ASIA PACIFIC LAW REVIEW
2020, VOL. 28, NO. 1, 69–96
https://doi.org/10.1080/10192557.2020.1786252

Routledge
Taylor & Francis Group

Hong Kong's data breach notification framework — inadequacies and corrective actions required

Rebecca Ong

School of Law, City University of Hong Kong, Hong Kong SAR, China

ABSTRACT

Data breaches resulting from information security failures continue to be a matter of pressing concern. Given the increasing number of compromised data security incidents globally, data breach notification has emerged as an issue of increasing urgency. In response, breach notification laws have been enacted to ensure individuals are appropriately informed when their personal identifiable information (PII) has been compromised, so as to enable affected individuals to mitigate any harm so arising. Mandatory data breach notification laws are an important development in this regard. Such laws mandate that an organization that has suffered a data breach involving personal identifiable information shall notify affected individuals and in some cases, regulators. This article argues that for Hong Kong to maintain its rightful place across international norms, as a modern, legally and commercially trustworthy and reliable jurisdiction, and at the same time continues to assure its citizens that the confidentiality of their PII is secure, a mandatory approach to data breach notification needs to be implemented.

ARTICLE HISTORY
Received 27 December 2019
Accepted 23 March 2020

KEYWORDS
Data breach; elements of data breach notification; critiques of notification law; deficiencies of Hong Kong existing framework

I. Introduction

Today, virtually all of an organization's or company's daily transactions and key records are created, used, shared and stored in digital form (hereafter 'e-data') using networked computer technology. Corporate and organizational practices as well as consumer economic behaviours, are being increasingly described, managed and recorded in information technology systems, and as a consequence vast amounts of corporate proprietary information and consumers' personal identifiable information (PII) are being systematically accumulated into organizational repositories. Such repositories are patently valuable given both the confidential nature of their content and the potential for their use in consumer profiling, client acquisition and marketing purposes, to name but three. The increasing dependence on e-data and ever expanding data repositories in a networked interconnected environment, however, exacerbates potential vulnerabilities that can result in major harm to organizations and companies. Clearly, unless organizations have in place strong data security measures, society faces a new set of harms related to any breaches

CONTACT Rebecca Ong lwong@cityu.edu.hk School of Law, City University of Hong Kong, Hong Kong

of repository content, whether occurring accidentally or maliciously — such harms occurring at different levels of social ecology, namely, confidentiality harms, integrity harms and availability harms.[1] At the societal level, fraud resulting from these harms can spawn billions of dollars in economic loss and burdens both market places and the legal system as a whole. On the interpersonal level, the harms erode commercial trust; on the individual level, the harms hinder commercial identity development for corporate entities, organizations and consumers.[2]

The United States (US), the European Union (EU) and Australia, to name but three jurisdictions have responded by developing data breach notification laws that encompass elements of privacy law, corporate governance and information security law.[3] The first data breach notification law, implemented in California in 2003[4] requires any California business which has suffered a data breach of *unencrypted* computerized[5] personal information to notify Californian residents about the breach. In most cases, individuals affected by a data breach must be notified within a stipulated time frame or without reasonable delay. Organizations may however delay notification where the notification may impede a criminal investigation. The law had a seismic effect in exposing the number and scale of data breaches involving corporations.

The Californian Civil Code §1798.29(a)[6] and §1798.82(a)[7] have since been widely used as a model by other US state legislatures although there are variations between different state-based laws. For example, state laws differ as to, inter alia, how personal information is defined, what triggers notification, whether an investigation on the data breach is required to determine whether affected individuals need to be notified, whether a law enforcement agency and/or credit reporting agency must be notified, the timing of notification and the penalties for non-compliance.[8] It is worth noting that aside from the state laws on data breach notification, there are some sector-specific federal privacy-related laws such as the Federal Trade Commission Act (FTC Act),[9] the Gramm-Leach Bliley Act[10] and the Health Insurance Portability and Accountability Act (HIPAA).[11]

---

[1] Andrea M Matwyshyn, 'Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation' (2005) 3 Berkeley Business Law Journal 129 <https://pdfs.semanticscholar.org/d606/72cab2afa2bbe8c0b9b8057c62f3775b2976.pdf> accessed 20 July 2019.

[2] Ibid.

[3] Thomas J Smedinghoff, 'Trends in the Law of Information Security' (2005) 17(1) Intellectual Property & Technology Law Journal 1.

[4] Californian Civil Code §1798.29(a) and §1798.82(a) <https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29> and <https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82> accessed 22 July 2019.

[5] It is worth noting that while the laws mainly relate to computerized data, some states, for example, Georgia, Maryland, Massachusetts, New York and Utah, include personal information held in written or other forms, thereby covering a broader scope of data for which notification must be given. For example, Massachusetts defines data as any material upon which written, drawn, spoken, visual, or electro-magnetic information or images are recorded or preserved, regardless of physical form or characteristics. See Massachusetts General Law Annotated Ch 93H, §1-6.

[6] Californian Civil Code (n 4).

[7] Ibid.

[8] Mark Burdon, Bill Lane and Paul von Nessen, 'The mandatory notification of data breaches: Issues arising for Australian and EU legal developments' (2010) 26 Computer Law and Security Report 115, 116.

[9] FTC Act <https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act> accessed 30 August 2019.

[10] Gramm-Leach Bliley Act (Privacy of Consumer Financial Information) <https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf> accessed 30 August 2019.

[11] Health Insurance Portability and Accountability Act (HIPAA) <https://www.ncbi.nlm.nih.gov/books/NBK500019/> accessed 30 August 2019.

Data breach notification laws have also been implemented in the EU and Australia via the General Data Protection Regulation (GDPR)[12] and the Privacy Amendment (Notifiable Data Breaches) Act 2017[13] respectively. In contrast to the US's sectoral-based laws, the comprehensive data protection laws under the EU's GDPR[14] and Australia's Privacy Act[15] provide a stronger level of protection of data. Under the GDPR, there are two different levels of notifications, the first, where the breach is likely to lead to 'a risk for the rights and freedoms of the individuals' and the second, where the breach is likely to lead to 'high risk to the rights and freedoms of the individuals'. Only the latter requires notification to affected individuals.[16] A data breach must be reported without undue delay and where feasible, not later than 72 hours to the supervisory authority after having become aware of the breach.[17] Where the breach is not reported within 72 hours, an explanation must be provided. A request from the law enforcement authority suffices as an explanation. As with the Californian law, there is no obligation to notify however where for example, the data were protected by technical and organizational measures (i.e. the data was encrypted).[18]

In Australia, not all data breaches require notification; the obligation to notify[19] only comes into play when individuals whose personal information was involved in any data breach was likely to result in *serious harm* (referred to as eligible data breaches). Determining whether the breach is likely to cause serious harm requires an assessment of the suspected data breach. This requires a determination of the type of information involved, its sensitivity, whether the information was protected by security measures, who might have obtained the information, the possibility those persons could have circumvent the security technology or the methodology used to protect the information and the nature of the harm.[20] Situations where the obligation to notify is not necessary include: (a) where data breaches are notified under Section 75 of the My Health Records Act; (b) where an enforcement body believes on reasonable grounds that notifying individuals would be likely to prejudice an enforcement-related activity conducted by, or on behalf

[12] See GDPR, art 33(1) <https://gdpr-info.eu/art-33-gdpr/> accessed 30 August 2019.

[13] Australia's Privacy Act 1988 (Cth) was amended by the Privacy Amendment (Notifiable Data Breaches) Act 2017 to establish a regime for mandatory notification of eligible data breaches.

[14] In addition to the GDPR, data breach notification provisions under other EU directives continue to apply. For example, breach notification provision for telecoms operators and Internet service providers as set out in Regulation 611/2013 under the e-Privacy directive. Data breach notifications are also required under: (a) EU Directive 2016/680 on the processing of personal data by competent authorities relating to areas of judicial cooperation in criminal matters and police cooperation; and (b) the Security of Network and Information Systems Directive (SNISD) 2016/1148.

[15] Australia's Privacy Act regulates the handling of personal information about individuals (natural persons) that includes the collection, use, storage and disclosure of this information, as well as access to and correction of personal information. The Act contains the Australian Privacy Principles (APPs), which comprise obligations as regards personal information that bind Commonwealth agencies and large private companies. See Angela Daly, 'The Introduction of Data Breach Notification Laws in Australia: A Comparative View' (2018) 34 Computer Law and Security Review 477.

[16] GDPR, art 34(1).

[17] Ibid, art 33(1).

[18] Other circumstances where notification is not necessary under the GDPR are where the controller had taken measures that would ensure that the high risk to the rights and freedoms of the individuals is no longer likely to materialize; or when it would involve a 'disproportionate' effort, in which case controllers can make a public communication. See GDPR, art 34(3).

[19] The obligation to notify applies to government agencies, businesses and not-for-profit organizations with an annual turnover of AU$3 million or more, credit reporting bodies, health service providers, and tax file number recipients. See Office of Australian Information Commissioner, 'Notifiable Data Breach Scheme' <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme> accessed 22 July 2019.

[20] Notifiable Data Breaches Act, s 26WG.

of, the enforcement body;[21] and (c) where a Commonwealth law prohibits or regulates the use or disclosure of information (a secrecy provision).[22]

It can be seen from the brief overview of data breach notification laws in the US, the EU and Australia above that the laws have become increasingly more comprehensive and detailed than when it was first promulgated in California. Notwithstanding, it is apparent that the underlying objective of these laws was to provide a degree of protection to individuals affected by a data breach by giving them an opportunity to mitigate themselves from harms flowing from the breach.

In October 2018, Hong Kong was disturbed by an admission from Cathay Pacific Airways Limited of an unauthorized access to their repository of personal data of almost ten million of its customers. The airline reassured that confidential customer profile data were not successfully harvested, that only a handful of credit cards were actually exposed, and then too, absent any of their critical identifying data (e.g. their Card Verification Value digits (CVVs)). What was most disturbing however was that the breach had occurred and was detected much earlier in 2018, Cathay taking over seven months to make the admission. What was Hong Kong's response to this data breach that had attracted significant media attention in Hong Kong and elsewhere? To date, there has been very little research done on data breach notification in Hong Kong. This article fills the gap by examining data breach notification in the Hong Kong context.

The structure of this article is as follows. Part II looks at the phenomenon of data breaches, its impact in terms of consequences and cost of data breach, the potential value of stolen data, and recent data breach incidences in Hong Kong. Part III follows with an evaluation of essential elements for data breach notification. The article then deals with the data breach arena in Hong Kong, examining Hong Kong's data protection framework and its deficiencies (Part IV). It proceeds with critiques of notification law (Part V) and concludes at Part VI with recommendations as to the changes deemed appropriate.

II. Data breaches

Data breaches (also known as data 'spills' or 'leaks') are unauthorized access to and disclosure of sensitive personal, corporate or organizational information, by an individual, group or information technology system, such access being either accidental or maliciously intentional.

Examples of malicious incidents include the intentional unauthorized access to personal information by hacking into computer systems or networks, and theft of laptops and data storage devices by employees or external parties, while the loss of laptops, or devices that store data are deemed incidents unintentional or accidental. Unintentional incidents can also include failure to dispose of PII securely such as the improper shredding of confidential documents or mistakenly providing personal information to the wrong person (human error).[23] Although protection for individuals in so far as data breaches

[21] Ibid, s 26WN. Although the enforcement body may still be required to provide a statement to the Commissioner. See Office of Australian Information Commissioner, 'Notifiable Data Breach, Exceptions to Notification Obligations' (May 2018) <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/exceptions-to-notification-obligations> accessed 28 August 2019.

[22] See Notifiable Data Breaches Act, s 26WP(2) (where there's no need to notify the Commissioner) and s 26WP(3) (to individuals).

[23] Daniel Solove, 'A Taxonomy of Privacy' (2006) 155 University of Pennsylvania Law Review 477 <https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf> accessed 20 July 2019.

are concerned is seen in the form of privacy laws, corporate entities and organizations are nevertheless still required to implement adequate security measures to ensure the integrity and safety of their data repositories.

The US experience shows that the scale of data breach is too large to remain unnoticed. Table 1 provides a very small sample of six of the largest US data breach incidents that occurred in the US between 2005 and 2017.

A. Consequences and cost of a data breach

Both the individuals and the companies or organizations that experienced a data breach are victims and suffer the consequences of the breach. In the case of the individual victims, there are psychological costs of understanding, interpreting and deciding how to react to information provided by notification, and any financial costs, inconvenience, and time spent addressing potential harm. In addition, the breach can cause physical, material and non-material damage including a loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudo-anonymization, damage to reputation, and any other significant economic or social disadvantages to those individuals.[24] This is so as stolen data may be used for telemarketing phishing scam, where personalized emails trick consumers into revealing financial information or clicking on links that plant malware on their computers. Criminals armed with stolen data can also impersonate affected individuals and call financial institutions purporting to be from legitimate customers seeking to get money transferred or a mailing address changed.

Breached companies and organizations suffer direct and indirect costs as a result of the breach. Direct costs include the cost of investigations into the cause of the breach, the repair, restoration, and fortification of information security systems, if necessary, the notification of customers the setting up of consumer call centres, the calculation and payment of legal fees and/or settlement awards and the provision of credit monitoring.[25] Indirect costs to companies and organizations include reputational damage and the time companies and organizations must spend on breach investigation and damage control, as well as employee retraining and education. Empirical studies[26] have also shown that disclosing data breaches can negatively affect stock market valuation. For instance, Campbell et al. found a negative effect on stock price for data breaches caused by 'unauthorized access of confidential information'.[27]

In 2018, an IBM cost of data breach study reported that the average cost of a data breach was US$3.86 million, an increase by 6.4 per cent from 2017.[28] Ponemon Institute reported that the ten largest expenses caused by data breaches were: remediation, loss of customers, business disruption, regulatory fines, legal costs, public relations cost of stolen

[24] General Data Protection Regulation, Recital 85.

[25] Sasha Romanosky, Rahul Telang, and Allesandro Acquisti, 'Do data breach disclosure laws reduce identity theft?' (2011) 30(2) Journal of Policy Analysis and Management 256.

[26] Huseyein Cavusoglu, Barry Mishra, S Raghunathan, 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' (2004) 9(1) International Journal of Electronic Commerce. See also K Kannan and others, 'Market Reactions to Information Security Breach Announcements' (2007) 12(1) International Journal of Electronic Commerce.

[27] Katherine Campbell, Lawrence Gordon, Martin P. Loeb, and Lei Zhou. 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market' (2003) 11(3) Journal of Computer Security 431; ibid.

[28] Charlie Osbourne, 'IBM: A data breach will now cost your organization $3.86 million, if you are lucky' *ZDNet* (July 2018) <https://www.zdnet.com/article/ibm-a-data-breach-will-now-cost-your-organization-3-86-million/> accessed 28 July 2019.

Table 1. Six of the largest data breaches, 2005 to 2017.

Attribute	ChoicePoint	Target	eBay	Anthem	Yahoo	Equifax
Company overview	Data broker selling information for identifying and verifying individuals' credentials to businesses and governments	Discount general merchandise retailer with over 1900 stores	Online auction site	Health insurer	Internet service company	Credit bureau
Cause of breach	Failure to maintain reasonable procedures for credentialing new subscribers	Unauthorized access to payment card data	Company's network hacked	Unauthorized access to IT system	Users' accounts hacked	Application vulnerability on company's website
Date breach was made public	February 2005	December 2013	May 2014	January 2015	2016	July 2017
Scope of breach	145,000 consumer reports accessed fraudulently	70 million debit and credit card account details	145 million users names, addresses, birthdates and encrypted passwords exposed	80 million past and present customers' personal information — addresses, medical identification numbers, social security numbers, income data and employment information	3 billion users accounts — birthdate, email addresses, passwords, security questions and answers	147.9 million consumer records containing social security numbers, birthdays, addresses & driving licence numbers
Who was affected	Individuals whose identity was stolen and used fraudulently Other businesses	Target customers Banks and credit card companies who replaced payment cards	eBay users	Anthem's past and present customers	Yahoo past and present users	Equifax consumers and business customers
Cost of breach	US$30 million	US$156 million	Fall of yearly revenue of at least US $18 billion due to loss of users' confidence	Data breach settled at US $115 million	At least US$385 million — US$350 million representing the price slash by Verizon for the buy-out and US$35 million fine by SEC	US$439 million at the end of 2017; expected to reach more than US $600 million

record, direct financial loss, notification costs, credit card re-issues, and identity theft repair and credit monitoring.[29]

B. Potential value and uses of stolen data

Data breaches can impact the lives of millions of people and financially cripple corporate entities and organizations. Ablon et al. reported that once a breach occurs, the acquired personal data can appear within days on black markets enabling criminals to sell financial, health and identity information,[30] thereby causing various forms of identity, tax and loan fraud.[31] Criminals often buy datasets from multiple hacks to commit fraud. The idea is to collect enough information to get past identity verification and authentication checks that banks and other institutions employ. For example, a whole package of PII which includes an individual's full name, date of birth, address, phone number, mother's maiden name, Social Security number, and driver's licence number costs US$30–$40 for US data, US$35–$50 for UK data, and US$15–$20 for Asia data.[32] Armor 2018 report reveals that credit card data is sold for US$10 and personally identifiable information that could include everything from a name and address to an Social Security number or even a credit report is selling for US$40–$200.[33]

C. Recent data breach experience in Hong Kong

By and large, most of the sample data breaches listed in Table 1 have had little direct impact on Hong Kong citizens. Nevertheless, data breaches at global entities whose footprints extend to Hong Kong — like Yahoo, eBay, Facebook and Marriott International, to name but a few — have indeed directly affected a number of Hong Kongers. Local-to-Hong Kong breaches have been experienced, and together with the extended reach data breaches, have certainly shaken the confidence of Hong Kong society and heightened societal privacy concerns.[34] There certainly has been an increase in local data breach incidences. The 2018 'Report on the Work of the Office of the Privacy Commissioner for Personal Data' of the Legislative Council of the Hong Kong Special Administrative Region (HKSAR) informed that:

---

[29] Data breaches cost US businesses an average of $7 million — here's the breakdown: <https://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4> accessed 28 July 2019.

[30] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, 'Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar' (2016) RAND Corp <https://www.rand.org/pubs/research_reports/RR610.html> accessed 20 July 2019.

[31] Terry Herr and Sasha Romanosky, 'Cyber-crime: Security under Scarce Resources' (24 June 2015) American Foreign Policy Council Defense Technology Defense Brief No. 11.

[32] Ericka Chickowski, 'Cybercriminal's Black Market Pricing Guide' *Dark Reading* (September 2019) <https://www.darkreading.com/threat-intelligence/cybercriminals-black-market-pricing-guide/d/d-id/1335798?image_number=2> accessed 20 November 2019.

[33] Armor, 'The Black Market Report' (March 2018) <https://cdn.armor.com/app/uploads/2018/03/27222933/2018-Q1-Reports-BlackMarket-DIGITAL-min.pdf> accessed 20 November 2019.

[34] For example, a Symantec study has reported that at least 2 million Internet users in Hong Kong were affected by cybercrime (including hacking and data breach) in a 12-month period ending September 2017. The study revealed that the cybercrime rate was higher than Japan and Singapore with victims losing US$28 on average and spending 19 hours dealing with the consequences. 43% of the polled individuals had been victims of identity theft, credit card fraud and had their account password compromised. See XY Su, 'At least 2 million Internet users in Hong Kong were hit by cybercrime in a 12-month period, survey says' *South China Morning Post* (Hong Kong, 27 March 2018) <https://www.scmp.com/news/hong-kong/community/article/2139170/least-2-million-internet-users-hong-kong-were-hit> accessed 2 April 2019.

> In 2018, 129 data breach incidents were reported to the [Privacy Commissioner for Personal Data], representing an increase of 22% as compared with 106 incidents of 2017 and 80% higher than 2014. The data breach incidents involved hacking, system misconfiguration, the loss of documents on portable devices, inadvertent disclosure of personal data by fax, email or post, etc.[35]

Data breaches in Hong Kong have thus far affected public hospitals, government agencies and local businesses. Some of the significant recent ones being:

(1) Hong Kong registered voter data: Prior to the earlier alluded Cathay Pacific's October 2018 data breach, the breach that attracted the most public attention and concern in Hong Kong was that of March 2017 following the Hong Kong Chief Executive's election — where the personal data of 3.78 million registered voters (stored in two notebook computers that went missing from their placement at the Asia World Expo) were compromised. One of the missing computers was said to contain the names of the roughly 1,200 members of the Chief Executive Election Committee, with the other containing information about all of Hong Kong's registered voters, including their names, addresses, Hong Kong Identity Card (HKID) numbers, and the geographical constituencies in which they were registered.[36]
(2) Travel agent customer data: In 2017, three travel agencies were the victims of separate cyber-attacks on their computer systems and databases potentially containing the 'names, HKID card numbers, passport numbers, credit card information, phone numbers, email address, mailing address and purchase history' of their customers.[37] The travel agencies were held to ransom with the perpetrators demanding a six-figure ransom payment for the release of information, payable in bitcoin.[38] One of the victim agencies was Hong Kong's largest travel agency, whose share price plummeted when news of the hacking was reported. Despite the company reaching out to its customers and notifying them of the incident and having put in place measures to mitigate further complications to lost data, the fact that the data remained at the mercy of the perpetrators and it was unlikely that a total recovery of all information stolen was possible left members of the public disillusioned.
(3) Internet service provider: A few months into the New Year, in April 2018, Hong Kong's second largest broadband provider reported its discovery of an unauthorized access to its inactive customer database, so compromising the personal details of 380,000 customers, including details of about 40,000 credit cards.[39]

---

[35] 'Legislative Council Paper — Report on the Work of the office of the Privacy Commissioner for Personal Data in 2018' (Legislative Council Panel on Constitutional Affairs, LC Paper No. CB(2)958/18-19(05)) <https://www.legco.gov.hk/yr18-19/english/panels/ca/papers/ca20190318cb2-958-5-e.pdf> accessed 22 July 2019.

[36] 'Legislative Council Paper — Loss of Notebook Computers containing Personal Data of Election Committee Members and Electors' (LC Paper No. CB(2)1650/16-17(01)) <https://www.legco.gov.hk/yr16-17/english/panels/ca/papers/ca20170619cb2-1650-1-e.pdf> accessed 28 July 2019.

[37] Naomi Ng, 'Hack attack on popular Hong Kong travel agent WWPKG puts customer data at risk' *South China Morning Post* (Hong Kong, 17 November 2017) <https://www.scmp.com/news/hong-kong/economy/article/2118745/hack-attack-popular-hong-kong-travel-agent-wwpkg-puts> accessed 2 April 2019.

[38] Ernest Kao, Danny Lee, and Christy Leung, 'Two Hong Kong travel agencies apologise as hackers demand payment for stolen customer data' *South China Morning Post* (Hong Kong, 4 January 2018) <https://www.scmp.com/news/hong-kong/law-crime/article/2126763/hong-kong-travel-agency-apologises-hackers-demand-payment> accessed 2 April 2019.

[39] Danny Mok, 'Personal data of some 380,000 Hong Kong broadband customers hacked, service provider says' *South China Morning Post* (Hong Kong, 18 April 2018) <https://www.scmp.com/news/hong-kong/law-crime/article/2142317/personal-data-some-380000-hong-kong-broadband-customers> accessed 2 May 2019.

(4) Medical faculty records: Earlier in September 2016, Hong Kong's top medical school, the University of Hong Kong's Li Ka Shing Faculty of Medicine, also suffered compromised data, when a laptop computer (containing personal information of 3,675 patients including their names, HKID and telephone numbers, diagnoses and medication lists) went missing from its office at Queen Mary Hospital. It was further reported that only 901 of those patients' data were encrypted.[40]

(5) Toy manufacturer: A hack on a locally-based digital toymaker firm, VTech Holdings database in November 2015 exposed information on 6.4 million children and adults. The database in question was in VTech's children's app store and 'Kid Connect' messaging system's data which contained and hence exposed customers' names, email address, password, Internet Protocol (IP) address, mailing address, download history, and children's names, gender and birthdates — and of customers from the US, Canada, the United Kingdom (UK), Ireland, France, Germany, Spain, Belgium, the Netherlands, Denmark, Luxembourg, Latin America, Hong Kong, China, Australia and New Zealand.[41]

D. Addressing data breaches from the legal perspective

Certainly, given the increased value of PII and the correspondingly heightened risks of its unauthorized access and the potential for its subsequent misuse, there has been renewed attention towards corporate and governmental information security measures regarding the protection of personal information.[42] However unlike information privacy, data breach notification comes under the purview of information security in that security, as opposed to privacy, becomes the dominant framework. Viewing data breaches as 'security issues' requires the focus to be directed at organizational security practices and hence, is the target of any legislation. Consequently, any security breach notification requires an evaluation of the effectiveness of an organization's security practices in protecting consumers' PII.

The global trend in recent years, in response to data breaches, has been towards enacting robust breach notification laws as seen in the US, the EU and Australia. Hong Kong, however, does not (as yet) deem notification on data breaches as mandatory, and instead, makes notification voluntary, leaving the obligation to notify those affected by the data breach and relevant authorities (for example, the Office of Privacy Commissioner) at the discretion of the organization that experienced the breach. The author's contention is that such voluntary schemes are inadequate to the task, and the author shall make a final supportable set of convincing conclusions. A first step to this is to evaluate the more pertinent ingredients of data breach notification.

---

[40] Raymond Yeung, 'University of Hong Kong's medicine department "sorry" for patient data breach' *South China Morning Post* (Hong Kong, 4 September 2016) <https://www.scmp.com/news/hong-kong/health-environment/article/2014282/university-hong-kongs-medicine-department-sorry> accessed 2 April 2019.

[41] The charges brought by the US Federal Trade Commission was settled with VTech paying US$650,000. See 'Smart toy maker VTech settles privacy charges with FTC' *CNET* (8 January 2018) <https://www.cnet.com/news/vtech-ftc-children-privacy-settlement-hacker-data-breach/> accessed 12 April 2019.

[42] Mark Burdon, Bill Lane and Paul von Nessen, 'Data breach notification law in the EU and Australia — Where to Now?' (2012) 28(3) Computer Law and Security Review 296.

III. Breach notification — the essential elements

The underlying objective to data breach notification is to provide affected individuals with a group notice emphasizing that a social harm has occurred as a result of a security breach that has affected the relationship between the organization and a group associated with that organization, thereby giving the larger society a legitimate claim to be informed of the breach.[43] Notification provides the opportunity to affected individuals to respond quickly to protect themselves from further harm and to shine a light on the breached company. Public notification of the breach highlights the weaknesses of or vulnerabilities in the organization or company's data security practices and can act as an incentive for the company to take steps to avoid or at least mitigate such risk in the future.[44] As US Justice Louis D. Brandeis famously said, 'Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants'.[45]

Hence, notification laws are seen to have two main effects — first, to empower consumers to take action to mitigate any potential harm caused by the breach and second, to force companies to bear the cost of their risky actions and to induce them to increase their investment in data protection controls. Consequently, breach notification laws in the US, the EU and Australia, for example, have adopted a variety of approaches in key areas such as notification triggers, exceptions to notification and the definition of personal data breach.

A. Personal data breach

The first element in notification of data breach is the definition of 'personal data breach'. The criteria in most US states for triggering a notification is the 'unauthorized access or acquisition' of an individual's first name (or initial) and last name in combination with a limited set of sensitive-personal data elements such as Social Security numbers and credit card numbers. In some cases, account number, credit card number or debit card in combination with necessary security code, access code or password permitting access would be required. By comparison, the EU's GDPR[46] defines data breach more broadly as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data'.[47] Unlike the US, personal data is not specifically limited to a set of personal data elements; instead it refers to any data that

[43] Priscilla M. Regan, 'Federal Security Breach Notifications: Politics and Approaches' (2009) 24(3) Berkeley Technology Law Journal.

[44] Lillian Ablon, Paul Heaton, Diana C. Lavery and Sasha Romanosky, 'Consumer Attitudes Toward Data Breach Notification and Loss off Personal Information' (2016) RAND Corp <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf> accessed 28 August 2019.

[45] Louis D Brandeis, *Other People's Money and How the Bankers Use It* (Frederick A. Stokes Company, New York, 1914) 92.

[46] The GDPR came into effect on 25 May 2018. Previously, data protection in the EU was based on the Data Protection Directive 95/46/EC which was built upon OECD's 1980 Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data seven principles. The OECD's seven principles are: (i) notice — individuals should be notified when their personal data is collected; (ii) purpose — use of personal data should be limited to the express purpose for which it was collected; (iii) consent — individual consent should be required before personal data is shared with other parties; (iv) security — collected data should be secured against abuse or compromise; (v) disclosure — data collectors should inform individuals when their personal data is being collected; (vi) access — individuals should have the ability to access their personal data and correct any inaccuracies; and (vii) account-ability — individuals should have a means to hold data collectors.

[47] GDPR, art 4(12). The definition in art 4(12) is largely identical to the definition in the e-Privacy directive except that it excludes the term 'electronic communication services', resulting in a cross-sectoral application.

can be directly or indirectly associated with a living individual including the IP address of the individual.

In Australia, not all data breaches require notification; only 'eligible data breaches', that is, a 'data breach' (in this case, there is no separate definition given) that is likely to result in serious harm to one or more individuals from the perspective of a reasonable person and an exception to the requirement for notification cannot be established.[48]

B. Notification trigger

Notification trigger is the threshold that indicates when and in what circumstances the organization should notify the relevant authority and/or affected individuals in event of a data breach. Jones categorized notification triggers into acquisition-based and risk-based triggers.[49] As the name suggests, acquisition-based triggers require notification where personal information has been acquired or believed to have been acquired without authorization. Acquisition-based are more consumer-oriented because the broad notification allows more consumers to be made aware of potential breaches and they can take action to mitigate potential harms before they arise. Because of that, a low threshold is set for notification in acquisition-based triggers. This is most notably seen in California's data breach notification law where the obligation to notify arises when an organization has suffered or believes it has suffered a data breach.[50] Given the low threshold requirement for acquisition-based triggers, acquisition-based triggers act as a regulatory tool of reputational sanction — organizations are 'encouraged' through the embarrassment of public notification to improve security measures within the organization.[51] Risk-based triggers on the other hand, require notification where the breached organization has identified a risk arising from the breach. Thus, risk-based triggers focus on a higher trigger threshold requiring notification where a risk assessment determines a risk of harm to consumers. These triggers tend to be more business-oriented because they require the organizations to determine whether a risk of harm will or is reasonably likely to arise.[52]

One reason for imposing a higher trigger is to reduce 'notification fatigue' caused by unnecessary notification. A number of US states have thus raised the trigger threshold by requiring an element of harm such as 'reasonable likelihood of harm or material harm' as is seen in the state laws of Alaska,[53] Arkansas,[54] Connecticut,[55] to name three while Michigan, Montana and Pennsylvania require that the breach has or is likely to cause

[48] A Notifiable Data Breach (NDB) scheme was established under the Privacy Amendment (Notifiable Data Breaches) Act 2017 requiring all agencies and organizations with existing personal information security obligations under the Australian Privacy Act 1988 to notify effective 22 February 2018, individuals whose personal information was involved in any data breach that was likely to result in *serious harm* (referred to as eligible data breaches).

[49] Michael E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3(3) A Journal of Law and Policy for the Information Society 555.

[50] Under Californian Civil Code §1798.29(a) and §1798.82(a), any state agency, person, or business that conducts business in California and owns, licences, or maintains computerized data that includes personal information, has an obligation to notify Californian residents of the discovery of unauthorized acquisition of *unencrypted* computerized personal information without reasonable delay. See <https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29> accessed 22 July 2019 and <https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82> accessed 22 July 2019.

[51] Paul M Schwartz and Edward J Janger, 'Notification of Date Security Breaches' (2007) 105 Michigan Law Review 913.

[52] Ibid.

[53] Alaska Statute Title. 45.48.010 et seq.

[54] Arkansas. Code Annotated. §§ 4–110-101–108 (2005).

[55] Connecticut. General. Statute. § 36a-701b (2005); as amended (2012, 2015, 2018).

substantial loss or injury or a reasonable likelihood that the information will be misused as in the states of Maine[56] and Maryland.[57]

By comparison, the GDPR provides for two different levels of notification, the first, where the breach is likely to lead to 'a risk for the rights and freedoms of the individuals' and the second, where the breach is likely to lead to '*high risk* to the rights and freedoms of the individuals', and that only the latter requires notification to affected individuals.

Australia's notification trigger threshold on the other hand, only requires the Privacy Commissioner and affected individuals to be notified when the unauthorized access or disclosure of information would result in *serious harm* to the individual (an eligible breach). In other words, notification is not required where the breach does not result in serious harm.[58] No definition is provided as to what 'serious harm' might include or encompass. Presumably, assessments will be made by a person or a team of persons in the organization who have been informed based on details immediately available that has been obtained following reasonable inquiries and/or investigations. Notwithstanding, Section 26WG of the Notifiable Data Breaches Act provides a number of factors that can be used as references. These include the kind of information involved, the sensitivity of the information, whether the information is protected by one or more security measures and the likelihood the measures could be overcome, the persons or kinds of persons who have obtained or could have obtained the information and the nature of harm.[59] A breach is considered to be more serious where medical and credit card information is disclosed as compared to merely a name or any residential address which is not linked to any other information or where the information is password protected as compared to the use of a stronger encryption method. The seriousness of the breach is also dependent on the harm caused. For example, did the breach result in physical or financial harm to the affected persons or was the breached information previously made publicly available?

C. *Encryption*

Given that one of the objectives of data breach notification laws is to provide data breach victims with a 'head-start' to proactively protect their data, the issue of whether a notification is triggered and when it is triggered can be dependent on whether personal information disclosed is encrypted. Thus, encryption can be used to define the parameters for notification.

In the US, state-based encryption exemptions tend to range from where notification of breach is required in cases of unauthorized acquisition of unencrypted personal information such as in California — §1798.82(a) to varying plethora of exemptions.[60] For example, much of the encryption exemptions depends on the restrictiveness of the definition like requiring the transformation of data using 128 bits or higher or requiring any other method that

[56] Maine Revised. Statute Annotated Title 10, § 1346–49 (2005); as amended (2006).
[57] Maryland Code Annotated Commercial. Law § 14–3501–3508 (2007); as amended (2017).
[58] For the purposes of the Privacy Amendment (Notifiable Data Breaches) Act 2017, harm was given a wide scope and thus includes physical, psychological, emotional, reputational, economic and financial harm. See Office of the Australian Information Commissioner, 'Part 4 Notifiable Data Breach Scheme' <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/> accessed 5 October 2019.
[59] Notifiable Data Breaches Act, s 26 WG.
[60] M Burdon and others, 'Australian Data Breach notification: avoiding the State/Federal overlap' (Proceedings of the 5th International Conference on Legal, Security, and Privacy Issues in IT Law, Barcelona, 2010).

renders the data unreadable or unusable. Some US states require additional security measures such as encryption keys, passwords or codes that would enable the unauthorized person to decrypt the information obtained.[61] Jones identified three types of encryption safe harbour,[62] stating that an encryption provision is based on the notion that encrypted data is secure and requires no notification if the encrypted data is breached. There may be a rebuttable presumption that no risk exists unless the encrypted data is breached. A breached entity may also operate under the assumption that there is no likelihood of harm unless harm is proven to exist. According to Jones, encryption may also be treated as a factor when assessing the risk to individuals in the event of a data breach.

In certain circumstances, the use of redaction may be seen as another exemption to breach notification.[63] A redacted document is a document that has been modified, edited or revised and any confidential or sensitive information has been removed from it.[64] Although proven useful in terms of hard copies, redaction as an encryption exemption is generally difficult to achieve in the electronic equivalent of a hard copy redaction unless the words of the hard copy had first been blacked out before scanned.[65]

Much like the US states' notification scheme, encryption exemptions are provided under the GDPR. In most cases, there is no obligation to notify Data Protection Authorities if appropriate technical and organizational measures are in place such as when the data is encrypted or where other measures have been undertaken to ensure the high risk to the rights and freedoms of the individuals is not likely to materialize. This is the same in Australia, where in assessing whether the unauthorized disclosure will result in serious harm to the individual, one needs to consider whether the information is protected by one or more security measures and if so, the likelihood the measures could be overcome.

IV. Critiques of notification laws

Given the lack of market-based incentives aimed at enhancing corporate information security measures, the embarrassment factor through reputational sanction of breach notification laws has been seen as a significant regulatory tool. In effect, the negative publicity arising from notification is seen as an incentive for organizations to invest adequately in information security and thus avoid the detrimental impact on share price that can result through notification. Notwithstanding, critics argue that breach notification laws inflict unnecessary costs on both organizations and consumers.[66] Whether or not the legal arena mandates breach notification, a breached organization still incurs the cost of investigating a data breach, repairing any information technology systems, and restoring business services and consumer confidence. Costs increase further when notification is mandatory with expenses incurred, for example, of legal fees in determining whether breach should be notified, remediation measures such as costs of customer notification, public relations campaigns, and regulatory fines or fees imposed by regulatory agencies. Other costs include

[61] Ibid.
[62] Jones (n 49).
[63] Kansas, Iowa, Michigan, Ohio as some examples.
[64] See Bryan A Garner, *Black's law dictionary* (10th edn, Thomson West, 2014).
[65] Burdon and others (n 60).
[66] See for example, Regan (n 43); J Freedman, 'Industry seeks one law on data breach alerts' (2006) 64 The Congressional Quarterly Weekly Report 314.

free credit monitoring for affected individuals, defending possible lawsuits for data breach, employee training, termination or disciplining and reputational damage.

There is also the contention that stolen data resulting from a data breach are likely to lack provenance or information about the place of their origin and hence, affected individuals may not associate the harm that they suffer with the organization that had breached the data.[67] Risks are normally applied to the organization/institution that mistakenly relied on the fraudulently presented information, for example, in credit card applications, rather than the organization in which the breach took place. Hence, any form of redress (possible civil liability or compensation envisaged) against the breached organization could prove difficult to achieve.

Another argument made is that consumers could be subjected to 'information overload' or 'the boy who cried wolf' syndrome[68] in which laws not carefully thought off may result in consumers receiving a flood of breach disclosure notices (not all warranting attention) and so resulting in unintentional consumer complacency and even failure to take appropriate steps to mitigate loss.

V. The data breach arena in Hong Kong

A. Background to Hong Kong's data protection framework

The Personal Data (Privacy) Ordinance (PD(P)O) establishes Hong Kong's data protection and privacy legal framework. Two influential international instruments shaped Hong Kong's privacy standards — the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980[69] and the EU Directive 95/46.[70] All organizations both private and public that collect, hold, process and use personal data (data users) must comply with the PD(P)O and its component six data protection principles (DPPs).

The PD(P)O first came into force on 20 December 1996. The regulatory regime was overhauled in 2012 with the reforms (mainly changes to the DPPs) brought into force in 2013. Hong Kong's data protection regime is a 'one size-fits-all' data protection regime — in other words, the same level of protection is afforded for all personal data with no differentiation in data types. Hong Kong's PD(P)O is principle-based with its core provisions encapsulated in the six DPPs as its cornerstones and aims to protect the privacy of individuals in relation to their personal data. The DPPs are based on the OECD Guidelines and are as set out in Schedule 1 of the PD(P)O; the DPPs are: (1) purpose and manner of collection; (2) accuracy and duration of retention; (3) use; (4) security; (5) information to be generally available; and (6) access. Aside from imposing security safeguards on the keeping of personal data by a data user and the granting of rights to data subjects, the

[67] See Schwartz and Janger (n 51).

[68] See Cass S Sunstein 'Information Regulation and Information Standing: Akins and Beyond' (1999) 147 University of Pennsylvania Law Review 613.

[69] The Guidelines represent an international consensus on what principles should govern the collection and processing of personal data. See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 28 August 2019.

[70] Although the GDPR became effective in May 2018 thereby repealing the EU Directive 95/46, reference will be made to EU Directive 95/46 which forms the basis of Hong Kong's PD(P)O.

PD(P)O established the Office of the Privacy Commissioner for Personal Data (PCO), an independent statutory body, to oversee the enforcement of the PD(P)O.

B. Deficiencies of the current framework

1. Voluntary nature

Although Hong Kong was the first Asian jurisdiction to enact a comprehensive personal data privacy legislation and to establish an independent privacy regulator, it has failed to move in time with the developments of the digital age. One of its main criticisms is that despite the increasing incidences of data breach in Hong Kong, notification of data breach remains voluntary — there is no requirement for breached organizations and companies to notify affected individuals, the Privacy Commissioner or other relevant authorities of a data breach. This is regardless of whether the breach is 'contained', whether the affected numbers are small or whether its potential impact may be far reaching. The review and overhaul of the PD(P)O in 2012 failed to introduce mandatory data breach notification provisions to better protect individuals despite the strong support for the scheme by the PCO and the fact that there were already a number of data breach incidents prior to the overhaul. The government's stance may be due to the public views received during the government's public consultation held between 2009 and 2010 where 64 per cent of the respondents agreed to the setting up of a voluntary notification scheme while only 16 per cent favoured a mandatory scheme.[71] Indeed, the 2010 Consultation Report on the Review of the PD(P)O (Consultation Report) had mentioned that privacy breach notification is not yet mature and imposing a mandatory requirement may cause onerous burden on data users.[72]

To assist data users in giving data breach notifications under a voluntary scheme, the PCO issued a Guidance on Data Breach Handling and Giving of Breach Notifications (Guidance Note) in 2010 (revised in December 2016). The Guidance Note provides useful information and assistance as to the steps that should be taken when a data breach occurs. Aside from providing an explanation as to what amounts to a data breach and the objective behind data breach notification, the Guidance Note advises on how to assess the risk of harm providing examples of what might increase the extent of harm suffered.[73] For example, where the data user[74] decides to notify data subjects, the Guidance Notes advises that notification should be made as soon as practicable after detection of the data breach by phone, in writing, via email or in person. Notification to the Privacy Commissioner is also alluded to by informing that such may be made by submitting a Data Breach Notification Form (downloadable from the PCO's website).

2. Guidance Note merely a guide

While the Guidance Note provides a comprehensive navigational guide as to what should be done in event of a data breach, the Guidance Note remains merely a 'Guide' and the

[71] The survey was conducted by the Hong Kong Research Association. See *Consultation Report on the Review of the Personal Data (Privacy) Ordinance* (hereafter '*Consultation Report*') Annex 4 <https://www.cmab.gov.hk/doc/issues/PCPO_report_en.pdf> accessed 9 October 2019.

[72] Ibid.

[73] 'Guidance on Data Breach Handling and Giving of Breach Notifications' <https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf> accessed 28 August 2019.

[74] A data user is defined under s 2 of the PD(P)O as a person who controls the collection, holding, processing or use of the data.

record shows that accordingly, it is treated as such by organizations — some 'good suggestions' perhaps, but no more. Organizations are not penalized administratively or by statute for their decision not to notify persons affected, law enforcement agencies, or the PCO itself, and unsurprisingly, may simply decide to not do so. The potential reasons for an organization whose data has been breached to elect not, rather than, to report, a data breach suffered is readily ascertainable. Some of these are as follows:

a. Reputational and financial loss. A prime reason for not reporting a data breach is to protect the breached organization against reputational damage and consequently, a potential reduction in the organization's market value. In 2018, Facebook had US $119 billion wiped off its market value after the company informed investors that user growth had slowed in the wake of the Cambridge Analytica scandal.[75] That loss in market value was separate to the further US$13 billion loss that resulted from a data breach in September 2018 that affected 50 million users.[76] Although in Hong Kong, the diminution in the market value of Cathay Pacific when it suffered a data breach in 2018 was not as high as Facebook's, its Cathay Pacific shares did hit a nine year low when it plummeted by 6.59 per cent after the data breach was announced.[77]

b. No necessity or obligation for notification. Given there are no 'rules' providing for when relevant authorities and/or affected individuals should be notified, breached organizations may simply seek to justify their failure to notify by stating that 'having assessed the "risk of damage" to affected individuals', it concluded that there was no pressing need, no necessity *per se*, to notify any affected individual or even the relevant authorities. The issue here is how does one determine whether an investigation was indeed conducted by the breached organization and whether there is a procedural standard or an investigation protocol that the organization has to comply with? And if so, how comprehensive is the procedure?

Further in voluntary notification schemes, only responsible organizations will notify relevant authorities and bear the relevant costs; this 'penalizes' responsible organizations by making them less competitive but is more beneficial to irresponsible organizations.

c. Weak enforcement. Hong Kong's DPP4(1) and (2) provide that: 'a data user shall take reasonably practical steps to ensure that the personal data held is protected against unauthorized or accidental access, processing, erasure, loss or use, having particular regard to the kind of data and the harm that could result ...' and that where a data processor is engaged (whether within or outside Hong Kong) to process data on behalf of the data user, DPP4(2) provides that the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. A data breach can potentially arise through an organization's contravention of these DPPs — for example, by its failure to

[75] R Neate, 'Over $119bn wiped off Facebook's market cap after growth shock' *The Guardian* (28 July 2018) <https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock> accessed 28 August 2019.

[76] K Kelleher, 'Facebook loses around 13bn in value after data breach affects 50 million of its users' (28 September 2018) <http://fortune.com/2018/09/28/facebook-stock-falls-after-security-breach/> accessed 28 August 2019.

[77] 'Cathay Pacific shares hit a 9 year low after a data leak affected 9.4 million passengers' *Reuters* (24 October 2018) <https://www.cnbc.com/2018/10/24/reuters-america-update-1-cathay-pacific-shares-hit-9-yr-low-after-data-leak-affects-9-point-4-mln-passengers.html> accessed 28 August 2019.

take 'reasonably practical steps', either through incompetence, or insufficient attention to the task at hand. DPP4 compliance is to be judged on a case-by-case basis. 'The reasonably practicable steps' that organizations are required to take to protect personal data they processed are to be assessed on the basis of whether or not they are proportionate to the harm that could result from the unauthorized access to the data in question.

Nevertheless, it remains true that contravention of any of the DPPs does not in itself constitute an offence under the PD(P)O or result in the imposition of penalty. At most, an enforcement notice may be issued to correct any shortcomings where the investigation reveals that the organization has not complied with the PD(P)O and its DPPs.[78] It is only a criminal offence where the data user fails to comply with the enforcement notice issued or have complied with the enforcement notice, intentionally performs an act or makes an omission in contravention of the PD(P)O,[79] in other words, commits a new breach on the same facts. The maximum fine that can be imposed is HK$50,000 (approximately US $6,410) and two year imprisonment. A daily penalty of HK$1,000 (US$128) is imposed if the offence continues after conviction. Where the data user is a repeat offender, breaching more than one enforcement notice, the maximum fine is HK$500,000 (US$64,102) but still with just two year's imprisonment. The daily penalty is increased to HK$2,000 (US $256) if the offence continues after a second or subsequent conviction.[80] Hence, enforcement notices *per se*, are not sanctions; but rather seen as merely an 'authoritative' advice requiring the data user to rectify or prevent any recurrence of the data breach. For example, in the Cathay Pacific data breach, the PCO's enforcement notice directed Cathay Pacific to, inter alia, engage an independent data security expert to overhaul the systems containing personal data to ensure that the systems are free from malware and known vulnerabilities and to conduct regular reviews on the security of its networks.[81]

It is difficult to see how such a 'gloved hand' approach to data breaches can encourage data users to adopt either a more committed attitude towards ensuring better security measures within the organization, or greater responsibility and respect towards individuals' data privacy and their resultant loss in event of breach.

According to Hong Kong's privacy watchdog, Hong Kong saw a record number of user data breaches in 2018, totalling 129.[82] Table 2 below provides a brief summary of the number of notification of data breach incidents received by the PCO, the number of warnings and enforcement notices issued and compliance checks conducted between 2015 and 2018.

As noted, in Hong Kong, although notification of a breach is merely strongly encouraged by the PCO, it is not the only way to initiate an enquiry or an investigation. The PCO may conduct an investigation into the breach incident based on public complaints. Compliance checks and compliance investigations (formal probe) by the PCO can also be conducted on PCO's own initiative. This is normally carried out once the PCO has decided there are reasonable grounds to believe there may have been contravention of

[78] PD(P)O, s 50(1).
[79] Ibid, s 50A(3).
[80] Ibid, s 50A(1).
[81] See PCO, 'Data Breach Investigation Report No: R19-15281, Cathay Pacific Airways Limited and Hong Kong Dragon Airlines Limited, Unauthorised access to personal data of passengers' (6 June 2019).
[82] Holmes Chan, 'Data breaches hit record high in 2018 says Hong Kong Privacy Watchdog' *Hong Kong Free Press* (Hong Kong, 1 February 2019) <https://www.hongkongfp.com/2019/02/01/data-breaches-hit-record-high-2018-says-hong-kongs-privacy-watchdog/> accessed 12 March 2019.

Table 2. Summary of data breach incidents, warnings and enforcement notices issued by PCO and number of compliance checks.

	2018	2017	2016	2015
Data breach incidents	129	106	89	98
Number of affected individuals	765,834	86,000*	104,000	871,000
PCO warnings	16	26	36	17
Enforcement notices issued	0	3	6	67
Compliance checks by PCO	289	253	259	279
PCO initiated investigations	4	1	4	76

*The number excludes 1,968 complaints made in relation to the Registration and Electoral Office (REO) loss of two laptops containing personal information of 3.7 million voters during the election of Hong Kong's Chief Executive in March 2017.

Source: 'Report on the Work of the Office of Privacy Commissioner for Personal Data 2017' (Legislative Council Panel on Constitutional Affairs, LC Paper No. CB(2)851/17-18(03)).

a requirement under the PD(P)O.[83] A compliance check is a means of alerting an organization over the PCO's concern about data protection measures and invites the organization to take remedial action. Random compliance checks may also be conducted on organizations within a specific industry, for example, travel agency industry, real estate industry or the insurance industry. As an example, in October 2018, the PCO initiated a compliance investigation on Facebook Hong Kong Limited (Facebook Hong Kong) on the Cambridge Analytica incident concerning the unauthorized use of Facebook account holders' data. Upon completion of investigation, the PCO did not find any evidence of Facebook Hong Kong's involvement in the incident given that it is Facebook Ireland Limited and not Facebook Hong Kong that controlled the collection, processing, holding and use of all Facebook Hong Kong's account holders' data.[84]

C. *Penalties*

The imposition of penalties (administrative or otherwise) for violation of requirements is commonly seen across global jurisdictions. In the US, for example, the Department of Health and Human Services fined health insurer, Anthem, US$16 million for a breach that occurred in 2014, a breach that exposed the data of 79 million individuals.[85] Before the GDPR came into force in May 2018, UK's Information Commissioner's Office (ICO) penalized TalkTalk Telecom Group Plc with a record fine of £400,000[86] for failing to notify the ICO of a data breach within 24 hours of detection[87] as required by relevant regulations.[88] Under the GDPR, a fine of up to four per cent of a data controller's (organization's) annual global turnover or €20 million whichever is higher can be imposed.

[83] PD(P)O, s 38(b).

[84] See PCO, *Annual Report 2017–2018* <https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport18_04.pdf> accessed 15 October 2019.

[85] 'Anthem to pay a record $16 million fine for insurance data breach' *Associated Press* (15 October 2018) <https://www.staradvertiser.com/2018/10/15/breaking-news/anthem-to-pay-record-16m-fine-for-insurance-data-breach/> accessed 28 August 2019.

[86] The maximum fine ICO is empowered to impose is £500,000 under s 55A of the Data Protection Act 1998.

[87] The ICO required data breaches to be notified as soon as they are detected and not after internal investigations had taken place. In the case of TalkTalk, ICO was notified on 1 December 2015 although the unauthorized access to customers' data occurred on 16 November 2015.

[88] The Privacy and Electronic Communications Regulations 2003 and the Notification Regulation (611/2013).

In Hong Kong, however, fines are only imposed for failure to comply with an enforcement notice. Therefore as we have previously seen, although Cathay Pacific had breached DPP4 and DPP2, and delayed in notifying the PCO of the data breach incident for seven months (after the initial attack), it was not penalized. Additionally, in comparison to the fines imposed in other jurisdictions, fines imposed under the PD(P)O are negligible and do not provide any real 'dis-incentive' for data users in Hong Kong to comply with and abide by the PCO's advice under the enforcement notice. For organizations, paying the non-compliance fine is the lesser (and 'cheaper') of two evils as notification of a data breach draws a heavier penalty by way of reputational damage and financial loss suffered through remedial measures or reduction in share price as alluded to earlier.

Further in terms of enforcement, Table 2 above shows only three enforcement notices issued for all data breaches of 2017 and four enforcement notices in 2018. There are neither any reported cases of non-compliance with the PCO's enforcement notice, nor is there evidence of any referral of data breach incidents to the Hong Kong Police for criminal prosecution as compared, for example, to cases involving direct marketing violations.[89]

In 2017, there were ten direct marketing cases being considered for prosecution by the PCO. Since the new direct marketing-related provisions came into effect in 2013, data users in 11 cases have been convicted of breaching the requirements under the PD(P)O. Linklaters, a global legal firm, suggests that investigation and prosecution relating to direct marketing practices have always been the focus of enforcement actions by the Privacy Commissioner. Two examples are provided, the first in April 2016, when a Community Service Order of 80 hours was imposed on an insurance agent for the offences of: (i) using the personal data of a data subject in direct marketing without taking specified actions/obtaining consent; and (ii) failing to inform the data subject, when using his personal data in direct marketing for the first time, of the data subject's right to request (without charge) that his personal data not be used in direct marketing. The second illustrative case was in May 2016, where a marketing company was fined HK$16,000 for the offences of: (i) using the personal data of a data subject in direct marketing without taking specified actions/obtaining consent; and (ii) failing to comply with the data subject's request to cease using his personal data in direct marketing.[90] According to the PCO's annual report 2017–2018, 187 cases were reported for alleged breaches of direct marketing as compared to 263 cases of alleged breaches of inadequate security for personal data. The cases indicate that the attention and the emphasis on the violation of direct marketing

[89] 'Report on the Work of the Office of Privacy Commissioner for Personal Data 2017, (Legislative CouncilPanel on Constitutional Affairs, LC Paper No. CB(2)851/17-18(03)). Under the PD(P)O, organizations are required to notify and obtain individuals' consent before using their personal data in direct marketing activities or transferring the data to another person for use in the latter's direct marketing activities. Direct marketers must also notify individuals of their right to opt-out when using the individuals' personal data for the first time. Individuals may at any time require the organization to: (a) cease to so use the data and/or; (b) require the organization to cease to transfer the data and to notify any person to whom their personal data has been so transferred to cease to use the data in direct marketing. In comparison with the breach of an enforcement notice, the use of personal data in direct marketing without the *data subject's* consent is punishable by a fine of HK$500,000 and imprisonment term of up to 3 years. A data user that provides a third party with personal data: (i) for the purposes of direct marketing; (ii) in return for consideration; and (iii) without the *data subject's* consent, will be liable to fines of up to HK$1,000,000 and a maximum of 5 years' imprisonment.

[90] See Linklaters, 'Data Protected — Hong Kong' <https://www.linklaters.com/en-hk/insights/data-protected/data-protected—hong-kong> accessed 28 August 2019.

provisions by the PCO is, at best, mis-guided. Surely, individuals affected by data breach incidents have equally as much to lose if not more, in the violation of their privacy so caused, as to that caused in the processes of direct marketing? Regretfully, this does not appear to be so in the PCO's books.

It has been contended in many Hong Kong data breach incidents that there was no need to take the matter further since breached organizations had cooperated with the PCO and had complied with the PCO's recommendations set out in the enforcement notice. A prime example is the 2017 Registration and Electoral Office (REO) data breach incident where the PCO concluded that the REO had breached DPP4 and issued an enforcement notice against it, which required the REO to establish effective internal guidelines for processing personal data and to ensure strict staff compliance with the guidelines. It also recommended, inter alia, that the REO conducts a privacy impact assessment and to implement Privacy Management Programme to embrace personal data privacy protection as part of their corporate governance responsibilities.[91] The PCO at the conclusion of its investigation reported that the REO lacked the requisite awareness and vigilance expected of it in protecting personal data. The security measures adopted by the REO were also not proportional to the degree of sensitivity of the data and the harm that might result from a data security incident. The PCO however, made no finding of an offence committed by the REO.

D. Regulation of data processors

Under the current law, there is no direct regulation of data processors and instead, data users have to bear the responsibility of ensuring data processors engaged by them have adequate data security measures in place to prevent any form of data breach — in effect, the data user is liable for its agent's or contractor's breach of the requirements under the PD(P)O. Under both DPP2 and DPP4, if a data user engages a data processor (whether within or outside of Hong Kong), the data user must use contractual or other means to ensure that personal data is protected from unauthorized or accidental access, processing, erasure, loss or use, and is not retained for longer than necessary for the purpose of processing the data. Thus, the ultimate responsibility to the PCO and the affected individuals falls squarely on the data users. In a 2012 non-binding information leaflet on Outsourcing the Processing of Personal Data to Data Processors, the Privacy Commissioner indicated the types of contractual obligations that could be imposed on a data processor engaged; they include that the data processor: (a) must not use or disclose personal data for any purpose other than for the purpose for which the personal data has been entrusted to it by the data user; (b) must take certain security measures to protect the personal data entrusted to it by the data user; (c) must comply with the DPPs; (d) must return or delete the personal data once it was no longer required for which it was originally entrusted by the data user; further that (e) sub-contracting was prohibited or restricted; and (f) audit and inspection rights had to be provided in favour of the data user. The Privacy Commissioner has also suggested that 'other means' of ensuring compliance by a data processor include ensuring that reputable data

[91] 'Investigation Report Number R-17: 6429' (12 June 2017) <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R17-6429_Eng.pdf> accessed 28 August 2019.

processors were selected by a data user and ensuring that sufficient due diligence was conducted by a data user as to potential data processors.

Given the large volumes of data being outsourced for processing, neither the PCO's Guidance Note nor the PD(P)O makes specific mention of data processors and their obligations. By comparison, under the GDPR, data processors are accountable to relevant authorities and affected individuals for any data breaches. It is strange that given their increasingly significant role, data processors are not held directly accountable for any contravention of the PD(P)O and its DPPs. Data breaches are not confined to data users. If the PCO is seriously committed to addressing data breaches, data processors should be included and held responsible. It is futile for data users to have to rely on their contractual arrangements with data processors for the recovery of any data breach losses data users may suffer.

VI. The way forward — conclusions

Having examined Hong Kong's data breach notification position, a framework incorporating the salient features of a data breach notification is proposed to bring Hong Kong in line with emerging international practice. Before such framework can be established, however, it is crucial for policymakers to agree upon the policy goal that is to be achieved, a prerequisite of which is a proper understanding of the problem to be addressed. What, for example, are the objectives behind establishing a mandatory breach notification scheme in Hong Kong? Is the objective of a proposed framework to reduce identity theft that is seen as one of the major problems faced in the US, the EU and Australia or is the goal to improve organizational data security practices?

A. Reducing identity theft

Despite the numerous data breach incidents experienced to date in Hong Kong, there have yet been no reported or detected incidents of identity theft stemming from those breaches. Neither the banks, the PCO nor the police recorded any increase in fraudulent financial transactions (including credit card payment claims) or insurance claims as any aftermath of the two major data breaches in Hong Kong — the REO data breach in 2017 and the Cathay Pacific breach in 2018 — although that is not to claim that identity theft may yet take place in the future. Nonetheless, one should be mindful that not all data breaches automatically result in identity theft — a 2007 Javelin survey attributed very few reported incidents of identity theft as a consequence of security breaches.[92] Scholars Romansky, Telang and Acquisti also found that data breach laws had no statistically significant effect on reducing identity theft.[93] Notwithstanding, breach notification may lead to a positive societal change in mindset towards treating data breaches as social harm. Such change in mindset would in turn create greater public awareness and could even encourage society as a whole to be more vigilant of their PII and cognizant of ways to protect it. Without mandatory notification, less information about breaches would be available, and this could result in societal complacency to the potential for harm from data breach.

[92] 'Javelin Strategy & Research Survey — February 2007' <https://www.privacyrights.org/blog/identity-theft-surveys-and-studies-how-many-identity-theft-victims-are-there-what-impact> accessed 28 August 2019.
[93] Romanosky, Telang and Acquisti (n 25).

B. Improve data security practices

Where the policy goal, however, is to improve organizational data security practices, data breach notification can be used to provide a change in organizational culture ensuring that greater respect, care and accountability becomes a priority in data handling and management. This would inevitably translate into improved internal organizational data security measures. Although notification is less helpful where a data breach has already occurred, than when adequate preventive measures exist in the first place, it does act as a deterrent to ensure future incidents are not left hidden.

C. When is notification warranted?

Having looked at the policy goals that might underscore Hong Kong's framework, attention can be directed at the necessary elements of such a framework. As not every security breach incident amounts to a personal data breach requiring notification, we can conclude that notification is only required where there is a breach of information security that results in actual compromise personal data.

Breach notification is dependent on what is meant by personal data breach that accordingly takes its reference to the definition of personal data. Generally, the more sensitive the personal data, the higher the risk of harm or damage will cause to the affected individuals. A good starting point of a personal data breach thus, is the 'unlawful loss, destruction and/or unauthorized access to, or disclosure of personal data which is reasonably likely to result in significant harm to individuals and organizations'.

It should be noted that although the definition of personal data under the PD(P)O is relatively similar with that of EU Directive 95/46, the Ordinance does not provide for a separate category for sensitive data.[94] Notwithstanding, it is clear that at the very least, sensitive data should include HKID numbers and credit card CVVs. It has been suggested that if the request and use of HKIDs as credentials is restricted, the restriction will contribute in the reduction of financial fraud such as new account frauds, credit card frauds and fraudulent insurance claims in the event of data breach. The suggestion while useful cannot be supported as aside from the effectiveness and expediency in the use of HKIDs as a means of identification and verification, there will be an increase in cost and inconvenience in using other forms of identifying particulars. A better solution is to ensure the collection, use, storage and retention of personal data as regulated under the PD(P)O and the DPPs are strictly enforced. For example, it appears that although Cathay Pacific had policies in place directing that information should not be kept longer than is necessary for the purposes for which it was collected and the information must be purged once the relevant customer's file had been marked inactive for seven consecutive years, the PCO found that close to a quarter million customers' HKID numbers were still retained 13 years after it had been dispensed with.[95] What is required therefore is regular robust reviews and close monitoring of internal organization's policies and procedures (for example, data retention policy) coupled with strict implementation and enforcement.

[94] However, unlike the GDPR (see arts 4(13), (14), (15) and art 9), there is no concept of sensitive data under Hong Kong's Ordinance. Thus, the collection and processing of medical and health data in Hong Kong, for example, is not subjected to additional processing requirements.

[95] See n 81 above.

It is important that a balance be struck between the need to promote public confidence in the data security practices of organizations and the costs that will be involved for organizations. To ease the implementation of mandatory notification, it is fitting that mandatory notification be first strictly implemented against public sectors and industries that handle sensitive personal data such as banking and finance industries and medical/health industries where a breach would result in considerable harm or economic loss. Having garnered public and organizations' support and confidence, the system can be extended to other industries.

D. Notification trigger

Another controversial issue is the notification trigger — the severity at which (both when and in what circumstances) organizations should notify the PCO, other relevant authorities (like the Hong Kong Police) and affected individuals in event of a data breach. As an international financial centre and dubbed one of the four Asian Tigers[96] (Dragons), Hong Kong fosters and supports a business-oriented environment. The liberal policies of the Territory's government are aimed at fostering internationalization and trade has driven and sustained Hong Kong's rapid economic growth rate.[97] It is hence unlikely for policymakers and legislators to agree to Jones's acquisition-based notification trigger.[98] With acquisition-based trigger, organizations are encouraged via reputational sanctions (embarrassment by public notification) to improve security measures within the organization. Instead, the author speculates a business-oriented trigger where notification is based on a high trigger threshold requiring a risk assessment to determine the risk of harm to consumers. Indeed, it has been suggested by respondents to the Consultation Report that the pre-requisite for notification is that the privacy breach may lead to a misuse of the unencrypted financial or identity data that will result in identity theft or financial loss.[99]

What then does one see the role of notices? Notices should prove to be useful to consumers — to notify them where there is likelihood of harm; rather than to needlessly alarm them when the likelihood of harm is minor. Where the purpose of the notice is to impose a reputational sanction, then it is necessary to identify the source of the breach but if as stated, the purpose of the breach notification scheme is to mitigate harm associated with the breach while also being supportive and sensitive to business operations, then knowing the source of the breach is less important.

E. Standard of risk required

What then might be the standard of such risk? Should notification be based on one that is 'reasonably likely' or 'likely' to cause harm, material risk of harm or high risk of harm to the rights and freedoms of the individuals (as in the EU GDPR)? Needless to say, organizations and companies would prefer a higher standard requiring that 'harm' be 'significant or

[96] The other Asian Tigers being Singapore, Taiwan and South Korea. See J Winkler, 'The 4 Asian Tigers economy growth' (July 3 2017) <https://www.docurex.com/en/four-4-asian-tigers-economy-growth/> accessed 28 March 2019.

[97] Hong Kong's GDP per capita reached US$46,199.385 in December 2017, compared with US$43,737.600 in December 2016. CEIC, 'Hong Kong SAR GDP Per Capita' <https://www.ceicdata.com/en/indicator/hong-kong/gdp-per-capita> accessed 28 August 2019.

[98] Jones (n 49).

[99] *Consultation Report* (n 71).

substantial' as opposed to one that is 'likely' or 'reasonably likely' to cause harm. We have previously proposed that the standard be one where the breach is 'reasonably likely to result in significant harm to individuals and organizations'. Given the significant impact the data breach can have on affected individuals, the author also proposes (as with the position in Australia), that 'harm' be defined widely so as to include physical, psychological, reputational, economic and financial harm.

F. Internal investigation and encryption

Given that notification can only be made after the organization has completed an internal investigation of the data breach, it is incumbent that organizations have in place a team of persons (data security experts) who can make an assessment as to the likelihood of harm based on the type of information disclosed, the sensitivity of the information, the type of encryption or security measures used and the possibility of such security measures being overcome. While each and every breach incident should be investigated to determine the weakness or flaws of the organization's security system, unnecessary notification to affected individuals (especially when the risk of harm is low), may de-sensitize individuals preventing them from acting when a serious threat does exist. Further in line with international norms, notification should only be necessary where data is not encrypted. In a breach of encrypted data, the breach, as mentioned previously, should be one that will result in a likelihood of significant harm, is likely to be favoured by businesses. The appropriate level of encryption should be one that commonly adopted for data security within the relevant industries. More importantly, regular reviews should be conducted on such encryption programs, etc.

An investigation report into the breach incident and the measures undertaken to rectify any harm that resulted should be submitted to the PCO, regardless of whether affected consumers are notified, with the PCO reserving the power to further investigations of the breach incident and to recommend additional and further measures such as imposing fines where it deems appropriate. The PCO should also be empowered to override the breached organization's decision not to notify affected consumers.

G. A two-pronged approach

In striking a balance between individuals' right to be notified of a breach of their PII and maintaining Hong Kong's support of a business-oriented environment, a model with a two-pronged approach is recommended. The first prong requires the PCO and the Hong Kong Police to be notified promptly and in any event no later than 72 hours when an unlawful loss, destruction and/or unauthorized access to, or disclosure of personal data has been detected. The second prong entails notifying individuals when 'there is a likelihood that the breach will lead to a misuse of the leaked personal data resulting in significant harm'. Although the first prong has a lower trigger threshold, its role is to provide an early warning allowing relevant authorities (specifically the PCO) to assess the effectiveness of the breached organization's response plan and remedial measures. The second prong provides a higher notification trigger so that consumers are not unnecessarily notified.

H. Increasing importance of the PCO

The PCO's role is enhanced in the proposed model. The PCO who has better professional assessment ability would be better placed to make an assessment on whether the data breach is such that it is 'reasonably likely to result in significant harm to individuals' so as to require affected individuals to be notified. Where notification is required, the PCO will serve the anonymized notices to affected individuals whose data was compromised in the breach and to other organizations and companies within the industries for example, insurance, financial sectors or the public sector, as relevant. The sharing of information about security breaches within the relevant industries/sectors will heighten the amount of information brought into PCO's systems. This not only increases the knowledge base among the public and organizations within the private industries and government entities but also allows the PCO to orchestrate and monitor a systemic response. With the information collated, statistical information regarding data breach incidents, data security practices and remedial measures can be prepared. This will go a long way in assessing and monitoring the data security health of Hong Kong.

The author proposes that the PCO continues to be the entity to be mandatorily notified of all data breaches in Hong Kong. Given that the standard imposed will likely be one that results in significant harm, providing that a minimum number of individuals must be affected by the breach to make it notifiable, will not be necessary. The PCO can be tasked with providing the recommended minimum appropriate levels of encryption, in addition to being the entity charged with overseeing the policy on mandatory breach notification, and imposing fines and criminal penalties where organizations knowingly fail to disclose a breach or unreasonably delay the notification of a breach. The maximum levels of fines that can be imposed should be significantly high to serve as a warning to organizations to remain committed to the protection of individuals' information privacy. This 'command and control' approach ensures organizations strictly comply with the PD(P)O and the DPPs in their data-handling responsibilities, especially in the design of measures to protect the security of individuals' PII.

The PCO's weak enforcement powers had been previously noted primarily in the miniscule numbers of issued enforcement notices. As stated earlier, enforcement notices are only issued after investigation by the PCO to prevent the recurrence of the breach with non-compliance of the notice, a criminal offence — and only three and four of such enforcement notices were issued in 2017 and 2018, respectively! It is the author's understanding that the small number of enforcement notices issued was due to a change in the PCO's policy on 'relying less on regulatory power and increased emphasis on promotion and education'.[100] Notwithstanding, it is difficult to create a culture of respect and accountability towards individuals' PII if the PCO lacks, or continues to act without, 'teeth'. It is clear that a robust enforcement approach is required. Although the PCO has on its own initiative conducted compliance checks and investigation, it is posited that this is insufficient to ensure organizations' commitment and compliance unless their failures in those regard are duly punished by law. For example, significant level of fines should be

[100] A Lum, 'Data breaches in Hong Kong have jumped 80% in five years, now privacy watchdog wants more power and resources to give future investigations "teeth"' *South China Morning Post* (31 January 2019) <https://www.scmp.com/news/hong-kong/law-and-crime/article/2184530/data-breaches-hong-kong-have-jumped-80-cent-five-years> accessed 30 August 2019.

imposed for failure to comply with breach notification requirements, the implementation of a comprehensive information security program with adequate encryption measures and annual review of such program/measures, lack of thorough organizational investigation upon discovery of breach or for repeated data breaches and possibly, criminal charges laid for serious violations.

It is useful to note that although the government is aware of PCO's lack of enforcement powers, proposals for enhancing PCO's enforcement powers by conferring criminal investigative and prosecution powers on the PCO and to empower the PCO with monetary penalty for serious contravention of DPPs, to name but two, were not supported.[101] Some of the reasons given for the lack of support were, inter alia, the loss of checks and balances, possible conflict of interest if the PCO was conferred investigation and prosecution powers and that it will confuse data users over the PCO's role and will deter users from seeking help from the PCO to comply with PD(P)O requirements. The submissions received during the public consultation were also against empowering the PCO to require data users to pay monetary penalty for serious contravention of the DPPs. There were concerns that given that the DPPs are couched in generic terms, and can be subject to a wide range of interpretations, it can be a subjective judgment as to whether an act is a serious contravention of a DPP. Further, it is uncommon for a Hong Kong non-judicial body like the PCO to have the statutory power to impose penalty; to empower the PCO otherwise, would vest the enforcement and punitive functions in a single entity and that is undesirable.[102] While the decision arrived at then (in 2010) were unfortunate and arguably not supportive of a strong data security environment, the author opines that the time is ripe for an urgent review and refer to the position and the powers of the UK's ICO[103] and the Office of the Australian Information Commissioner.[104]

For better monitoring of security breach incidents (type of breach, number of people affected, fines imposed, criminal charges laid, and so forth) in Hong Kong and for future research purposes, comprehensive records should be kept by the PCO with the cooperation of Hong Kong's police force. In this regard, the author notes the PCO's publication on its website of completed investigation reports. Certainly, this is commendable as a searchable public database recording investigations into data breach incidents and/or alleged data breach incidences which has a three-folded purpose — it provides the required transparency of the PCO's investigation process, it helps organizations to better understand their responsibilities and therefore, encourages and improves organizational compliance.

It goes without saying that increasing important role and proposed enhanced powers of the PCO may be an 'unwelcome and unnecessary burden' to existing PCO personnel. Providing the PCO with new responsibilities without adequate resources is not likely to be effective since the efficacy of these responsibilities depends very much on whether the PCO has the requisite personnel strength and the budget to shoulder them. Indeed, the Privacy Commissioner recently urged the government to increase the

[101] *Consultation Report* (n 71).

[102] Ibid.

[103] P Rappo, J Gollaglee, and L Bullock, 'The Information Commissioner Office New Enforcement Powers' *DLA Piper Publications* (20 February 2019) <https://www.dlapiper.com/en/uk/insights/publications/2019/02/the-information-commissioners-offices-new-enforcement-powers/> accessed 19 October 2019.

[104] See 'Civil penalties — serious or repeated interference with privacy and other penalty provision' <https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties/> accessed 19 October 2019.

PCO's manpower by 50 per cent (from the current 69 to 105), continuing that the PCO would remain 'enterprise-friendly' until it got more teeth. It is clear that whether Hong Kong's information security can be given a clean bill of health depends on the government's acknowledgment of the increasing importance of information security and its commitment to ensuring Hong Kong remains at least on par with international norms.

An aside and yet related issue is that it should be borne in mind that unlike the US[105] and Australia,[106] Hong Kong does not have separate 'specialized' regulations for health-care facilities in relation to health consumers' personal health information. In the next review of the PD(P)O, policymakers and legislators in Hong Kong will need to consider whether to treat medical health information as sensitive data requiring additional safe-guards and whether a lower threshold for notification be required in event of a data leak of health information.

I. Final remarks

Before data breach notification laws existed, organizations were able to keep tight control of, and absolute secrecy about, any information technology security flaws or data security failures they experienced. Breach notification as an example of regulation by disclosure imposes not only reputational sanction on breached organizations but also serves to mitigate the harm caused by the data breach.

Against the backdrop of increasing data breach incidences and its impact on businesses and individuals alike, this article has examined Hong Kong's data breach notification position. It highlighted the flaws and weaknesses inherent in Hong Kong's existing legal framework for data breaches; our final conclusions are that each of these need to be addressed, strengthened, and where relevant corrected or even overhauled: — that breach notification should no longer be voluntary and to the discretion of the organization suffering the breach, but mandatory in prescribed circumstances; that purposefully drafted laws be enacted, and not just mere 'guidelines'; and that such laws must be properly enforced. A mandatory approach as opposed to a voluntary approach in breach notification attempts to advance the objectives of deterrence, mitigation, transparency through information and public confidence. Such an approach may help to change organizational culture to one of the greater respect and accountability for individuals' PII and strengthened corporate social responsibility around privacy and security. Adopting a mandatory notification scheme will ensure Hong Kong maintains its rightful place across international norms, as a modern, legally and commercially trustworthy and reliable jurisdiction, and at the same time continues to assure its citizens that the integrity and confidentiality of their PII will at all times be protected.

Acknowledgments

I wish to thank RH Gillan for his assistance in proofreading and editing this article.

[105] HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) Act.
[106] My Health Records Act 2012 <https://www.legislation.gov.au/Details/C2017C00313> accessed 28 August 2019.

Funding

The work described in this article was fully supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China [Project No. CityU 11610016].

Notes on contributor

Rebecca Ong is an Associate Professor, School of Law, City University of Hong Kong, HKSAR China. She holds a PhD from the University of Leiden and a LLM from King's College London and the University of Strathclyde. She is also a Barrister-at-Law from Lincoln's Inn, England and an Advocate & Solicitor of the High Court of Malaya (not practicing). Her research interests lie in information technology law, data protection and privacy law.