Developing or Reviewing Information Security Policies Using an Ethics-Based Algorithm

Information security focuses on data. It aims to control access to the data and safeguard them from corruption, compromise or loss and defend them against threats that may be internal or external and malicious or accidental. An information security policy (IS policy) is a subset of an organizational policy that guides the principles and actions taken to protect enterprise information against threats and prevent attacks by malicious parties.[1] In addition, the code of conduct, which encapsulates the gist of the policy and sets internal standards, is a handy reference for frontline operating staff including nonprivacy professionals.[2, 3] A workable and enforceable security policy is crucial, and a code of conduct is of equal importance. An effective and pragmatic code of conduct can help guide frontline risk specialists and lessen the weight of their burden.

Achieving adequate information security requires not only appropriate hardware and software infrastructures, but, more important, staff with hard competencies (e.g., skills and knowledge) and soft competencies (e.g., a fair and just mind) to use the hardware and software, along with an approach to meet these needs. This approach should include data protection, data security and data privacy protection.

Developing and reviewing enterprise IS policies and deriving a code of conduct is necessary and urgent due to chronic data protection problems, the shortcomings in the concepts that guide management and influence the formation of the policies or strategies, and the lack of policies or the use of policies that are insufficient or dated. The way forward is to find an approach to address these shortcomings using the proposed ethics-based algorithm.[4]

Why Policies Should Be Developed and Reviewed

Many organizations lack a formal IS policy. Those that do have one are often inadvertently following principles that are invariably dated, limited and inadequate due to the advancement of technologies and changes in enterprise practice and laws. In addition, policy statements are often vague and not user-friendly, making them difficult to follow for stakeholders. This can lead to policies being forgotten or ignored.

Existing IS policies tend to focus mainly on tangible technical efficiency, financial viability and legal admissibility and include, in some cases, corporate social responsibility (CSR), return on investment (ROI), market share and profit margin. The weaknesses are inherent due to two factors. The first is that professionals are nurtured under problematic influences: the misinterpretation of risk; the flawed curricula across science and technology;[5] and the Simon doctrine, the concept of bounded rationality. A key assertion of Simon's theory is that decision-making is a rational behavior, which begets the assumption of rationality in decision-making.[6] The second is that policies often fall short when dealing with issues of ethics in post-implementation and post-contract situations that IT professionals face daily.

WANBIL W. LEE | DBA

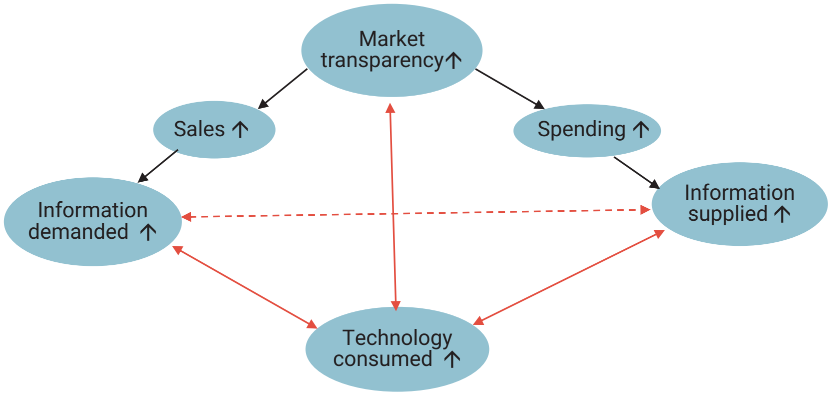
Is a cyberethics evangelist. He is president and founder of the Computer Ethics Society and is principal of Wanbil and Associates. He has five decades of experience in computing. He teaches information security and cyberethics to under- and postgraduate students, and he researches, consults and publishes in these areas. He has written more than 100 journal articles and conference papers.

An important reason that policies need to be developed and reviewed is the existence of the chain reaction of the circular technology-dependent information-intensive effect: Increases in the supply and demand of information; the consumption of technology; the use of energy; and finance, sales and spending culminate in the chronic data protection problem, a reflection of ongoing big spending and nonstop data protection against ever more sophisticated and ubiquitous cyberattacks and their negative consequences, forming a vicious circle (**figure 1**).[7] The expected growth of market share, the planned level of consumer satisfaction and the anticipated staff morale boost justify the individual and collective return on investment (ROI) in technology. When the organization survives, the targeted stakeholders reap the benefits. Consequently, huge volumes of data are generated and more technologies are used, creating cybersecurity concerns such as leaking of confidential and sensitive information, breaching of personal and enterprise data privacy, and an adversarial impact on the environment, such as increased consumption of energy and other resources, including carbon and paper, which can affect pollution and climate change. This consequence amounts to a multidimensional problem involving technical, financial, legal, ethical, social and ecological factors (the so-called hexa-dimension requirement).

This vicious circle effect means that as the marketplace becomes more transparent, business improves and more information is needed, and customers who are better informed become happier and tend to buy more; but at the same time, they demand more information. When organizations need more information to satisfy customer needs, they use more technology to generate more information and must manage increasingly larger volumes of information. In addition, this effect reflects a weak security policy and an insufficient understanding of the concepts and theories that guide management and influence policy formation. These concepts and theories are rationality-based and treat risk and damages primarily in financial terms. However, in reality, decision-making behavior is not always rational. People may feel differently toward problems and form solutions as individuals rather than as employees.[8] Contemporary problems are more than financial; they can be legal, technical, ethical, social and environmental. Plainly, existent countermeasures fail and problems persist, as the chronic data protection problem exemplifies.

FIGURE 1

Core Topics of Social Responsibility



Source: Adapted from Lee, W. W.; "Hexa-Dimension Code of Practice for Data Privacy Protection," *Encyclopedia of Information Science and Technology, 4th Edition*, IGI Global, USA, 2018, *https://www.igi-global.com/chapter/hexa-dimension-code-of-practice-for-data-privacy-protection/184194*

Why Better Policy Development and Review Are Urgent Needs

The increases in the incidence of cybersecurity and data privacy issues have intensified security and ethical concerns, as they extend beyond individuals and organizations to governments. In response to the big data dilemma, which can jeopardize the national economic welfare, the UK government established a data ethics council based on a proposal by the UK House of Commons to advocate for more urgency on data privacy.[9, 10, 11]

Also, security is becoming an important market differentiator, especially when there is no real product-based competitive edge.[12] Unfortunately, frontline information security personnel are forced to bear the brunt of the work, and they are in dire need of pragmatic guidance on how to meet organizational needs.

Understanding the Proposed Algorithm

An algorithm was proposed as a suitable approach to deal with these shortcomings.[13] As described in the *ISACA® Journal* article, "An Ethics-Based Algorithm for Governing Data Ethics,"[14] the algorithm comprises two components: the hexa-dimension metric and the ethical matrix. It aims to gain a view of the ethical issues arising with a problem such as shortcomings in IS policy, before proceeding to assess the hexa-factors.

Initially conceived as a checklist for decision-making in a technology-dependent and information-intensive context, the hexa-dimension metric provides decision makers with an idea of the quality or trustworthiness of the decision, action or policy. It can also be used for privacy protection policy formulation and the determination of pragmatically ethical and effective leadership. Note that on ethical and effective leadership, having values such as care, justice, integrity and respect is necessary but not sufficient. Values are the raw material of ethical leadership, and ethical reasoning, a production process to convert them into effective actions in complex and dynamic situations, is required.[15, 16] Hence, neglecting ethics tarnishes leadership quality; a tarnished leader is no good, thus not effective. Further, the hexa-dimension metric can serve as the basis for developing a code of practice or enterprise charter for ensuring and enhancing IS policies. The six factors/principles that make up the metric are:

1. Financial viability
2. Technical effectiveness
3. Legal validity
4. Ethical acceptance
5. Social acceptability
6. Ecological sustainability

The ethical matrix is a two-dimensional mathematical structure, originally developed as a decision-support tool for helping users reach sound judgments or decisions about ethical acceptability and optimal regulatory legal and technical controls for the field of food and agriculture.[17] The rows in the matrix identify the stakeholders or interest groups, which can be human or nonhuman entities, affected by the actions taken or decisions under consideration, including, for example, customers, providers and their employees, organizations and communities, animals and the environment. The columns of the matrix illustrate the ethical principles or values applicable to the interest groups (stakeholders) relevant to the issue in question, for example, the job security of employees in a project that may lead to a retrench of human resources. The stakeholders' concerns regarding the principles that would be met with regard to each ethical principle are recorded in the cells. Where a stakeholder has no concern about an issue under consideration with respect to a certain principle, the cell is empty. The number of columns may vary in accordance with the issue. The number of rows and columns varies depending on the problem. The matrix has been adapted to the other fields including IT. In this context, the matrix plays the role of a decision-support tool, helping provide users of the metric with a holistic view of the ethical issues arising in the problem of interest.

> The hexa-dimension metric can serve as the basis for developing a code of practice or enterprise charter for ensuring and enhancing IS policies.

The ethical matrix algorithm and the hexa-dimension metric algorithm are derived by operationalizing the ethical matrix and the hexa-dimension metric, respectively. The ethical matrix algorithm consists of seven steps, and the hexa-dimension metric algorithm consists of five steps. These steps can be applied and demonstrated in a sample case study.

Example Case Study

A fictional consulting assignment can be used to exemplify and echo the reasons for developing or reviewing an IS policy, the Meta-Alpha Corporation (Meta-Alpha) is a multinational, multi-industry enterprise headquartered in Hong Kong, China. Its operations span more than a dozen countries and it conducts a diversified range of business, including supplying power, mining operations; operations retail outlets including gas stations, convenience stores and supermarket chains; and providing software development and related services such as the Octopus card (which caught the attention of the worldwide media when it was involved in a scandal selling customers' private data[18]). Meta-Alpha has an enterprisewide ethics and IS policy. The policy features a three-level commitment to data governance that requires board members, executives and employees to avoid the intent and appearance of unethical use of customer data; to not compromise the policy for any reason; to not tolerate using the data to harass, discriminate or exploit clients, suppliers and partners; and to safeguard enterprise trade secrets and technical information.

With regard to the use of private data in electricity accounts:

- The chief executive officer (CEO) sold the customers' private data to third parties such as politically-oriented interest groups, online business

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

The matrix plays the role of a decision-support tool, helping provide users of the metric with a holistic view of the ethical issues arising in the problem of interest.

operators, and newspaper and periodical magazine distributors, which brought an income of more than HK$50 million to the enterprise and made the data available to subsidiaries and partners.

- The chief engineer monitored the accounts and deduced from them the data that were being consumed (i.e., when lights were on and for how long, when a television (TV) was on, how long appliances such as toasters and electric stoves were used, how many TVs and phones were in the household). The chief engineer claimed that this data would facilitate planning power generation and future development.
- The marketing department was tempted to use the information extracted from the data to predict race or ethnicity, marital status or family composition.
- The CEO claimed that the enterprise had done nothing wrong since selling data had become commonplace. The enterprise had a duty to run a profitable operation, and the revenue from the sales of the data went to enterprise profit, which was a positive return to shareholders. The CEO remained at the enterprise for a time but eventually resigned.
- The chairman of the board of directors announced that the enterprise decided to donate all of the HK$50 million to charity in the name of Meta-Alpha and eventually stepped down.
- The Hong Kong Office of the Privacy Commissioner for Personal Data decided to investigate and prosecute.

The legislators rebuked Meta-Alpha, charging, "You treat, I pay," a Cantonese-speaking Hong Kong saying people use to express their displeasure at being taken advantage of or treated unfairly. They said that Meta-Alpha was not a charitable donor and that clients were exploited, and their trust betrayed. They demanded Meta-Alpha refund all proceeds to the clients affected and undertake an independent investigation into the affair to be led by a judge.

The enterprise, the chairman and the CEO acted in contradiction to the enterprise's IS policy, which forbade unethical use of customer data, specifically the exploitation of customers. They compromised the enterprise's rules and regulations and violated the basic ethical principle known as the Golden Rule—Do unto others as you would have them do unto you—since the CEO would likely not want her own personal data to be made available to a bank to be sold or used for something other than the agreed-on purposes.

Account holders who innocently supplied their personal data when opening an account were exploited and cheated, which is why the chairman's claim to donate the money to charity in the name of Meta-Alpha attracted the legislators' rebuke. Selling the data to bring in extra income and using the data reviewed by the chief engineer to facilitate engineering planning, installation maximization and control of supply (hoping for improvement, thus reducing consumer burden) violates the categorical imperative. It may be tolerable in terms of consequentialism (i.e., an action is morally right if its consequences are beneficial or morally wrong if its consequences are harmful) but can raise questions from the perspective of utilitarianism (i.e., an action is morally wrong if its harmful results are greater than its beneficial results). The marketing department's thinking was dangerous. Its actions were not only intolerably unethical, but blatantly illegal.

By insisting that the organization had done nothing wrong, the CEO fell into the trap of misdirection, leading herself to believe in the fallacy that if it is not illegal, it is ethical. The organization claimed that since many enterprises sell data, then they should be able to as well. This is a relativistic argument. Yet, the claim shows no evidence that selling personal data without prior consent is ethical, since such an argument is based on a fallacious belief that an action must be ethical if a large number of people are doing it. The CEO argued that the enterprise owed the shareholders a duty to make a profit and executives owed themselves the duty to secure their job.

The chief engineer may have been wise to make use of big data as the information derived might have been helpful in economizing planning, such as facilitating a plan to cut costs and time. However, his action violated the terms of the Hong Kong Personal Data (Privacy) Ordinance (PDPO), which states that the data collected must not be used for unauthorized purposes.[19] The data are only to be used for accounting pertaining mainly to payment, not for engineering planning. Further, the possibility of preventing an increase in the price of electricity was uncertain.

Ethical issues are invariably complex, interweaved and counteracting or contradicting.

In sum, the consequences might have been good, but for whom? After all, the proceeds from selling the data benefitted the CEO and perhaps the enterprise and shareholders, but not the account holders and the rest of the population. The chief engineer and the marketing team should have considered the consequences of their actions. In particular, the CEO cheated cardholders and used them for her own gain. In addition, the CEO acted against the Golden Rule. Lastly, collecting personal data inconsistent with the purpose for which they were acquired and selling them without the data subjects' consent was not ethical. Ethical issues are invariably complex, interweaved and counteracting or contradicting. The ethical matrix is a tool that can help sort these issues out. It provides an overview of ethical issues arising from an action through a list of stakeholders and the values or principles they hold or respect against an ethical view.

Applying the Ethical Matrix Algorithm

This algorithm is based on the ethical matrix, which is a decision-support tool to provide a holistic view of the ethical implication of an action or decision. The matrix was originally designed for the field of food and agriculture[20] and adapted to information and communications technology applications.[21] It comprises four factors or key variables and seven steps. The steps are:

1. Assemble the group of decision makers.
2. Determine the stakeholders.
3. Determine the principles that the stakeholders respect.
4. Fill the cells of the matrix.
5. Estimate the factors.
6. Compute the factors.
7. Interpret the results to draw a conclusion.[22]

The factors are R-weight (the importance of principle to the issue being considered), C-weight (the degree of respect that stakeholder attach to a principle), S-stakeholder (the number of stakeholders) and S-principle (the number of principles). Applying the algorithm returns a matrix (**figures 2, 3** and **4**), and a conclusion can be drawn from the matrix.

FIGURE 2
Ethical Matrix

Respect for Stakeholders	Well-Being	Autonomy	Justice/Fairness
CEO	Job security; achievement	Performance as CEO; a clear conscience	Not stepping over the limit of authority
Chief engineer	Professional reputation; enterprise support	Performance as chief engineer	An envy-free share of financial support for engineering activity
Marketing	Improving promotion prospects	Independence from accounting and production constraints	An envy-free share of financial support for marketing activity
Account holders	Enjoyment of benefits	Materialization of the benefits; security of personal data	Fair, *prima facie*
Shareholders	Profit and return on investment (ROI)	Performance monitoring; enterprise reputation	Meeting a set profit margin
The enterprise's subsidiaries and partners	Achievement record	Independence	N/A
Regulators	Fair and proper trading	N/A	Fair and proper trading

FIGURE 3

D-Weight

Respect for Stakeholders	Well-Being	Autonomy	Justice/Fairness
CEO	5	5	5
Chief engineer	3	4	5
Marketing	3	4	5
Account holders	5	3	5
Shareholders	4	5	5
Subsidiaries and partners	4	4	5
Regulators	3	0	5

FIGURE 4

Products (I-Weight x D-Weight) and Sums

Respect for Stakeholders	Well-Being	Autonomy	Justice/ Fairness	∑Stakeholder
CEO	5 x 5 = 25	5 x 5 = 25	5 x 5 = 25	75
Chief engineer	5 x 3 = 15	5 x 4 = 20	5 x 5 = 25	60
Marketing	5 x 3 = 15	5 x 4 = 20	5 x 5 = 25	60
Account holders	5 x 5 = 25	5 x 3 = 15	5 x 5 = 25	65
Shareholders	5 x 4 = 20	5 x 5 = 25	5 x 5 = 25	70
Subsidiaries and partners	5 x 4 = 20	5 x 4 = 20	5 x 5 = 25	40
Regulators	5 x 3 = 15	5 x 0 = 0	5 x 5 = 25	40
∑Principle	135	125	175	

FIGURE 5

Hexa-Dimension Metric

The Measures	Verdicts	Check
Financial viability	Extra income is financially viable for the CEO, the enterprise and shareholders, but not at the expense of the participants.	√
Technical effectiveness	This is not a technical issue; thus, not applicable.	√
Legal validity	There is no *prima facie* evidence of illegal action.	√
Ethical acceptability	Data collection and data use ethically questionable; unacceptable.	√
Social desirability	This is questionable in a utilitarian view.	√
Ecological sustainability	This is not an ecology issue; air pollution or climate are nonissues; thus, not applicable.	√

In this example, the CEO's S-stakeholder suggested to the decision makers that the CEO was a dutiful worker who was concerned about optimizing the profit for the enterprise. The CEO's main concern was job security. Finding a way to improve or bring in a profit is natural and acceptable. However, the method of doing so must be consistent with ethical principles. The CEO fulfilled the duty of the office and did nothing illegal, but took actions that disobeyed the Golden Rule. This raises the issues of responsibility and rights: Should the chief executive not bear a certain responsibility? Was the CEO in a position to complain about being cheated? At the end of the day, it may have been a matter of conscience with respect to selling the account holders' personal data that led the CEO to leave the enterprise. Furthermore, both the chief engineer and the marketing department were also dutiful. All stakeholders were keen to see that the enterprise was fair and just.

Applying the Hexa-Dimension Metric Algorithm

This algorithm is based on the hexa-dimension metric, which is a decision-support tool in the form of a checklist. Its purpose is to provide a measure of the quality and efficacy of the consequences of actions, decisions or policies in terms of six factors, prompted by extant decision-making models, including the Simon model, which assumes rationality and focuses on physical and financial terms. It is expected that the metric serves as a good instrument not just for privacy protection policy formulation, but also for determining pragmatically what is ethical and effective in leadership, for which all professionals strive. It has four major key variables (λ, I-weight, S-weight and β-value) and is made up of five steps:

1. Assemble the group of decision makers
2. Determine the number of applicable principles (λ). (Not all principles are applicable in all cases.)
3. Assign and compute the factors—I-weight (the relative importance of each attribute/principle with respect to the case under study, expressed as a percentage), and S-weight (the actual or estimated satisfaction level for the outcome of the decision to achieve).
4. Compute the β-values, that is, the Coefficient of Success, planned (βp) and actual (βa) using the Wβ-Equation: $\beta = \{\sum [(I_i/I_s) + \varepsilon] + [S_i \text{ x } S_s]\}/2\lambda, i = 1, \ldots, \lambda$.

5. Interpret the results to draw a conclusion.[23] Applying the algorithm returns a metric (**figures 5** and **6**) and a conclusion can be drawn from the metric.

In this example, the difference between the planned and actual value using the equation[24] is close to 20 percent and significant, which indicates that the Meta-Alpha personnel used customers' data unethically and perhaps illegally, and it implies a neglect of the enterprise's IS policy. Thus, the IS policy must be reviewed with the aim to detect and rectify weaknesses and enforce effective execution of the policy.

FIGURE 6

The R-Weight and S-Weight Assigned by the Group

Attributes	R-Weight (Rank/ Importance)	S-Weight (Satisfaction Level)	
		Planned	Actual or Estimated
Financial viability	5	90 percent	90 percent
Technical effectiveness	3	100 percent	100 percent
Legal validity	5	100 percent	30 percent
Ethical acceptability	5	80 percent	20 percent
Social desirability	5	80 percent	20 percent
Ecological sustainability	3	50 percent	50 percent

> It is essential for enterprises to develop an IS policy, but it is just as important for enterprises that already have one to actively review it and ensure that it is effectively enforced.

Conclusion

In the current cybersecurity landscape, developing or reviewing IS policies is necessary and urgent. It is likely that there are still organizations lacking an IS policy, that existent policies are not complied with or effectively enforced, or that they need updating. Information security professionals are in urgent need of effective and pragmatic guidance for the frontline information security staff. Expenditures for countermeasures to ensure data security and protection, along with the cost of damages due to cyberattacks, are ever increasing. The change of technologies from traditional to data-transformative, and the *modus operandi* from a large-scale, stand-alone, single-site to a technology-driven, information-intensive environment render the information security function more complicated, due to new sociotechnological risk. Data privacy protection has become a primary concern as privacy infringement occurs more frequently and leads to potentially devastating consequences to individuals, enterprises and governments.

In the case of the example case study, the moral dilemma prompted the organization to make several changes. The enterprise made an effort to promote its code of conduct to cultivate an ethical organization. Each employee was issued a copy of the enterprise's code of conduct; an additional item was added to the annual staff performance review to seek evidence of knowledge of the enterprise's code of conduct and the ethical use of information; and awards were created to recognize job performances of ethical merit. The organization also restructured its IT department, elevating the chief information security officer (CISO) to equal status with the chief information officer (CIO), and created a chief ethics officer position within its legal department.

It is essential for enterprises to develop an IS policy, but it is just as important for enterprises that already have one to actively review it and ensure that it is effectively enforced.

Endnotes

1. Lee, W. W.; "An Ethics-Based Algorithm for Governing Data," *ISACA® Journal*, vol. 6, 2022, *https://www.isaca.org/archives*
2. Lee, W. W.; "Hexa-Dimension Code of Practice for Data Privacy Protection," *Encyclopedia of Information Science and Technology, 4th Edition*, IGI Global, USA, 2018, *https://www.igi-global.com/chapter/hexa-dimension-code-of-practice-for-data-privacy-protection/184194*
3. Lee, W. W.; "Hexa-Dimension Metric, Ethical Matrix, and Cybersecurity," *Encyclopedia of Information Science and Technology, 5th Edition*, IGI Global, USA, 2021, *https://www.igi-global.com/chapter/hexa-dimension-metric-ethical-matrix-and-cybersecurity/260203*
4. *Op cit* Lee 2022

[5] Lee, W. W.; "Ethical Computing," *Encyclopedia of Information Science and Technology, 3rd Edition*, IGI Global, USA, 2015, *https://www.igi-global.com/chapter/ethical-computing/112723*

[6] Simon, H. A.; *Administrative Behaviour, 3rd Edition*, The Free Press, USA, 1976

[7] *Op cit* Lee 2018

[8] Barnard, C. I.; *The Functions of the Executive,* Harvard University Press, USA, 1971, *https://www.hup.harvard.edu/catalog.php?isbn=9780674328037&content=toc*

[9] UK House of Commons Science and Technology Committee, *The Big Data Dilemma*, UK, 12 February 2016, *https://publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf*

[10] McKenna, B.; "House of Commons Science and Technology Committee Calls for Data Ethics Council," *Computer Weekly*, 12 February 2016

[11] McKenna, B.; "Government Accepts Data Ethics Council Proposal," *Computer Weekly*, 28 April 2016

[12] Langford, T.; "Security a Serious Market Differentiator Says Publicis CISO," *Computer Weekly*, 12 May 2016

[13] *Op cit* Lee 2022

[14] *Ibid*.

[15] Wood, R.; "What Is Ethical Leadership," University of New South Wales, Kensington, Australia, 2018, *https://www.wgu.edu/blog/what-is-ethical-leadership2001.html*

[16] Wood, R.; "Ethical Leadership Framework," University of New South Wales, Kensington, Australia, 2009

[17] Mepham, B.; M. Kaiser; E. Thorstensen; S. Tomkins; K. Millar; *Ethical Matrix Manual*, Landbouw-Economisch Institut (LEI), Netherlands, 2006

[18] South China Morning Post (SCMP), "Octopus Sold Personal Data of Customers for HK$44M," 27 July 2010, *www.scmp.com/article/720620/octopus-sold-personal-data-customers-hk44m*

[19] Office of the Privacy Commissioner for Personal Data, Hong Kong, "The Personal Data (Privacy) Ordinance," Hong Kong, China, 1996, *https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html*

[20] *Op cit* Mepham *et al.*

[21] *Op cit* Lee 2015

[22] *Op cit* Lee 2022

[23] *Ibid*.

[24] *Ibid*.