MANDATORY DATA BREACH NOTIFICATION: ITS ROLE IN PROTECTING PERSONAL DATA

Rebecca Ong*

Abstract: Data protection, an important aspect of the right to privacy, ensures that information about people is used fairly and properly. Among the regulatory measures that have been adopted to safeguard personal data is the requirement that individuals affected by a data breach be informed promptly, enabling them to act quickly and effectively to protect themselves from harm. At the same time, the existence of a duty to notify individuals affected by a data breach incentivises data users to adopt robust measures against data breaches. Many jurisdictions adopt a mandatory data breach notification system; this article examines the two leading notification models, the United States and EU models. It takes Hong Kong as a case study where there is only a voluntary system of notifying the Privacy Commissioner of any data breach in certain specified circumstances. It evaluates the operation of Hong Kong's voluntary notification system and examines the current moves towards adopting a mandatory notification system. It examines justifications for mandatory notification and how the notification mechanism works and concludes that mandatory notification is an indispensable element of an effective regulatory system.

Keywords: *Data breaches; data breach response plan; data protection principles; General Data Protection Regulation (EU); mandatory notification of data breach; Personal Data Protection Ordinance (HK); unauthorized access to personal information; US law and policy on notification*

I. Introduction

A data breach, which may lead to accidental or unlawful destruction of, loss of, alteration of, unauthorised disclosure of or access to personal data, may be malicious, unintentional or accidental. Malicious incidents are where attackers gain unauthorised access to personal information by hacking into computer systems or networks. Other forms of malicious incidents include phishing,[1] malware[2] and

* Associate Professor, School of Law, City University of Hong Kong. Email: lwong@cityu.edu.hk.

1 Phishing elicits information like usernames and password from a user to gain access to systems. It includes credential phishing, which involves the attacker tricking a user into surrendering his login details by e-mailing a link to a realistic-looking login page the user trusts, such as password reset requests from a bank or a web-based e-mail provider.

2 Malware is a software which is specifically designed to disrupt, damage or gain unauthorised access to a computer system.

ransomware.[3] Unintentional events include the theft of laptops and USBs. Accidental events that lead to data breaches include loss of personal computers, USBs and memory sticks, inadvertent sending of personal information to a wrong recipient and failure to dispose of personal information securely, such as improper shredding of confidential documents.[4]

Intruders who gain access to computer systems or networks do not always carry out such attacks for financial gain. Often attacks are politically motivated, for example, hacktivism or hacking for a political purpose by defacing websites or carrying out denial-of-service attacks; or they may be carried out by an organisation's disgruntled employees or by pranksters merely to "test" the organisation's IT security system.

A report by Surfshark showed approximately 15 million data records were exposed worldwide through data breaches during the third quarter of 2022. This figure had increased by 37 per cent compared to the previous quarter.[5]

Given the ever-increasing incidents of data breaches affecting various industries globally, this article first considers the effect such breaches can have on individuals and organisations. It then proceeds to briefly examine the data breach notification regulatory framework in the United States and the EU, drawing out the underlying purpose of data breach notification laws and the subtle differences between these two frameworks. Through a critical evaluation, the article examines what motivates organisations to report a data breach. It describes essential components of data breach notification laws and considers whether the breach disclosure laws are seen as a success or a failure. It then takes Hong Kong as a case study, where data breach notification continues to be voluntary and notes that the administration has recently expressed its willingness to adopt a mandatory notification system. The article concludes that, overall, a notification system is indispensable and that a mandatory notification system ensures data safety and empowers data subjects to better protect their rights and incentivises data users to adopt better data protection measures.

The Ponemon Institute, an independent United States research centre that conducts yearly data breach analyses, reported that the average global cost of a data breach for 2022 was US$4.35 million, a 2.6 per cent increase from 2021 and a 12.7 per cent increase from 2020.[6] With breach costs increasing over 15 per cent in the last two years, the findings suggest that loss caused by such data breaches may be passed on to the consumers by increasing the price of goods and services; 60 per cent of

3 Ransomware is a type of malicious software designed to block access to data or a computer system until a ransom is paid or other conditions are met.

4 Daniel Solove, "A Taxonomy of Privacy" (2006) 155 *University of Pennsylvania Law Review* 477, available at https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf (visited 5 May 2022).

5 Surfshark, "Data Breaches Rise Globally in Q3 of 2022" (19 October 2022), available at https://surfshark.com/blog/data-breach-statistics-2022-q3 (visited 5 January 2023).

6 "Cost of a Data Breach Report 2022" (IBM Corporation, July 2022), available at https://www.ibm.com/security/data-breach (visited 6 September 2022).

the surveyed organisations so raised the prices of their products and services.[7] The increasing frequency and scale of data breaches heightens the possibility of identity theft and identity fraud. Intruders of computer system networks, who steal personal and financial information, may use the information themselves or sell the information to third parties. When a breach occurs, personal information can appear on black markets within days, enabling criminals to sell financial, health and identity information,[8] causing various forms of identity, tax and loan fraud.[9] Notifying individuals affected by a data breach encourages them to be more vigilant against potential identity thefts and financial frauds. A contrary view has been expressed: to place the responsibility of protecting themselves against data breaches is to relieve the data holders from their responsibility of protecting data they hold.[10]

The greatest impact a data breach can have on individuals is identity theft. Victims of identity theft experience a loss of control over their personal information, a loss of confidentiality, identity fraud,[11] financial loss, unauthorised reversal of pseudonymisation, and damage to their reputation. Additionally, they may suffer other significant economic or social disadvantages. For example, the loss of sensitive personal information such as health data, political views, religion or trade union membership may increase the individual's exposure to discrimination and stigmatism. Aside from the social cost to individuals, considerable time is wasted and money expended by the data breach victim to analyse and mitigate the impact of the breach. Individuals whose personal and financial information was stolen but never used for fraudulent purposes would have suffered no financial loss but suffer unnecessary stress and inconvenience. Victims of data breach, even where they are not victims of identity fraud, may still have to take measures otherwise unnecessary to protect their personal information.[12]

To an organisation, the cost of a data breach can be both direct and indirect. The Ponemon Institute suggests the ten largest items of expenditure for an organisation are the cost of remediation, loss of customers, business disruption, regulatory fines, legal costs, public relations cost of stolen record, direct financial loss, notification

7 Shannon Williams, "Consumers Pay the Price as Data Breach Costs Reach All Time High" (Security Brief Australia, 25 August 2022), available at https://securitybrief.com.au/story/consumers-pay-the-price-as-data-breach-costs-reach-all-time-high (visited 14 September 2022).

8 Ablon Lilian, Martin C Libicki and Andrea A Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar" (RAND Corp, 2014), available at https://www.rand.org/pubs/research_reports/RR610.html (visited 25 August 2022).

9 Trey Herr and Sasha Romanosky, "Cyber-crime: Security under Scarce Resources" (June 2015) American Foreign Policy Council Defense Technology Program Brief, No. 11.

10 Sasha Romanosky, Rahul Telang and Andrew Acquisiti, "Do Data Breach Disclosure Laws Reduce Identity Theft?" (2011) 30:2 *Journal of Policy Analysis and Management* 256–286.

11 Identity fraud is committed when a fabricated, manipulated or stolen identity is used to gain a benefit or avoid an obligation. Real-life examples of identity fraud include using a stolen identity to make fraudulent purchases, or steal money, from a victim's account or using stolen personal information to open new accounts in the name of the victim.

12 Thomas Lenard and Paul Rubin, "Much Ado about Notification" (2016) 29:1 *Regulation* 44–50.

costs, credit card re-issues and identity theft repair and credit monitoring. Additionally, data breaches can have a negative impact on its stock prices.

Where there is no legal obligation to notify persons or entities affected by a data breach, organisations may prefer not to report or under-report data breaches out of concern for their business reputation and financial status. Alternatively, when an organisation is hacked, facilitated by poor information security practices, any unauthorised access to personal information is handled "quietly" and internally by the organisations concerned, with the organisations "absorbing" the losses incurred by the "breach" as a matter of customer service without the individual being ever aware of the unauthorised compromise to his personal information. The organisation's reputation generally overrides an organisation's need to inform affected individuals.[13] Organisations may also be conscious of the fact that a data breach disclosure makes traceable an otherwise untraceable security breach, bringing publicity to an event and thereby prompting costly investigative and legal action or regulatory scrutiny.[14]

Security breaches do not merely generate costs to organisations and individuals affected by a data breach; given the inter-connectivity and the inter-dependence between information systems and networks data breaches, they can propagate and affect others. In the language of economics, a lack of firms' information security causes negative externalities in the economy, which justifies government intervention in the form of laws aimed at reducing the costs of insecurity to society.[15]

For these reasons, there is a growing global trend towards enacting data breach notification laws, as evidenced in the United States, the EU and the Asia Pacific (Australia, South Korea, the Philippines, mainland China, Indonesia, Singapore and Taiwan).

Sections 2 and 3 provide an overview of the data breach notification regulatory framework in the United States and the EU. The United States is selected as it is the first modern economy that legislated against data breaches while the EU's General Data Protection Regulation (GDPR) is arguably the most significant development in data breach notification laws as mandatory notification requirements apply in all the member states of the EU.

II. Regulatory Framework in the United States

The United States policy and law on data breach notifications has been formulated and implemented at both Federal and State levels. California was the first United States' state to introduce notification requirements, which it did through the California Civil Code in 2003. Since then, all fifty United States' states have enacted

13 Paul M Schwartz and Edward J Janger, "Notification of Data Security Breaches" (2007) 105:5 *Michigan Law Review* 913.

14 *Ibid*.

15 Stefan Laube and Rainer Bohme, "The Economics of Mandatory Security Reporting to Authorities" (2016) 2:1 *Journal of Cybersecurity* 29.

data breach notification laws (the last state was Alabama).[16] Twenty-three states have followed California's legislative model.[17]

A. A review of relevant state laws

In California, s. 1798.29(a) of the Californian Civil Code requires "any state agency, person, or business that conducts business in California . . . or maintains computerized data that includes personal information, to notify Californian residents of the discovery of an unauthorized acquisition of unencrypted computerized personal information without reasonable delay".[18] Disclosure of the breach must be made, in writing or electronically, in the most expedient time possible, consistent with the legitimate needs of law enforcement. The Californian Attorney General must be informed where a breach affects more than 500 residents. Where the cost of providing the notice exceeds US$250,000 or the number of persons affected is more than 500,000, substitute notice in the form of conspicuous posting of the notice on the breached organisation's website and via major state-wide media for at least 30 days is required. The Californian law only applies to data breaches of *computerised unencrypted* personal information, thus incentivising organisations to encrypt data as only breaches of unencrypted data need be reported.

California's Consumer Privacy Act (effective in 2020) provides for new consumer privacy rights and business obligations with regards to the collection and sale of personal information. It provides a wider definition of personal information, including information that identifies, relates to or could reasonably be linked with you or your household (eg Internet protocol address, biometric information, geo-location data, etc). Consumers can sue for security breaches caused by the business's failure to implement and maintain reasonable security procedures and practices.[19]

Given that s. 1798.29(a) of Californian Civil Code has formed the basis of almost half of United States' state laws, the commonality of the laws is reflected in the mandatory requirement for the breached organisation to notify individuals affected by a data breach. Beyond this point, the state laws differ as to *inter alia* the scope of the definition of personal identifiable information, whether information is restricted to computerised data, what triggers notification, whether the Attorney General should be notified of the breach, the timing of notification and the penalties for non-compliance. These main features are as follows:

Personal identifiable information is information that enables an individual to be identified. Most United States' states consider a mixture of first name or last name,

16 Alabama Data Breach Notification Act of 2018.

17 Paul M Schwartz and Edward J Janger, "Notification of Data Breach Security Breaches" (n. 13).

18 California Legislative Information, available at https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29

19 California Consumer Privacy Act of 2018, available at https://oag.ca.gov/privacy/ccpa (visited 14 September 2022).

social security number, state driver's licence and financial account information. Some states include biometrics in their definition so that unauthorised access to biometric data is considered to be a leak of personally identifiable information.[20] Although state laws mainly relate to computerised data, there are others which do not.[21]

The triggering threshold varies between states. California has a low trigger threshold: a data breach need only affect 500 Californian residents for notification. Low trigger thresholds may be counter-productive since they diminish the notices' effectiveness by requiring notification where potential harm would be minimal, causing "notification fatigue". To minimise notification fatigue, other states[22] have adopted a risk-based trigger, requiring proof of "reasonable likelihood of harm or material harm"[23] while other states require that the breach has caused or is likely to cause substantial loss or injury[24] or a reasonable likelihood that the information will be misused.[25]

California's trigger is an acquisition-based trigger,[26] meaning that notification is required when an organisation has suffered or believes it has suffered an unauthorised acquisition of unencrypted computerised personal information. Acquisition-based triggers tend to favour consumer protection as notification is not left to the discretion of the data user organisation.

A notification must be made "within a reasonable period", most states opting for "in the most expedient time possible and without unreasonable delay". Other states require notification to be made as soon as is reasonably practicable or expedient but no later than 45 days.[27]

Failure to comply with state regulations usually attracts penalties and sanctions. This may include a fine or legal action for individual violations[28] or an institution of civil action for damages by the victims of a data breach.[29] The Attorney General or the state regulator may also be required to be notified of the breach.[30]

---

20 New Mexico, Washington and Texas. See BakerHostetler, "State Data Breach Law Summary: July 2018" available at https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf (visited 5 March 2023).

21 Georgia, Maryland, Massachusetts, New York and Utah. Massachusetts defines "data" as any material upon which written, drawn, spoken, visual, electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics: Security Breaches, Chapter 93H of Massachusetts General Law, s. 1.

22 Arkansas, Connecticut, Florida and Oregon. See BakerHostetler, "State Data Breach Law Summary" (n. 20).

23 Mark Burdon, Bill Lane and Paul von Nessen, "The Mandatory Notification of Data Breaches: Issues Arising for Australia and EU Legal Developments" (2010) 26:2 *Computer Law Security Review* 115. See also BakerHostetler, "State Data Breach Law Summary" (n. 20).

24 Michigan, Montana and Pennsylvania. See BakerHostetler, "State Data Breach Law Summary" (n. 20).

25 Maine and Maryland. See BakerHostetler, "State Data Breach Law Summary" (n. 20).

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

27 Maryland, New Mexico, Tennessee, Vermont, Washington, Wisconsin. Hostetler "State Data Breach Law Summary" (n. 20).

28 Florida, Idaho, Maine. BakerHostetler, "State Data Breach Law Summary" (n. 20).

29 California, Louisiana and Maryland. Baker Hostetler, "State Data Breach Law Summary" (n. 20).

30 New Jersey, New York, Virginia. BakerHostetler, "State Data Breach Law Summary" (n. 20).

B. A review of relevant federal laws

The United States has a number of sector-specific Federal privacy-related laws, such as the Federal Trade Commission Act, the Gramm-Leach Bliley Act and the Health Insurance Portability and Accountability Act.

(i) The Federal Trade Commission Act

The Federal Trade Commission is an independent United States law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. Its primary legal authority comes from s. 5 of the Federal Trade Commission Act, prohibiting unfair or deceptive practices in the marketplace. As an example, a decision and final order was issued concluding that a medical testing laboratory, LabMD, engaged in unreasonably deficient data security practices that may result in the unauthorised sharing of sensitive medical information that was likely to cause substantial injury to consumers and the privacy harm resulting from the unauthorised disclosure of sensitive health or medical information is in and of itself a substantial injury.[31]

(ii) The Gramm-Leach Bliley Act

This law, also known as the Financial Modernization Act of 1999, contains provisions intended to prevent the occurrence of data breaches. It requires financial institutions to keep their customers informed of their data privacy methods and strategies to prevent personal information from reaching non-affiliated third-party entities. The Act also requires the Securities and Exchange Commission to establish appropriate standards to protect customer information.

Section 504 of the Gramm-Leach Bliley Act regulates disclosure of consumer information. It also empowers the Securities and Exchange Commission to impose penalties on companies that fail to disclose the magnitude of data breaches, fail to properly detail their companies' policies and procedures in protecting consumer data or fail to implement adequate cyber-security measures.[32]

(iii) The Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act 1996 requires entities covered by the Act to notify individuals of a data breach of their health information.[33] Notification must be made without unreasonable delay and in any case no later than

---

31 See Federal Trade Commission, "Privacy and Data Security Update (2016)" (January 2017), available at https://www.ftc.gov/reports/privacy-data-security-update-2016 (visited 10 November 2022).

32 Daniel Farris, "SEC Uses Safeguard Rule to Sanction, Penalize Investment Firm for Data Breach" (Polsinelli, 1 October 2015), available at https://www.polsinellionprivacy.com/blog-five/2015/10/1/sec-uses-safeguard-rule-to-sanction-penalize-investment-firm-for-data-breach (visited 10 March 2022).

33 The Health Insurance Portability and Accountability Act 1996 s. 164.404(a)(1).

60 days after discovery of a breach[34] in writing or by electronic mail. It is dispensed with if after assessing the risk of *inter alia* the nature and extent of the protected health information involved, to whom the disclosure was made, whether the protected health information was actually acquired or viewed and whether the extent to which the risk to the protected health information has been mitigated, it is demonstrated there is a low probability that protected health information has been compromised.[35]

Violation of the Health Insurance Portability and Accountability Act's provisions attracts fines. There is no private right of action under the Health Insurance Portability and Accountability Act, although in *Byrne v Avery Center for Obstetrics & Gynaecology*, the Supreme Court held that where necessary the Act can provide the standard of care for common law negligence claims to be initiated against health care providers.[36]

(iv) Cyber Incident Reporting for Critical Infrastructure Act of 2022

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires "covered entities", that is, organisations in certain critical infrastructure sectors, to report substantial cyber-security incidents to the Department of Homeland Security within 72 hours after the organisation reasonably believes that a cyber-incident has occurred. Ransomware payments made in response to ransomware must be reported within 24 hours. It is expected that the Critical Infrastructure Security Agency with the Department of Homeland Security will soon define the scope of these requirements, including the scope of "covered entities" required to report, the definition of a "substantial" cyber-security incident triggering the requirement and the information that must be conveyed in any report to agency.[37]

III. Regulatory Framework in the EU

The EU has a comprehensive data protection regime under the General Data Protection Regulation[38] (GDPR) that came into effect on 25 May 2018.[39] Directive

34 *Ibid*., s. 164.404(b).

35 *Ibid*., s. 164.402(2).

36 *Byrne v Avery Center for Obstetrics & Gynaecology* (2014) 314 Conn. 433.

37 "Expansive Federal Data Breach Reporting Becomes Law" (Ropes & Gray, 22 March 2022), available at https://www.ropesgray.com/en/newsroom/alerts/2022/March/Expansive-Federal-Breach-Reporting-Requirement-Becomes-Law (visited 14 September 2022).

38 Other data breach notifications include breach notification provision for telecoms operators and ISPs as set out in regulation 611/2013 under the e-Privacy directive 2002/58/EC and 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 2016/1148. The Security of Network and Information Systems Directive was replaced on 16 January 2023 by Directive 2022/2555, which has improved the existing cyber security status in different ways, for instance by increasing the level of harmonization regarding security requirements and reporting obligations.

39 Previously, data protection in the EU was based on the Data Protection Directive 95/46/EC which is built upon OECD's 1980 Guidelines Governing the Protection of Privacy and Trans-Border Flows of

95/46/EC, which the GDPR replaced, enabled EU member states to enact their own notification laws, but there was no uniformity in their approach.

The GDPR not only introduced a uniform system throughout the EU but it is also wider in scope than the state-specific laws which were in place before this regulation came into effect. For instance, it applies equally to controllers and processors that are established in the EU and those not within the EU but where the processing of data relates to individuals in the EU. This means organisations that offer goods and services to individuals in the EU or monitor people in the EU will need to comply with the Regulations even though they are based outside the EU.

The GDPR defines personal data breach as "a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". Controllers are required to inform the supervisory authority when the breach is likely to lead to "a risk for the rights and freedoms of the individuals", meaning a case-to-case assessment is made as to whether there is a risk for the affected individuals.

Data breaches must be reported without undue delay not later than 72 hours to the supervisory authority after having become aware of the breach.[40] The notification must explain the likely consequences of the breach and measures taken by the controller to address and to mitigate the breach. Where possible, the type of breach, the number of those affected and the amount of records breached should be included. However, affected individuals must be notified without undue delay where the breach is likely to result in a "high risk to the rights and freedoms of the individuals" (a "risk-based approach"), unlike the stipulated 72-hour requirement under art. 33.[41] Since the Regulation also applies to data processors, a breached data processor must also notify the data controller who owns the data affected without undue delay.

Organisations can do away with individual notification where it can be shown that (i) the data was encrypted or (ii) measures had been taken where the high risk to the rights and freedoms of the individuals is no longer likely to materialise or (iii) when it would involve a "disproportionate" effort, controllers can make a public communication.[42]

In the EU, the level of fine in the case of a data breach depends on *inter alia*, the nature, gravity and duration of the breach, which includes the type of personal information affected, previous record of data breaches and the degree of the organisation's cooperation. Presumably, lower penalties would be imposed on organisations that promote a culture of data protection and are able to show they have taken the necessary measures to comply with the GDPR.

Personal Data seven principles. The regulation adopted to protect the privacy and protection of all personal data collected for or about EU citizens, especially in relation to the processing, use or exchange of such data. The OECD's seven principles are notice, purpose, consent, security, disclosure, access and accountability.

40 GDPR art. 33(1).

41 *Ibid*., art. 34(1).

42 *Ibid*., art. 34(3).

Despite GDPR's ability to levy significant fines, it has been reported that "the vast majority of organizations are not being fined for failing to protect customer's data and where organizations are fined, the majority of the fines are too small to register with the organizations that are being penalized",[43] demonstrating a step backward for the GDPR, which needs to be urgently addressed.

IV. Objective of Notification Laws

Primarily, notification requirements seek to achieve two objectives: to promote the individual's right to know thereby enabling him to mitigate against the risk of unauthorised disclosure of his personal information and to provide a market-based incentive for the enhancement of organisational information security measures.[44] The latter is to encourage the adoption of encryption technologies for better protection of personal information and the reputational sanction that follows as a result of a data breach disclosure. The dual objective underlining data breach notification laws demand a "delicate balancing act" that requires gauging the risks of providing adequate notification to individuals while attempting to minimise corporate compliance cost burdens relating to unnecessary notification.[45]

Not all data breaches require notification: exemptions are seen as an integral part of data breach notification laws to minimise the scope of notification. I list three types of exemptions: (i) exemptions for information that is publicly available; (ii) where the organisation after due investigation determines that there has been no breach or a breach that has occurred is unlikely to result in harm to the affected individual and (iii) encryption safe harbours. Given that data notification laws are intended to prohibit the unauthorised disclosure of personal information, as long as there is no violation of the individual's privacy, there is no need for an organisation processing widely known information about an individual who is a public persona to inform him.[46] Notification is also not required if upon reasonable investigation, it is found that a breached security system has not resulted in or is not reasonably likely to result in substantial economic loss.[47]

---

43 Josephine Wolff, "How is the GDPR Doing?" (20 March 2019, Slate), available at https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html (visited 30 July 2022).

44 Paul M Schwartz and Edward J Janger, "Notification of Data Security Breaches" (n. 13). See also Thomas J Smedinghoff, "The State of Information Security Law: A Focus on the Key Legal Trends" (2008) 37:1–2 *EDP Audit, Control & Security Newsletter* 1–52, available at https://www.tandfonline.com/doi/full/10.1080/07366980701838449 (visited 10 April 2023).

45 Mark Burdon, "Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws" (2010) 27:1 *Santa Clara High Technology Law Journal* 63.

46 Note further that personal information collected or exchanged, eg for public safety and the safeguarding of prevention, investigation, detection or prosecution of criminal offenses, is exempt from GDPR. See GDPR art. 23.

47 For example, see Arizona's trigger threshold of "reasonable investigation and likelihood of substantial economic loss".

Organisations can avoid being subjected to notification requirements by encrypting all electronically stored data; in other words, once sensitive personal information has been encrypted in accordance with the requirements of the relevant state statute, it no longer poses a threat and thus no longer requires the breach of encrypted information to be disclosed. An encryption safe harbour relieves the organisation from the expense and humiliation of having to send out breach notifications to victims of data breach.

Encryption safe harbours are therefore intended to reduce corporate over-notification of data compromise and to avoid notification fatigue. Three types of encryption harbours have been identified: (i) no notification is required where encrypted data is breached; (ii) unless harm is proven to exist, no risks exist and notification is not required where the breach involves encrypted data and (iii) where encryption is treated as merely a factor to consider when assessing the risk to individuals whose records were breached.[48] The United States' data breach notification approach leans towards the first two types of Jones' encryption harbours. California's data breach laws, for example, require notification only when there is an unauthorised acquisition of *unencrypted* computerised personal information. Thus, encryptions used in encryption safe harbours like in the United States are seen more as measures undertaken to reduce compliance cost and are regarded as a market-based incentive to encourage the adoption of information security measures rather than to reflect the rights-based protection prevalent in comprehensive regimes seen in the EU.

The EU framework underscores the individual's right to know and the protection of personal data. Thus, information privacy principles stipulate the minimum standards regarding the collection, storage and use of personal data by data collecting organisations in comprehensive frameworks. As compared to the United States, information privacy rights for individuals and organisational obligations are established regardless of the sector/industry—they are seen as measures to remedy deficiencies in organisational obligations in the application of information privacy principles.

Given that the EU's comprehensive framework is non-sectoral, focussing on protection of personal data, the GDPR has a separate provision for "personal data breach"; in other words, the addition of the personal data breach provisions is to specifically address the phenomenon of data breaches. By comparison, the United States approach focuses on the curtailment of powers in combination with laws governing industry-specific practices seen in the likes of the Health Insurance Portability and Accountability Act. The laws in the United States were designed purposely to mitigate identity theft; hence they are fundamentally different to laws that are designed to provide and ensure protection of individual's personal data under comprehensive frameworks.[49] There is also the daunting task of regulatory compliance

48 Michael E Jones, "Data Breaches: Recent Developments" (n. 26).
49 Mark Burdon, "Contextualizing the Tensions and Weaknesses" (n. 45).

by United States organisations whose operations span multiple states since there are subtle yet significant differences in the states' regulations. For example, there is neither a standard definition of personal information nor a consistent mechanism for reporting data breaches. Consequently, United States' states that adopt a broader definition of personal information will have a broadened definition of the data breach. This is because the applicability of United States laws relates to the affected individuals' place of residence and not to the residence of the breached organisation.

V. The Motivating Factor

Is there a motivating factor that would incentivise organisations to invest or increase their investment in information security systems? Could the impact of a data breach on its share price be one motivating factor since, as previously observed, a possible consequential organisational cost arising as a result of a data compromise is the impact it can have on the organisation's share price?

A data breach's impact on the share price may be dependent on the type of industry of the breached organisation. While software vendors' share prices suffer significantly when information of their products' vulnerability is announced,[50] the impact on the share prices of other industries is inconclusive. One reason could be attributed to the lack of awareness by investors[51] in that, there is a lack of investors' appreciation on the "reality of damage", in other words, a lack of appreciation on the extent of damage a hacking incident, for example, can cause. In a physical incident, like the direct (or indirect) effect of an oil spill to the environment, the damages are clear and tangible but in a denial-of-service attack on the operation of a website, much depends on the length of time and the extent of the interference.[52] The positive impression that might be gained in protecting and securing individuals' information vis-a-vis the relatively limited effect information security investment can have on the organisation's share valuations does call into question the rationale for making these investments in the first place.[53]

---

50 Rahul Telang and Sunil Wattal, "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Prices" (2007) 33:8 *IEEE Transactions on Software Engineering* 544–557.

51 Anat Hovav and John D'Arcy, "The Impact of Denial-of-service Announcements on the Market Value of Firms" (2003) 6:2 *Risk Management and Insurance Review* 97–121.

52 Anat Hovav and Paul Gray, "The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis" (2014) 34:1 *Communications of the Association for Information Systems* 893–912.

53 Joseph H Anthony, Wooseok Choi and Severin Grabski, "Market Reaction to E-commerce Impairments Evidenced by Website Outages" (2006) 7:2 *International Journal of Accounting Information Systems* 60–78. See also, Huyesin Cavusoglu, Bihendra Mishra and Srinivasan 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* 70.

Another way of understanding the impact of a data breach is to consider the losses relative to fraud.[54] If it is true that on average, businesses lose 5 per cent of their annual revenue to fraud and that the cost of a cyber-event or a data breach represents only 0.4 per cent of the organisation's revenues, then one may conclude that the cyber-attacks and data breaches represent only a small fraction of the business liabilities that the organisation the faces. Given that it represents a small portion of the cost of doing business, there is little motivation for organisations to invest heavily in IT risk and security management.[55] Organisations are also likely to under-invest since the harms arising from a data breach are passed on to the affected individuals instead of being borne by the organisation.[56] Organisations do not directly suffer from the anxiety, stress, inconvenience and social disadvantage like discrimination and stigmatism as individuals do as a result of a data breach. It is therefore not surprising that "without legislative and regulatory frameworks, companies have no real incentives to invest in organizational security countermeasures".[57]

VI. Main Elements of a Data Breach Notification Regime

(i) One main consideration in shaping notification laws is the type of personal information that must be covered by the notification requirement. This is crucial as it determines the type of harm from which the law will protect individuals. A broad definition of personal information, for example, one that includes biometric information, can lead to a similarly broad definition of what constitutes a data breach.[58] At its core, the law should be one that applies to personally identifiable information that either directly identifies an individual or does so in combination with other information. Canada, for example, provides a broad definition, where "Personal Information" is defined as encompassing any factual or subjective information, recorded or not, about an individual, including, but not limited to, name, age, ethnic origin, religion, Social Insurance Number, email address, health information, financial information, biometric information, employee files, credit reports and education history.[59]

---

54 Sasha Romanosky, "Examining the Costs and Causes of Cyber Incidents" (2016) 2:2 *Journal of Cybersecurity* 121–135, available at https://academic.oup.com/cybersecurity/article/2/2/121/2525524 (visited 25 April 2022).

55 *Ibid*.

56 Ross Anderson and Tyler Moore, "The Economics of Information Security" (2006) 314 *Science* 610–613.

57 Anat Hovav and Paul Gray, "The Ripple Effect of an Information Security Breach Event" (n. 52).

58 See eg the California Consumer Privacy Act.

59 Phillip Yanella, "Mandatory Data Breach Notification in Canada: Understanding Your New Obligations" (Ballard Spahr, 13 September 2018), available at https://www.cyberadviserblog.com/2018/09/mandatory-data-breach-notification-in-canada-understanding-your-new-obligations/ (visited 21 April 2022).

(ii) The second element of a notification regime is to identify the type of data breach that requires notification. Generally, such a data breach would refer to an incident in which an individual's personal information is put at risk because of the exposure through loss, unauthorised access, acquisition and/or disclosure. The definition should be sufficiently comprehensive to cover financial risks due to identity theft and/or fraud but also to include other forms of risks flowing from the compromise of data such as discrimination and stigmatisation. References can be made to the EU's GDPR and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Under the GDPR, data breach is seen as a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed while PIPEDA treats data breach as a "breach of security safeguards" and defined as the "loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguard or from a failure to establish those safeguards". Given the era of Big Data, IOT and AI, the compromise of information should cover information contained on paper and electronically.

Further, providing illustrative examples of events that suggest that the data was compromised would serve as a positive step in reducing the uncertainties that may arise when identifying a potential data breach.

(iii) The third important element of a data breach notification regime is identifying the notification trigger threshold. This is dependent on whether the notification trigger is an acquisition-based trigger (similar to that adopted in California) or one that is risk based. In other words, should relevant authorities be notified when organisations believe there was an unauthorised acquisition of personal information or when there is a reasonable likelihood of harm or a real risk of significant harm?[60]

Tempering a notification requirement with a harm/risk threshold limits the frequency of events that trigger notification. Under a risk-based approach, the risk associated with a compromise of data is affected by many factors including whether the breach was intentional or accidental, whether the data was encrypted and the number of records compromised. Norm Archer et al. suggest four dimensions to the risk associated with a data breach:

1. How sensitive is the information? Was the information at account level or identity level?

   The sensitivity of the information is related to the severity and the likelihood of real and significant harm to individuals wherein the harms should not be limited to financial harms and economic disadvantage but

60 Note that South Korea (Personal Information Protection Act 2011 art. 34), mainland China (China Cybersecurity Law, 2018 art. 42), Indonesia (Kominfo Regulation 20 art. 28) and Taiwan (Personal Data Protection Act, 2015 art. 12) do not require a minimum standard of seriousness. The requirement is for affected individuals to be notified of all data breaches regardless of the type of breach or potential for harm.

also include harms that would result in social disadvantage: the damage to reputation, psychological distress and humiliation being possible consequences stemming from stigmatism and discrimination. Under the GDPR, the loss of control of data relating to sensitive personal information such as racial or ethnic origin, health or genetic data or history of criminal convictions is likely to be considered high risk for notification.

2. What was the extent of protection provided?

   This requires an assessment of the level of safeguards employed—whether firewalls and state-of-the-art encryption technology, for example, was installed.

3. How did the breach occur? Was it targeted, opportunistic or accidental?

   How the compromise happened must be considered alongside with the number of records breached and number of individuals affected by the data breach. A ransomware attack on a hospital information system, for example, would be seen as high risk not just due to the enormous amount of data held by the hospital but also because the breach can lead to delays in treatment due to re-scheduling of medical appointments and surgeries.

4. Has any misuse of information occurred to date?[61]

   In the example of a hospital data breach, were the patients' personal information used to illegally obtain prescription drugs or to submit medical insurance claims?

   Aside from an acquisition-based or risk-based approach, there is a third possibility—that notification should be given when there is unauthorised data access. The latter may not be favourable due to notification fatigue concerns but one that is worth considering where the unauthorised data access is paired with the reasonable likelihood of financial and material harm.

   Depending on the regulatory requirements, relevant authorities or affected individuals may not necessarily be notified.[62] It may be that upon conclusion of the risk assessment exercise, it is found that the breach had little or no significant effect on the individuals given that the data was encrypted, the decrypted key was not compromised and the data was effectively restored from a readily available back-up within a few hours. Even so, it is important for the breach to be documented to form a comprehensive knowledge base for the purposes of future research and policy-making decisions.

(iv) The fourth element is the time period within which notification must be given. Notification of the breach must be made as soon as possible within a time frame that is expedient and without unreasonable delay. The GDPR requires

61 Norm Archer, Susan Sproule, Yufei Yuan, Ken Guo and Junlian Xiang, *Identity Theft & Fraud: Evaluating & Managing Risk* (Ottawa: University of Ottawa Press, 2009), 98.

62 See GDPR, art. 34(1).

the breach to be reported without undue delay and no later than 72 hours while Canada's PIPEDA requires notification to be made as soon as feasible. Whatever the stipulated period may be, the right balance must be struck between risks that may result from notification delays and risks arising due to premature notification. On the one hand, delayed notification will undermine enabling affected individuals to receive accurate information and to take mitigating measures; on the other hand, rushed notification may cause unnecessary anxiety due to incomplete investigation.

Notification without undue delay is dependent on two factors, namely (a) the organisation's ability and capacity to detect breaches and (b) how the data was compromised. It may be that a breach is discovered months after it occurred, as in 2018, when Cathay Pacific Airways took seven months after a data breach was discovered to inform 9.4 million passengers across 15 jurisdictions of the data breach.[63]

Notification periods may be dependent on how data was compromised. A hacking or malware incident will certainly require more time for assessment and investigation when compared with an accidental physical loss or an insider negligent incident.[64] "Triggering threshold" needs to be carefully considered to avoid the possibility of notification fatigue. Aside from "prejudicing criminal investigations", it may be prudent to require data breaches to be notified "without unreasonable delay" or "as soon as practicable" instead of within an explicit time frame as in EU's GDPR of 72 hours since investigations into the data breach incident may not have been completed within the stipulated time period.

(v) Fifthly, legal consequences may follow the failure to comply with notification requirements. Public litigation may be initiated by a government agency such as the Attorney General or the Information Commissioner. In most private civil actions, the arguments raised are for lost time and money expended in resolving the fraudulent charges, lost time and money spent by affected people protecting themselves against future identity thefts and the loss of control over the value of their personal information.[65]

Through the threat of sanctions, data notification laws ensure that the purposes underlying the disclosure law are complied with, the rationale being the theory of deterrence under which compliance is treated as a function of (1) the probability of an offender being punished and (2) the severity of the penalty.[66] The negative sanctions provide the regulated community with a strong

63 "Cathay Pacific Executives Grilled Over Data Breach Crisis" (Reuters, 14 November 2018), available at https://www.reuters.com/article/us-cathay-pacific-cyber/cathay-pacific-executives-grilled-over-data-breach-crisis-idUSKCN1NJ0CN (visited 20 April 2022).

64 Fabio Bisogni, "Proving the Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution?" (2016) 6 *Journal of Information Policy* 154–205.

65 Sasha Romanosky, "Examining the Cost and Causes of Cyber Incidents" (2016) 2:2 *Journal of Cyber Security* 121–135.

66 See Tom H Tietenberg (ed), *Innovation in Environmental Policy: Economic and Legal Aspects of Recent Developments* (Aldershot: Edward Elgar Publishing, 1992). See also Darren Sinclair, "Self-regulation versus Command and Control? Beyond False Dichotomies" (1997) 19:4 *Law & Policy* 529.

incentive to avoid transgressions.[67] However, two factors can affect the level of compliance: (a) the cost of compliance and (b) the level of enforcement. If the cost of compliance (ie the cost of disclosure of a data breach incident) is seen to be higher than the cost of non-compliance (the imposition of a fine for failure to notify), there is a greater likelihood of non-compliance. Further, if enforcement is weak and the level of enforcement (the fine) is less than the level of compliance, then it makes more sense not to comply.

While it may be attractive to follow the GDPR and to impose significant fines, one must be mindful that fines are discretionary rather than mandatory and they are imposed upon completion of investigation on a case-by-case basis. The level of fine imposed may be influenced by the type and severity of the breach, the time the organisation took to assess, investigate and notify relevant parties, the types of personal information involved, the strength of the organisation's information security measures and the organisation's level of cooperation with the authorities. Also important is whether the organisation was a "repeat offender" of data breaches. A fact that the breach incident is not the organisation's first is clear evidence that the organisation's security measures are wholly inadequate.

VII. A Comprehensive Data Breach Response Plan

It is apparent that what matters most to individuals whose information has been compromised is to ensure that the notification of data breach is timely and the information provided is clear so that it informs the individual what information has been compromised, explains the risk involved in a language that is simple to understand, states the remedial measures that should be taken and lays out clearly what is required of the affected individuals.

Although months may have elapsed between the date of the data breach and the date of notification, I contend that the length of time can be reduced if organisations have in place an adequate data breach incident response plan that addresses all arrangements necessary in event of a data breach. The aim of the response plan is to provide practical guidance on ways to reduce the impact of a breach, meet the regulatory obligations and support affected individuals in minimising the risk of harm. Part of the data breach response plan includes improving the organisation's security protocols and policies to minimise the risk of a data breach and necessitating the appointment of a chief security information officer and the establishment of organisational risk management and information security teams who will be responsible and accountable for the assessment and investigation of data breaches.

The data breach response team may also be tasked to minimise immediate harm to the organisation, notify relevant authorities and affected individuals (where

67 Darren Sinclair, "Self-regulation versus Command and Control?" (n. 66), 534.

necessary) and prevent future breaches. This would require the engagement of IT security experts to assess the organisation's computer and network security systems and advise on the optimal security strategy for the organisation. As "prevention is better than cure", proactive monitoring and regular review and up-to-date security systems should be made mandatory for early identification of system vulnerability that may be exploitable. Needless to say, installing appropriate up-to-date firewall, detection prevention systems and anti-malware software is a necessity. Additionally, employee security training and awareness programs on data protection, data handling practices and knowledge of clear reporting lines will help employees recognise and prevent cyber-attacks like ransomware. This together with an organisational handbook on how to handle a breach will be a useful source of valuable information to mitigate the risks and to meet necessary obligations without delay. Proper and reliable back-up of data will also assist in mitigating the consequences of a data breach should one occur. Further, as a critical part of an organisation's cyber-risk management strategy, data breach simulations should be organised to test the organisation's security preparedness in the event of a data breach or cyber-threat. These measures will certainly help in possibly contributing to a lower fine being imposed by the relevant authorities should a data breach occur.

VIII. Data Breach Notification in Hong Kong

In 1996 Hong Kong became the first Asian jurisdiction to enact a comprehensive personal data legislation in the Personal Data (Privacy) Ordinance (Privacy Ordinance), drawing inspiration from the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980[68] and the EU Directive 95/46.[69]

The Privacy Ordinance applies to all organisations both private and public that collect, hold, process and use personal data (data users). The Ordinance covers any data relating directly or indirectly to a living individual (data subject), from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable. In this connection the Ordinance set out six data protection principles. They are as follows: (i) Personal data shall be collected for a lawful purpose directly related to the data user; (ii) personal data should be accurate, up to date and kept no longer than necessary; (iii) personal data should be used for the purposes for which they were collected at the time of collection or a directly related purpose unless the data subject gives consent otherwise;

68 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, available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (visited 28 September 2022).

69 Although the GDPR became effective in May 2018, thereby repealing the EU Directive 95/46, reference is made to EU Directive 95/46, which forms the basis of Hong Kong's Personal Data (Privacy) Ordinance.

(iv) a data user must take all practicable steps to protect the personal data against unauthorised or accidental access, processing, erasure or other use; (v) the principle requires openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used; (vi) data subjects are provided the right to access their personal data and to correct the data where necessary.

A. Government consultation on the privacy ordinance

In 2009 the Constitutional and Mainland Affairs Bureau of the Hong Kong Government conducted a comprehensive review of the Privacy Ordinance to examine in what ways the Ordinance could be improved; one of the matters that the review addressed was the desirability of introducing a mandatory or voluntary data breach notification system.[70] The consultation document observed that a mandatory notification system would impose an undue burden on business operations. The Bureau proposed that, in line with a number of overseas jurisdictions which have adopted a voluntary notification system, it would be prudent to start with a voluntary notification system. This would give the administration time to refine the notification system as it learns from experience.

The public views submitted during the consultation exercise[71] overwhelmingly supported the introduction of a voluntary notification system[72] with a small minority rejecting any requirement of notification.[73] There was some support for the introduction of a mandatory notification requirement, especially where a data breach was likely to cause serious harm or high risk to data subjects.[74]

Having completed the public consultation, the Bureau published its consultation report in October 2010.[75] It noted that the consensus was in favour of starting with a voluntary notification scheme, supported by guidance notes issued by the Privacy Commissioner's Office. The experiment of a voluntary notification scheme

70 Consultation document on the Review of the Personal Data (Privacy) Ordinance, August 2009, available at https://www.cmab.gov.hk/doc/issues/PDPO_Consultation_Document_en.pdf/ (visited 4 April 2023).

71 The submissions are attached to the Consultation Report in Annex 4. See Consultation Report on the Review of The Personal Data (Privacy) Ordinance, available at https://www.cmab.gov.hk/doc/issues/PCPO_report_en (visited 8 March 2023). For an overview of the submissions on the notification requirement, see Consultation Report on the Review the Personal Data (Privacy) Ordinance, paras. 3.7.6 to 3.7.19, available at https://www.cmab.gov.hk/doc/issues/PCPO_report_en.pdf

72 Those who favoured a voluntary notification system included the Bar Association, Freshfields, Microsoft, Hospital Authority and Office of the Government Chief Information Office. Some supporters of a voluntary scheme expressed the view that since the proposed privacy breach notification system is still at the initial stage of development, there was no clear standard for notification for a mandatory notification requirement to be introduced. A mandatory system may result in over-notification. The fear was expressed that a mandatory notification requirement might lead to a "notification fatigue". See eg the submission of Baker & McKenzie.

73 Such as the Hong Kong Investment Funds Association.

74 Those supported this included the Law Society, Consumer Council, Hong Kong Internet Society and Hong Kong Medical Association.

75 Consultation Report on the Review of the Personal Data (Privacy) Ordinance, available at https://www.cmab.gov.hk/doc/issues/PCPO_report_en.pdf

would allow the administration the opportunity of fine tuning the notification system having regard to the actual operational experience. The administration would also have time to assess the impact of the notification requirement with a view to making the system reasonable and practicable. The Bureau also explained that the Privacy Commissioner's Office would undertake promotional and educational initiatives to raise awareness of the guidance note issued by it, promote adoption of a privacy breach notification system by data users voluntarily and assist data users in making appropriate notifications.[76]

After the release of the Consultation Report in October 2010, the Bureau allowed a period of two months for further public representations and received a large number of submissions.[77] The large number of responses the Bureau received included a detailed submission by the Privacy Commissioner. The Privacy Commissioner referred to the voluntary notification scheme already in place and submitted that Hong Kong was ready for the introduction of a mandatory breach notification system. The Commissioner noted that it had received 80 voluntary notifications during the period 1 April 2008 to 15 December 2010. The Commissioner referred to its recently issued detailed guidance on when and how to notify a data breach: "Guidance on Data Breach Handling and the Giving of Breach Notification". With this notification arrangement in place, time was ripe for the introduction of a mandatory notification system. The Commissioner, however, made it clear that it was not proposing a fully pledged mandatory notification system immediately. It suggested that a mandatory notification requirement "could be introduced by stages to ensure a gradual process for the implementation with reference to the factors such as the amount of data being held by data users, the sensitivity of the data and the risk of harm that may be inflicted as a result of a security breach".[78]

Having considered the responses to its consultation report of October 2010, the Bureau submitted its report on the consultation in April 2011.[79] The Bureau reaffirmed its view expressed in its consultation document of October 2010 that Hong Kong should start with a voluntary notification system, with the Privacy Commissioner's Office being responsible for the administration of the voluntary notification system.

---

76 *Ibid*., paras. 3.7.21 and 3.7.23.

77 These submissions are listed in the Report on Further Public Discussions on the Review of the Personal Data (Privacy) Ordinance April 2011, available at https://www.cmab.gov.hk/doc/issues/Written_Submissions.pdf (visited 5 March 2023).

78 *Ibid*., the submission of the Privacy Commissioner, paras. 3.11 to 3.14.

79 "Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance" available at https://www.cmab.gov.hk/doc/issues/Report_on_FPD_en.pdf. For a helpful account of the 2009–2010 consultation exercise, see the response of the Privacy Commissioner on the Report of the Bureau on further discussion of the Consultation Report. The Commissioner's response is included in a LegCo paper submitted on 31 May 2011, available at https://www.pcpd.org.hk/english/data_privacy_law/amendments_2012/files/legco_paper_20110531_e.pdf

B. Voluntary notification system

Hong Kong's voluntary notification scheme was formally established in 2010. The Guidance on Data Breach Handling and the Giving of Breach Notifications (Guidance Note) in 2010 (revised in 2019) was issued by the Privacy Commissioner's Office providing useful information when notification should be made, for example, where there is a reasonably foreseeable risk of harm arising from the breach.[80]

While a voluntary notification system could be a starting point, it submitted that such a mechanism cannot be regarded as a permanent solution. There are three main reasons why such an arrangement cannot adequately address the increasing number of data breach incidents.

First, given the voluntary nature of the current mechanism, there may be under-reporting as organisations try to avoid possible damage resulting from making public data breach incidents; some may also delay reporting, as seen in the Cathay Pacific Airways data breach incident.[81]

Second, a data breach is a contravention of the data protection principles enunciated in the Privacy Ordinance. Section 4 of the Ordinance provides as follows: "A data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under this Ordinance." The fourth data protection principle requires the data user to adopt contractual or other means to prevent unauthorised or accidental access. Yet failure to comply with this requirement is not a criminal offence. It is only failure to comply with an enforcement notice issued by the Privacy Commissioner that constitutes an offence.[82]

Third, only a mandatory notification system can best guarantee that affected data subjects (i) are promptly notified of a data breach and (ii) are able to take necessary remedial measures such as cancelling a credit card or changing passwords. There will also be improved compliance with the Ordinance since organisations are likely to carefully reconsider their data collection policies and processes.

Fourth, voluntary breach notification "penalises" responsible organisations as they need to bear relevant costs and time to disclose a data breach making them less competitive when compared to irresponsible organisations.

Once considered a pioneer in data privacy protection, Hong Kong is now seen to be out of step with international developments, where we have seen a number of jurisdictions adopting a framework that mandates notification. The adoption of a mandatory approach eliminates inconsistency in handling data breaches, allows a

80 "Guidance on Data Breach Handling and Giving of Breach Notifications" https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf (visited 28 September 2022).

81 "Cathay Pacific Executives Grilled Over Data Breach Crisis" (n. 63). See also text indicated by n. 62.

82 The Commissioner may conduct an investigation into an alleged breach of a requirement imposed by the Ordinance (s. 38), for which the Commissioner has been given extensive powers. After the completion of an investigation the Commissioner may require the data user to take remedial measures or, in the case of a more serious breach, serve an enforcement notice on the data user (ss. 47 and 50). Failure to comply with an enforcement notice is a punishable offence (s. 50A).

level playing field for organisations and brings Hong Kong in line with global data protection practices.

C. Time for mandatory notification?

In January 2020, the Constitutional and Mainland Affairs Bureau of the Hong Kong Government submitted a discussion paper to the Legislative Council Panel on Constitutional Affairs on a review of the Privacy Ordinance conducted in 2019 and possible amendment of the Privacy Ordinance, including the introduction of a mandatory notification system. It recommended six amendments to the Privacy Ordinance.[83] They are as follows: (i) the introduction of mandatory data breach reporting, (ii) imposing requirements on setting out data retention policy, (iii) increasing Privacy Commissioner's sanctioning powers, (iv) regulating data processors directly, (v) expanding the definition of personal data and (vi) regulating doxxing.

The Bureau identified four requirements for establishing a mandatory notification scheme. They are as follows:

(a) *Definition of personal data breach*: Referencing article 4(12) of the EU's GDPR, a personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"; the government's paper recommended that a new definition of personal data breach be adopted. The new definition is important as it clarifies and distinguishes the breach from the more generic "data breach", which is used to refer to security incidents that impact non-personal and personal data.
(b) *Notification threshold*: The recommendation is for a data breach having "a real risk of significant harm" to be reported. The recommended threshold is thus a risk-based trigger rather than an acquisition-based trigger.[84] However, there are no further details as to what "a real risk of significant harm" threshold entails. For example, whether the data breach must affect a minimum number of individuals (eg 500 individuals, as is the threshold for California and Singapore) or whether the data should be encrypted (in California, notification is required where data breached was not encrypted). Additionally, no information is provided as to whether the Privacy Commissioner, the affected individuals or both the Privacy Commissioner and affected individuals should be notified. Presumably, the Bureau and the Privacy Commissioner's Office are still fleshing out the necessary details.

---

83 Legislative Council Panel on Constitutional Affairs Review of the Personal Data (Privacy) Ordinance, LC Paper No. CB(2)512/19–20(03) for discussion on 20 January 2020, available at https://www.legco.gov.hk/yr19-20/english/panels/ca/papers/ca20200120cb2-512-3-e.pdf (visited 7 March 2023).

84 Michael E Jones, "Data Breaches: Recent Developments" (n. 26). Note that the current threshold in Privacy Commissioner's Guidance on Data Breach Handling and the Giving of Breach Notifications is "real risk of harm is reasonably foreseeable".

(c) *Notification timeframe*: The recommended timeframe is within a specified timeframe (eg as soon as practicable and under all circumstances, in not more than five business days) wherein the Privacy Commissioner is empowered to direct the data user to give notification to the impacted individuals. Stipulating a notification timeframe will certainly avoid a similar incident like Cathay Pacific Airways in 2018, when the airline took five months to inform the Privacy Commissioner after the breach was discovered and seven months to inform 9.4 million passengers across at least 15 jurisdictions of the data breach.[85]
(d) *Mode of notification*: Notification to the Privacy Commissioner is by way of e-mail, fax or post. Information to be included in the notification include a description of the data security incident, the cause of data breach, the type and amount of data involved, an assessment of the risk of harm, the remedial action taken by the data user and the protective action that data subjects should take.[86]

The Hong Kong Government has now shown a greater willingness to implement a mandatory notification system, moving away from its committed view expressed in 2010 that voluntary notification system would better suit Hong Kong's circumstances. The voluntary notification system has been in operation for almost 15 years and has been improved over the years. The continuing breaches of data point towards upgrading the voluntary notification system to a mandatory notification system. In fact, an informal survey conducted by the present author in 2020 among private sector stakeholders from a range of industries—namely, commercial, banking, insurance, legal and medical on their views towards mandatory notification—found support for the introduction of a mandatory notification system, although concerns remain as to the reporting threshold and cost of remedial support to affected individuals.[87]

As of date, there does not appear to be any positive measures taken to introduce a mandatory notification system. The only measure that the government has taken has been to criminalise doxxing activities and to enable the Privacy Commissioner to investigate and prosecute doxxing.[88] While doxxing intrudes into an individual's personal privacy and causes psychological harm and harassment to the victims and their family members, I argue that the impact a data breach can have on individuals is the same if not more harmful. Nevertheless, I accept that the sentiment contributing to the speedy criminalisation of doxxing is attributable to the events related to the social unrest in the territory in 2019.

---

85 "Cathay Pacific executives grilled over data breach crisis" (n. 63).
86 Legislative Council Panel on Constitutional Affairs Review of the Personal Data (Privacy) Ordinance (n. 83).
87 In a semi-structured interview with private sector representatives, it was found that 50 per cent supported a mandatory scheme for better data protection. See Rebecca Ong and Sandy Sabapathy, "Hong Kong's Data Breach Notification Scheme: From the Stakeholders' Perspectives" (2021) 42 *Computer Law and Security Review*. Pg. 1–16.
88 The Personal Data Protection Ordinance was amended to criminalise doxxing on 8 October 2021 by way of the Personal Data (Privacy) (Amendment) Ordinance 2021.

As the Privacy Commissioner continues to comprehensively review the Ordinance and to formulate proposals for legislative amendments for *inter alia*, establish a mandatory notification mechanism and empower the Privacy Commissioner to impose administrative fines, I submit that while it is likely that the risk-based trigger will be retained as a notification trigger threshold for Hong Kong, it is uncertain whether the preference would be for the recommended single threshold of "a real risk of significant harm" or a two-level threshold as provided under the GDPR.[89] In addition, I argue that data breach laws would be more effective if they are proactive in nature; in other words, instead of imposing liability on organisations for failing to notify individuals following a breach, organisations should be penalised instead for failing to prevent the unauthorised disclosure or compromise of data. Consultations between the Bureau and the Privacy Commissioner's Office are on going but there is no timeline as to when the proposed amendments would be tabled for further discussion at the Legislative Council.

IX. Conclusion

Mandatory notification laws have been successful with evidence pointing to the rising data breach reporting numbers. In Netherlands, Germany and the UK, 15,400, 12,600 and 10,600 breaches were reported to the respective supervisory authorities in the first 8 months after GDPR took effect.[90] In Australia, the Office of the Australian Information Commissioner reported receiving 1,132 notifications (comprising of 964 notifications under the Notifiable Data Breach scheme and 168 voluntary notifications) between 1 April 2018 and 31 March 2019 as compared to 114 voluntary notifications in 2016–2017 and 107 voluntary notifications in 2015–2016.[91] The increase in data breach reporting is a reflection of the increased attention and compliance organisations are giving to information security, IT risk management and incident response plans.

Breach reporting obligations promote accountability, transparency and trust. At the same time, they provide an effective means of regulating businesses' data security practices to prioritise the protection of consumer data and relevant systems.

The success or failure of a notification regime depends largely on the policy objectives of such a regime. If one views disclosure laws as the individual's right to know that information has been compromised for loss mitigation purposes then

89 Threshold to notify regulatory authorities is "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" while threshold to notify affected individuals is when the breach is likely to result in high risk to the rights and freedoms of natural persons.

90 See DLA Piper GDPR Data Breach Survey: February 2019, available at www.dlapiper.com (visited 20 April 2022).

91 Office of the Australian Information Commissioner, "Notifiable Data Breaches Scheme 12-month Insights Report" (13 May 2019), available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/ (visited 29 November 2022).

the laws appear to be working. However, where the laws are seen as "sunlight" onto the organisations' security practices and thus "disinfecting" problematic security areas, data breach laws do not appear to be terribly successful, as evidenced by the increasing number of data breaches and data records compromised.[92]

In the United States, the laws were initially developed to address a specific concern—identity theft—whose numbers increased exponentially as a result of data breaches. The laws have since evolved to facilitate improved data security practices and to enhance individuals' knowledge of organisational data collection activities. The laws are far from perfect, but they appear to be working well in creating the necessary awareness of the immense value of personal information and the consequential harm from the standpoint of individuals and organisations. Although a "one size fits all" solution does not exist, it is possible to adopt a positive model for breach notification with the essential elements shaping the development of an effective data breach notification policy. Certainly, a new model that mandates preventive measures by organisations to avoid data breaches and penalises those that fail to do so is a step in the right direction.

Since 1996, the focus of Hong Kong's Personal Data (Privacy) Ordinance has been on the collection and the use of personal data. The increasing high-profile data breach incidents in recent years has resulted in the focus being increasingly tilted towards data security. In crafting the notification mechanism for Hong Kong, reference will be made to the experience gained from the EU and Australia. While earlier attempts to introduce mandatory data breach notification had not met with much success, we certainly expect to see light at the end of the tunnel in the not-too-distant future.

92 Joseph Schuessler, Delmer Nagy, H Kevin Fulk and Art Dearing, "Data Breach Laws: Do They Work?" (2017) 12:4 *Journal of Applied Security Research* 1–13, available at https://www.researchgate.net/publication/319357667_Data_Breach_Laws_Do_They_Work (visited 7 March 2023).