdoing, to scrutinising the available legislative protections for whistleblowers. This paper will also discuss whistleblowing in relation to cyber whistleblowing, which essentially means making disclosures on any misconduct that occurs on the internet. Cyber whistleblowing can provide the basic framework for combating misdeeds online, as it forms a central part of cyber security. Whistleblowing has its roots in less than desirable circumstances, often offering little to no benefit to whistleblowers involved. The act of blowing the whistle, all share common traits, to call attention too, and to punish any and all wrongdoings. Legitimising whistleblowing would enormously help to remove the stigma that is often tied to whistleblowers. This would also give rise to more voluntary whistleblowing in relation to cyber security.

Keywords: Whistleblowing; cyber space; accountability; compliance

INTRODUCTION

The internet is a vast, and more often than not, provides an endless space of possibilities. The internet is where people find information, upload pictures and stories of their family and friends, as well as selling and buying things you never thought you wanted, let alone needed. However, with the implosion of the internet, so does come with it a new set of dangers, one brings to light information or offences that was previously left hidden.

CYBER SPACE AND WHISTLEBLOWING

As cyber space offences are somewhat new to the landscape, so are the attempts to unearth them. A scenario can be seen from the United States. In March 2016, FBI raided the corporate headquarters of Tiversa, a Pittsburgh-based security firm under investigation for providing the Federal Trade Commission (FTC) with false information about data breaches at companies that declined to purchase Tiversa's data protection services. The story unfolded when a former Tiversa employee, Richard Wallace, testified in a 2015 Federal Trade Commission hearing that Tiversa provided the FTC with doctored evidence purporting to prove that selected organizations had suffered a data breach.[1] According to a report by the House of Representatives Committee on Oversight and Government Reform, information provided by Tiversa "formed the basis for multiple enforcement actions and dozens of warning letters" including the high-profile LabMD enforcement action. Although Tiversa's alleged conduct may be an egregious outlier, a company's conduct need not be malicious, to be subject to a cyber whistleblower complaint about the company problems, as well as creating public relations and regulatory issues. Even companies that diligently seek to detect and prevent cyberattacks can become subject to regulatory scrutiny by virtue of a cyber whistleblower's tip. This is also coupled with significant incentives for whistleblowers. Motivation for whistleblowers can come in many forms, including earning immunity from government, in addition to capitalizing on the monetary bounty program incentives promulgated by various regulatory agencies. The bounty programs in the US can provide financial incentive to the tune of millions of dollars, depending on the outcome or information provided.[2]

However, as whistleblowing claims are relatively new, many organizations are unaware of their existence. Furthermore, if many of these claims are pursued and resolved quietly, this would leave many corporations and their directors in the dark and oblivious to the potential dangers that could arise. Cyber-attacks today have become more sophisticated and targeted to specific victims depending on attacker's

motivation, for example for financial gain, espionage, coercion or revenge; opportunistic untargeted attacks are also very prevalent.[3]

In addition, many companies that have yet to experience a massive security breach will likely believe that their current cyber controls are sufficient, resulting in the corporation taking a somewhat passive approach. The word cyber was originally used to denote a specific meaning in the world of cybernetics, but has now expanded to anything related to computers and the like.[4] Even when the risk is exposed and understood, the corporation will weigh the time, costs and expertise required to implement stronger controls. This then often acts as a deterrent to sufficient and adequate implementation of cyber regulations in the corporation.

However, corporations and regulators alike have recognized the growing importance of cybersecurity, and are steadily increasing cyber monitoring and control. This leads to more frequent expeditions, seeking for cyber whistleblowers, to enhance their supervision and enforcement capabilities. When a corporation ignores its concerns about cyber leaks and dangers, this would pose huge risks for them. Their employees, once ignored by the internal structure of the corporation, may disclose their grievances externally. These whistleblowers can also receive potentially huge awards for bringing their concerns to law enforcement officials.[5]

Essentially, silencing cyber whistleblowers would not work in the corporations' favour. The lack of concern can invite whistleblower retaliation claims, and to ignore them would invite regulators' notice and scrutiny. Hence, corporations need to follow common sense and best practices when dealing with employees' concerns. Such measures could include formal mechanisms for receiving employee concerns, the steps taken after those disclosures, compliance programs, written policies, in addition to management training.[6]

With the explosion of the internet, it comes with it the lion's share of dangerous probabilities. From trolling to cyber stalking, the perils of cyber space are endless. As in the real world, those who seek to preserve the sanctity of cyber space are known as cyber whistleblowers. As with their counterparts in reality, cyber whistleblowers will blow the whistle on any cyber related misconducts.

For instance, in the US, while there are no federal laws that specifically protect cyber whistleblowers, existing anti-retaliation provisions are often broad enough to cover employees who raise information regarding security concerns. Most notably, federal statutes prohibiting retaliation against corporate whistleblowers, who report misconduct in connection with federal funds, as well as state wrongful discharge actions, may well apply to cyber whistleblowers.[7]

CYBER WHISTLEBLOWING AND CYBER SPACE

Whistleblowing can also be seen in cyber space and the problem with cyber space lies in its infinite vastness. Cyber space allows a great deal of secrecy in order to carry out its function. Yet, this secrecy can also hide actions that would not necessarily meet the expected ethical or social standards. Moreover, excessively secretive environments actually promote abuses of power, by creating an insider mentality that blurs the lines between the need to get results and what is acceptable behaviour towards those on the outside.[8] This is similar to how cyber bullying works an 'us against them' mentality.

'Cybersecurity whistleblowers', are defined as individuals who escalate concerns regarding internal management of cyber risks, cyber threats, data breaches, or other cybersecurity related information to supervisors, compliance officers, and boards of directors, play a crucial role in the modern-day compliance functions of regulated entities.[9]

As whistleblower provisions are becoming increasingly relevant in the context of cybersecurity, the Securities Exchange Commission (SEC), has signaled a renewed focus on cyber-based threats. In 2017, the SEC announced the creation of a dedicated Cyber Unit, and Chairman Jay Clayton released a lengthy statement in which he pledged the SEC would continue to prioritize its efforts to promote effective cybersecurity practices.[10]

In 2018, Christoper Wylie blew the whistle on arguably the largest tech scandal in history, cementing his role as a bona-fide cyber whistleblower. Known as the Cambridge Analytica scandal, it involved users' data from Facebook that had been compromised. Facebook

said in a statement on March 16 2018 that Cambridge Analytica received user data from Aleksandr Kogan, a lecturer at the University of Cambridge. Kogan reportedly created an app called "this is your digital life" that ostensibly offered personality predictions to users while calling itself a research tool for psychologists. The app asked users to log in using their Facebook accounts. As part of the login process, it asked for access to users' Facebook profiles, locations, what they liked on the service, and importantly, their friends' data as well.[11] The story of how whistleblower Christopher Wylie had built media mogul Steve Bannon's "psychological warfare tool" by harvesting millions of people's Facebook profiles had erupted across every news channel.[12] Wylie has called for data scientists and engineers to have "a professional code of conduct", that forces them to consider the ethical implications of everything they're doing. Wylie has also stated that one solution he'd like to see is more oversight and regulation to make users feel safe using the internet, the same way they do when "going to a doctor or getting on an aeroplane".[13] Hence, it becomes more important than ever to ensure that the long arm of the law is able to reach even the farthest reaches of cyber space.

LEGISLATIVE PROTECTION

Whistleblowers often faced difficulties whenever they proceeded to make disclosures. Realising this posed a big problem, many countries took certain and positive steps to end it. The USA is an interesting example, where whistleblowers are protected, by virtue of the Sarbanes-Oxley Act 2002. Some whistleblowers are also celebrated as heroes, for their fearless and selfless disclosures. Blowing the whistle in the USA is deemed an accepted part of the cultural landscape.[13] Johnson cites the reasons as being, among them, "changes in the bureaucracy which is more educated and professional, the wide range of laws that encourage whistleblowing, federal and state whistleblower protection, institutional support for whistleblowers, and a culture that often values whistleblowing".[14]

The Malaysian position in relation to whistleblowing initially seemed somewhat stagnant and docile, as compared to their more gregarious Western counterparts. This of course is to be expected, as Malaysia is still experiencing growth in this area. However, the whistleblowing landscape has drastically changed, courtesy of the Whistleblower Protection Act (WPA) 2010.

The WPA 2010 is primarily aimed at providing protection to whistleblowers who gave information of corrupt practices in the public and private sectors. In order to receive protection, it has to be ensured that the complaint is made to an officer of specific enforcement agencies. The five key enforcement agencies are the Royal Malaysian Police Force, Royal Malaysian Customs Department, Road Transport Department, Malaysian Anti-Corruption Commission and the Immigration Department of Malaysia. Other agencies include institutions such as the Securities Commission, Bursa Malaysia and the Companies Commission of Malaysia, which are of particular significance to whistleblowers from the corporate sector. Section 7 provides;

"A whistleblower shall, upon receipt of the disclosure of improper conduct by any enforcement agency under section 6, be conferred with whistleblower protection under this Act as follows: (a) protection of confidential information; (b) immunity from civil and criminal action; and (c) protection against detrimental action, and for the purpose of paragraph (c), the protection shall be extended to any person related to or associated with the whistleblower".

The full scheme of whistleblower protection begins with s 7 and ends with s 10. These areas of protection typically cover confidential information, immunity from civil and criminal action and protection against detrimental action. A 'detrimental action' includes:

a. "action causing injury, loss or damage;
b. intimidation or harassment;
c. interference with the law, employment or livelihood of any person including discrimination, discharge, demotion,

suspension, disadvantage, termination or adverse treatment in relation to a person's employment, career, profession, trade, or business or the taking of disciplinary action; and

d. a threat to take any of the actions referred to in paragraphs (a) to (c)". Section 10(1) and (2) of the WPA 2010 provides that;

1. "No person shall take detrimental action against a whistleblower or any person related to or associated with the whistleblower in reprisal for a disclosure of improper conduct;
2. A whistleblower may make a complaint to any enforcement agency of any detrimental action committed by any person against the whistleblower or any person related to or associated with the whistleblower".

If found guilty of such an offence s 10 (6) states that;

6. "Any person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding fifteen years or to both".

Although the WPA 2010 seems clear on its stand regarding whistleblowing, there exists some confusion. This is because Malaysia's Penal Code contains a provision that seems to go against the WPA 2010. Under section 203A (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". Meanwhile section 203A (2) states that "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".

As information of improper conduct can be acquired whilst in the course of duty, whether it is an officer of a public body or an officer of a private body, if it is read together with WPA 2010, this could lead to some confusion. Potential whistleblowers face another dilemma, one that is both ethical and legal, if they decide to blow the whistle

This paradox must be resolved, and the way in solving this would lie in the proposition that by blowing the whistle, whistleblowers would benefit many people. Whistleblowing must be promoted as a means to protect society, and although it seems to only refer to precluding confidential information from being disclosed, there is no official declaration that states so.

As whistleblowing becomes more widespread in Malaysia, careful consideration and understanding is essential in dealing with disclosures. These issues must be handled vigilantly and deftly, as cyber space is an ever revolving area. Extra care is needed in handling disclosures, in order to avoid uncertainty. As such, the rules and players may be different, but the game stays the same.

CONCLUSION

Increased recognition of the affirmative role that whistleblowing plays in promoting accountability and governance, has led many governments to legislate specific provisions to regulate whistleblowing disclosures. These legislations will also provide a much needed safety net, to protect sincere and honest whistleblowers from reprisals. Whistleblowers would feel more emboldened to blow the whistle if they are guided by their own personal morality, more than anything else. However, this scenario would be possible only when whistleblowing, as well as cyber whistleblowing, progressively becomes adequate, as the better alternative to anonymous disclosures. This work is supported by GGMP-2018-020

NOTES

[1] What Can be Done about Cyber Security Whistleblowers?, https://www.securityroundtable.org/what-can-be-done-about-cybersecurity-whistleblowers/, (accessed on 10/10/2020).

[2] Harjinder Singh Lallie, Lynsay A. Shepherd, , Jason R. C. Nurse, et. al., Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, https://arxiv.org/pdf/2006.11929.pdf, (accessed on 21/10/2020).

[3] Yar, Majid, & Steinmetz, Kevin, F., Cybercrime and Society, 3rd edition, Sage Publication, London, p. 11, 2019.

[3] Lombard, Sulette, Regulatory Policies & Practices to Optimise Corporate Whistleblowing: A Comparative Analysis, Springer Publication, Singapore, 2020, p. 5.

[4] Awner, Jonathan, L., & Dickins, Denise, Will There be Whistleblowers?, https://poseidon01.ssrn.com/delivery.php? (accessed on 21/10/2020).

[5] Hammer, Dallas, &Bundschuh, Evan, The Rise of Cybersecurity Whistleblowing, https://wp.nyu.edu/compliance_enforcement/2016/12/29/the-rise-of-cybersecurity-whistleblowing/, (accessed on 3/2/2020).

[6] Bellaby, Ross, W., The Ethics of Whistleblowing: Creating a New Limit on Intelligence Activity, Journal of International Political Theory, 2018, Vol. 14(1), p. 61.

[7] Pacella, Jenifer, M., The Cybersecurity Threat: Compliance and the Role of Whistleblowers, 11 Brook. J. Corp. Fin. & Com. L. 2016, , p. 40.

[8] Barry, William & Fleming, Brian, How to Manage Cyber-Whistleblower Risk, http://www.cfo.com/cyber-security-technology/2018/03/manage-cyber-whistleblower-risk/, (accessed on 3/2/2020).

[9] Sherr, Ian, 'Facebook, Cambridge Analytica and data mining: What you need to know', https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/, (accessed on 3/2/2020).

[10] Cadwalladr, Carole, 'Our Cambridge Analytica scoop shocked the world. But the whole truth remains elusive', https://www.theguardian.com/uk-news/2018/dec/23/cambridge-analytica-facebook-scoop-carole-cadwalladr-shocked-world-truth-still-elusive, (accessed on 3/2/2020).

[11] Janning, Finn, Khlif, Wafa & Ingley, Coral, The Illusion of Transparency in Corporate Governance: Does it Help or Hinder True Ethical Conduct?, Palgrave McMillian, Sweden, 2020, p. 27

[12] Collins, Katie, 'Chris Wylie: Blowing the whistle on Cambridge Analytica? Worth It', https://www.cnet.com/news/chris-wylie-blowing-the-whistle-on-cambridge-analytica-worth-it/, (accessed on 3/2/2020).

[13] Cheng, Xintong, Karim E, Khondkhar & Lin, Karen Jingrong, A Cross-Cultural Comparision of Whistleblowing Perceptions, Int. J. Management and Decision Making, Vol. 14, No. 1, 2015, p. 17

[14] Johnson, Roberta Ann, "Whistleblowing: When It Works and Why", Lynne Rienner Publishers, London, 2003, p. 4.

REFERENCES

Awner, Jonathan, L., & Dickins, Denise, Will There be Whistleblowers? https://poseidon01.ssrn.com/delivery.php? (accessed on 21/10/2020).

Barry, W. & Fleming, B. How to Manage Cyber-Whistleblower Risk, http://www.cfo.com/cyber-security-technology/2018/03/manage-cyber-whistleblower-risk/, (accessed on 3/2/2020).

Bellaby, R. W. 2018. The ethics of whistleblowing: creating a new limit on intelligence activity. *Journal of International Political Theory* 14(1): 61.

Cadwalladr, C. 'Our Cambridge Analytica scoop shocked the world. But the whole truth remains elusive', https://www.theguardian.com/uk-news/2018/dec/23/cambridge-analytica-facebook-scoop-carole-cadwalladr-shocked-world-truth-still-elusive, (accessed on 3/2/2020).

Cheng, Xintong, Karim E, Khondkhar & Lin, Karen Jingrong. 2015. A cross-cultural comparision of whistleblowing perceptions. *Int. J. Management and Decision Making*, 14(1): 17.

Collins, K. 'Chris Wylie: Blowing the whistle on Cambridge Analytica? Worthit',https://www.cnet.com/news/chris-wylie-blowing-the-whistle-on-cambridge-analytica-worth-it/, (accessed on 3/2/2020).

Hammer, D. & Bundschuh, E. The rise of cybersecurity whistleblowing. https://wp.nyu.edu/compliance_enforcement/2016/12/29/the-rise-of-cybersecurity-whistleblowing/, (accessed on 3/2/2020).

Harjinder Singh, Lallie, Lynsay A. Shepherd, Jason R. C. Nurse, et. al., Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, https://arxiv.org/pdf/2006.11929.pdf, (accessed on 21/10/2020).

Janning, F., Khlif, W. & Ingley, C. 2020. *The Illusion of Transparency in Corporate Governance: Does it Help or Hinder True Ethical Conduct?* Sweden: Palgrave McMillian.

Johnson, R. A. 2003. *Whistleblowing: When It Works and Why.* London: Lynne Rienner Publishers.

Lombard, S. 2020. *Regulatory Policies & Practices to Optimise Corporate Whistleblowing: A Comparative Analysis*. Springer Publication.

Pacella, J. M. 2016. *The Cybersecurity Threat: Compliance and the Role of Whistleblowers*. 11 Brook. J. Corp. Fin. & Com. L.

Sherr, I. 'Facebook, Cambridge Analytica and data mining: What you need to know', https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/, (accessed on 3/2/2020).

What Can be Done about Cyber Security Whistleblowers? https://www.securityroundtable.org/what-can-be-done-about-cybersecurity-whistleblowers/, (accessed on 10/10/2020).

Yar, Majid & Steinmetz, K. F. 2019. *Cybercrime and Society*. 3rd edition. London: Sage Publication.

Hazlina Shaik Md Noor Alam
Pensyarah Kanan
Fakulti Undang-undang
Universiti Kebangsaan Malaysia
43600 Bangi, Selangor
Emel: hazlinashaik@ukm.edu.my