Data Privacy Law in the Language of Trust Relationship in U.S. and Singapore: A Model for Thai Personal Data Protection

By

Visakha Phusamruat

A dissertation submitted in partial satisfaction of the requirement for the degree of Doctor of Science of Law in the Graduate Division of the University of California, Berkeley

Committee in charge:
Professor Laurent Mayali, Chair
Professor Kenneth A. Bamberger
Professor Coye CheShire

Fall 2018
Abstract

Data Privacy Law in the Language of Trust Relationship in U.S. and Singapore: A Model for Thai Personal Data Protection

By

Visakha Phusamruat

Doctor of Science of Law

University of California, Berkeley

Professor Laurent Mayali, Chair

This dissertation aims at a better understanding of the role of data privacy law in promoting organization-individual trust relationship. It focuses on data security breaches in U.S. and Singapore, and the interactions of the regulatory designs, agency implementations and the emergence of organization’s post-breach responses towards affected individuals that reflects and reinforces the value of trust in their relationship. Examining the divergent approaches adopted by U.S. and Singapore provides lessons for a regulatory design for privacy in Thailand.

Based on the comparative analysis of the selected data security breach decisions from the key regulators in both jurisdictions—the Federal Trade Commission (FTC) and the Personal Data Protection Commission (PDPC)—and on the U.S. and Singapore’s organizational perception of privacy, the study found a divergence as to the U.S. and Singapore design and enforcement approach to individual-organization trust relationship. The non-right-based privacy of the Singaporean Personal Data Protection Act, coupled with the enforcement agency’s interpretation, constructs the direct venue and the gap for organizations to perform trustful behaviors towards individuals following the breach. Desirable post-breach responses from organizations are consistently witnessed from the PDPC decisions such as voluntary and prompt notification and remedies provided to individuals, and the Personal Data Protection Commission’s interpretation covers individual interests informed by values in the society. The regulatory design aligns its ‘no ideal of privacy’ with the organization’s perception and more established practices based on trust relationship on the ground and the PDPC mitigating criteria applied to induce organization in initiating voluntary post-breach responses towards better protection of individual privacy interests.

Despite more established culture of privacy among U.S. corporations, the integrated practices on the ground, and the long-standing enforcement against unreasonable data security practices under Section 5 of the FTC Act, its current mechanism does not facilitate a venue for trust relationships that drive organizational post-breach responses towards individuals. Unlike the PDPC, the FTC enforcement does not formally recognize post-breach responses of organizations consistently. In a small number of cases where
those post-breach responses were recognized, only limited normative implications can be inferred from those contexts. Much ambiguity and uncertainty due to the unclear boundary of liabilities set under Section 5 has left organization actors with high risks, without adequate assurance for organizations to perform desirable post-breach behaviors. The legal ideal of U.S. privacy rightness, as exemplified by Section 5, is based on the notions of self-control, independence and informational duties, and does not cover broader individual privacy interests, which could be promoted through trust relationships.

The U.S.’s consumer protection approach, in tandem with Singapore’s trust relationship based approach of Singapore provide a great lens for Thailand to meet the dual legal ideals of privacy rightness and promoting trust relationship. Thai specific conditions and this hybrid iteration have led to the implementation in a complementary ways. The pending Personal Data Protection Bill of 2018 and regulatory oversight should allow organizations with some limited space to practice exercising discretion towards desirable post-breach responses, alongside mitigating penalties imposed by the regulator to encourage these desirable practices. Rather than treating the breach notification and post-breach responses as reporting duties, the Thai Bill could offer an opportunity to cultivate privacy awareness and enhance an organization’s trustful behaviors towards affected individuals. The consumer protection provisions regarding advertisings could be interpreted by the Thai consumer protection agency to trigger investigations against unfair and deceptive data security practices, and regulate consumer contracts in businesses involved in handling sensitive personal data. This consumer protection-based model would provide a readily available means to protect consumer privacy interests, engage media and public vigilance to uncover breach incidents and increase individual and organizational awareness of privacy and data security.
A dedication to all teachers,

*Charlie & Skip,*

and their gifts for sharing
**Contents**

Dedication i  
Preface iii  
Acknowledgements v  

*Chapter 1* An Introduction 1  
*Chapter 2* U.S. and Singapore: Privacy Legal Ideals and Characteristics 20  
*Chapter 3* U.S. and Singapore: Data Security Breach Enforcement 58  
*Chapter 4* Post-Breach Responses and Trust Relationship: Evidence from Cases and Interviews 89  
*Chapter 5* Lessons for Thai Personal Data Protection Law 124  
*Chapter 6* Moving Forward 158  

Reference 164  
*Appendix A* Post-Breach Responses in the PDPC and FTC Decisions 172  
*Appendix B* Interview Excerpts: The Role of DPO in Enhancing Trust Relationship in Singapore through Data Breach Notification 194
This dissertation focuses on the way we understand data privacy and security before we talk about their problem. The author argues that today’s unentangled problem could arise from the current frame we look into this subject, thus inviting the audience to reexplore privacy from its conditioning. The author refers to this privacy conditioning as trust relationship—the process through which individual forms and maintains a relationship with others in the society, involving trust and distrust decision-making in everyday sharing of personal data—that continuously shapes and defines individual privacy as it goes. With this trust relationship lens, the author hopes to bring in an alternative way of understanding privacy that enables us to tackle the perceived problem at its root of our understanding and imagination of it—and therefrom, to reconstruct the conditioning for privacy forming in the next moment. Chapter 1 recollects from the compliance, law and trust scholarship to propose the overarching research questions of how law can promote trust relationship, assurance and openness.

In this dissertation the author explores data security regulatory designs and enforcement approaches in the three landscapes of the U.S., Singapore and Thailand, where the personal data protection bill has not yet been enacted. With focus on how each regulatory design and the key regulators in each jurisdiction paid attention into this individual-organization relationship concerning data breach, chapter 2 and chapter 3 of this dissertation set aims to first address the legal ideals fixed upon and envisioned by the legal structure, which were further implemented by the regulators in U.S. and Singapore. By applying comparative method to analyze the conditions placed by legal structure and regulator’s interpretation through selected cases, the author puts forward the implications for the divergent privacy ideals and approaches stemming from the cases of U.S. and Singapore: the ideals of self-control versus interdependency (trust relationship).

Mainly, the U.S. ideal on promoting self-control set upon the preconditions of informational transparency and equality principles, substantiated by informational duties such as disclosure obligations. Singapore, by contrast, rests on the pragmatic ideal of promoting trust in data processing business environment. This idea fixes on that an individual is able to depend on organizations’ reasonable judgment, their choices to exercise care in treatment of personal data and remedies when breach occurs. I illustrate these contrasts drawn out from the design of legal objectives and structures, the principles and venue emerged from the regulator’s interpretation. These divergences found in Chapter 2 and Chapter 3 are observable in terms of definitions of trustworthiness, subjects of protection, reliance on insider/outsider, legally protectable individual interests based on expectation and beyond expectation, aspects of harm and injury covered from economic loss and social protected values. Applied with encapsulated trust relationship, the author argues that the Singaporean regulatory design resonates this characteristic, which serves as a mechanism to reinforce trust within individual-organization relationship in combination with the legal assurance integrated into the design. Such characteristic of trust relationship is not apparent in U.S. regulatory design and enforcement, in which its current fragmented rules and lack of perspective line left relatively high risks and uncertainty for business actors to coordinate in compliance.
Chapter 4 continues to bring some evidence on the post-breach responses seen through the FTC and PDPC cases. The latter found the emerging desirable behaviors initiated by organizations in terms of promptness in notifying breach and remedies towards affected individuals beyond legal requirement. Such pattern correlates to the characteristic of Singapore regulatory design based on trust relationship that pave the venue to meet the organizational logics developed upon individual experience and trust in rendering post-breach response. The presence of state laws mandating data security breach notification in U.S. has obscured the visibility in observing trust relationship works underground. To this limit, some similar post-breach behaviors and corporations shared similar worldview on the individual relationship of trust deserves more in-depth investigation to see how it works along with the U.S. mandate SBN laws.

Chapter 5 takes us to the landslip site of the Thai personal data protection and the long overdue bill. Examining the 2018 revised Thai Bill in the U.S. and Singaporean models, the author explains the hurdles that causes each to be unfit within the present context of Thailand. Such context is based on the responses of regulator, business and individual actors from the very first data breach that received wider attention from the public early in this year. An adjustment is necessary in employing the U.S. and Singapore approaches to be in practical use within the constraints of Thai ideal of democratic identity and the loose soil that needs supports of trust relationship and cooperation. This, in turn, has led to the author’s proposal of consideration for a serpentine path, a hybrid approach that tailor for the Thai situation respecting the nation’s symbolic presence and substantive needs. In this limited context of Thailand, the author examines the possible condition that two ideals and approaches co-exist and complement each other.

With promises of some light onto the overarching questions—How law can promote trust relationship through the alignment and gap—the author identifies points of intervention or influence for legal architects to consider. This involves deconstructing the previously discussed multi regulatory designs for data privacy and security into the interplay of four elements: venue and structure, actors and character, force and flow, space. The author brings in the supporting evidence from the interview of data protection officers in organizations operating in Singapore to open up the reconstruction of law in connection with the present data breach situation, organization’s established worldview, and the ongoing meaning-making process of data security and privacy. In this attempt, the author calls for the consideration, along with other forces, this function of law residing in its communicative power, often unattended by most legal scholars. Four elements for legal intervention are addressed in the uncovered design of the open-unfinished gap, the opportunity lying on the confusion and ambiguities of meaning; the intrinsic interests in trust relationship, and alignments. Indeed, law could reposition to a subdominant role and open itself as a space for dialogue and negotiation of privacy and security meaning, and turn the momentous attentions of all players to trust relationship between individual and organization in privacy after-breach.

Taking a journey from the ideals to find possible converging point on the ground, the author aims to open more discussion on the role of law, in which law performs less active, but more reflective and coordinating to the established interests and relationships among players on the ground as an alternative to redesigning future of privacy.
Acknowledgements

The idea of this dissertation would not have been possible in the beginning without the generous space offered by Professor Mayali. It got a name, *Trust in the Language of Privacy*, given by Professor Morrill during the research design class. It was molded into the trust relationship after receiving advice from Professor Cheshire. Guidance from Professor Bamberger founded its sight and frame. Interviewees gave its voice to speak. Other pioneers in the field, Professor Schwartz, Richards & Hartzog paved and reassured its path. The Thai Government scholarship fed along its journey. The Habermasian tree built the shed for it to rest. Berkeley home nurtured its spirit. With endurance contributed by my beloved family, partner, and good friends, it strived for completion.

I wish to dedicate this dissertation to these intellectuals and the genuine connections in everyday life that inspired me and brought about the usefulness of this dissertation. All flaws are mine.
Chapter 1

Introduction

Abstract

This dissertation aims at a better understanding of the role of law in promoting trust relationship among business and individual actors. It focuses on data security breaches in U.S. and Singapore, and how divergent in their regulatory designs and agency implementations provide different accounts of how trust and cooperation values will be reinforced by actors in action.

Based on the analysis of selected data security breach decisions from the key regulators in U.S. and Singapore--the Federal Trade Commission (FTC) and the Personal Data Protection Commission (PDPC)--and the interview excerpts on organization’s perception on privacy and trust relationship, the study found that the Singaporean Personal Data Protection Act provides a platform and avenue for trust relationship to emerge among actors. This aspect has been amplified by the PDPC when implementing the law against unreasonable data security practices. By contrast, section 5 of the FTC Act and the FTC’s interpretation when enforcing against unreasonable data security practices do not provide similar platform or avenue for trust relationship and coordination among actors.

This can be explained from the divergence in the regulatory designs that portray different images and characteristics of relationships between business and consumers actors as to the trust and cooperative attitudes, dependent and independent relationship as expected by the law concerning data security breach. These legal predispositions, when carried on by the enforcing bodies through their interpretations on cases, have brought about different levels of motivations and assurance for business actors to deliver trustful responses to affected individuals from data breach. These are i.e. admittance of breach, corrective and remedial acts when the law does not require them to do so. In particular, it casts light onto the how the agency would mitigate risk and uncertainty involved in a situation in the way that would allow the businesses to be willing to act on consumer trust when the breach occurs. This attitudes, motivation and assurance provided by the regulatory design and agency implementation implies how relationship of trust will be taken into account by businesses in their responses towards individual, thus reinforcing trust into the business-individual relationship after the breach.

The interplay of trust relationship approach to a data security breach illustrated by the Singaporean approach, taken together with the self-control function in the U.S. approach have provided lens for an alternative design of data security protection in Thailand. The hybrid design will serve the situation in needs of promoting trust and cooperation while also fulfilling individual needs of data privacy and security rights.

Outline

The dissertation is outlined as follows. Chapter 1 introduces the problems, research design and literature review on law, data security breach and trust. Chapter 2 provides a contrasting picture of U.S. and Singaporean regulatory designs regarding data security breach— “the platforms and characters”, that reflects diffused values, attitudes and characteristics of relationships among actors viewed from trust and coordination accounts. Chapter 3 offers a view from the ground— how the agencies give force to the platform and vision of law in actions. Despite similarities found
in their interpretations of “reasonableness” when applying to data security practices, there remains several differences in the key areas which provide different venues and forces for trust relationship and coordination. These are mainly regarding whether and how they recognize organizational responses after the breach, how they characterize the business actors involved in data processing, and assign them with different roles of a principal and a intermediary as well as distinct liabilities thereof. The types and patterns of post-breach behaviors delivered by the organizations to affected individuals are examined further in Chapter 4 through the FTC and the PDPC cases on data security breach. At varying type, degree and level of consistency these beyond-compliant behaviors were found by the FTC and the PDPC cases suggest some evidence of norm emergence from the relationship of trust between organization and individual, in align with the organizational worldview on trust. This puts forward the implication on the alignment between legal functions to such norms on the ground, which could promote these trustful post-breach organizational behaviors towards better individual privacy protection. Chapter 5 brings the situation of data security breach in Thailand into contrast with those of the U.S. and Singapore, whereby such understandings call for these following aspects to be considered in the upcoming legal reform of data security protection: first, how a regulatory design can assign the right focal point to be carried on by the businesses in compliance; second, how the Thai regulatory authority can provide the right motivation to trigger a desirable action in response to breach. And finally, recollecting from the earlier chapters, Chapter 6 raises the question on how the law can construct a proper environment for trust relationship and coordination in a specific setting; that are, what elements are necessary, and which form is required to preserve such conditions in a given setting. This study proposes a rethinking of the gap and ambiguity of law as an environmental space for openness, a necessary element for reinforcing trust relationship between business-consumer parties following the data breach incidents. Among the uncertainty and risks involved in the organization’s post-breach responses towards individual, the design of data privacy law can assure organization with some right direction, infuse right values in connecting with organizational interests in trust relationship. Such design could reduce risks perceived by organizations in post-breach responses and allow them to initiate trustful behaviors towards individuals in remediing breach and promote better privacy protection.

Chapter I Introduction, Research Design, and Literature Review

A. Introduction

Personal data breaches have become the emerging issues that threaten individual privacy and security globally. The threats from unauthorized disclosures of personal data have exposed individuals to greater risks of identity theft, financial loss and reputational damage. These incidents have mainly resulted from cybersecurity attacks and weak organizational data security governance. The emergence and widespread nature of such threats have called for proper regulation: one that ensures reasonable data security practices by businesses in collection, use and disclosure of personal data while also facilitating the free flow of data.

So far, many jurisdictions have passed comprehensive personal data protection laws to tackle the issues, following the model adopted by the EU. Others have deviated from such approach. The U.S. adopted a sectoral approach in regulating businesses and protecting individual rights through consumer protection regulations and contracts. Singapore’s Personal Data Protection Act (PDPA) was passed to serve the economic aims of becoming a trusted hub for data processing businesses despite ‘no privacy rights’ found in its constitution. Thailand, with the constitution
guaranteeing individual privacy rights, has delayed the opportunity to implement such rights into laws regulating business conduct, leaving individual personal data unguarded in practice.

This dissertation focuses on data security breaches in U.S. and Singapore and explores how divergent regulatory designs and agency implementations provide different accounts from trust relationship and cooperation perspectives. The implications derived from the comparative study of the U.S. and Singapore’s designs and implementations will help not only to visualize a regulatory design that meets the overarching themes of striking a balance between protecting individuals and facilitating the free flow of data—but also to answer the questions of why and how—to set the right attitude and motivation for businesses to comply with and to promote trust relationship and cooperation in a jurisdiction. How a regulatory design can construct a proper environment for trust relationship and cooperation to emerge in complying with the law is the question to be explored in the U.S. and Singaporean approaches to data security that could be applicable to the case of Thailand.

The Comparative Analysis: Convergence and Divergence

From the comparative analysis of the U.S. and Singaporean approaches, the study found some commonalities of their established sets of criteria for determining reasonable data security practices. However, the different legal basis—of fair and non-deceptive principle versus statutory protection obligation—when applied to the same security breach issues, draws different images of characters and relationships among them. From this, there are asymmetries as to the scope of applications and the extent to which each applies to different characters, and how post-breach behavior could be considered as mitigating causes in determining breach and liabilities.

Such divergence in the U.S. and Singaporean approaches also has implications for the conceptualization of data privacy and security, including aspects of value protected in both jurisdictions. The U.S. ideal of freedom is cultivated through self-control over information of oneself, surrounded with individualism, distrust and independence. The Singaporean realistic freedom is sustained through trust relationship and cooperation and dependent on the respect of others in the society. As a result, individual values comprise the U.S. data security and privacy, whereas in Singapore, the greater extent of protection has grown beyond this to include social dimensions of self-embarrassment, reputational effects and trust.

From trust and cooperation perspectives, the U.S. and Singaporean approaches depict varying arrays of trust and cooperation being embraced in the designs of platform and interactions among actors therein.

First, different legal basis and their constraints place different legal assumptions on characters and relationships taking place among actors within the platform. Singaporean consumers and businesses are preset with attitudes towards trust and cooperation under the PDPA, while their counterparts in U.S. are not under the FTCA. Also, as a result of reasonable person standard under the PDPA, all individual interests on personal data have been entrusted to businesses. Second, the obligations and liabilities designated under the laws to different business actors have implications for mutual interests and cooperation among them in complying with the law. Unlike the U.S., the Singapore’s PDPA, with its implementation by the Commission, does distinguish between businesses acting for their own and those de facto acting on/for other’s behalf in processing data. Such recognition creates a clear boundary between them as to obligations and liabilities arising from unreasonable data security practices, while it also ensures that both will be held liable, separately, when they do not fulfill the protection obligations. The design, therefore, creates a mutual interest for actors to cooperate in preventing data breach, where failure could trigger both of them under the investigation.
Finally, how the remedial and corrective behavior is recognized and considered by the agency in determining penalties and directions has an impact on business decision-making in initiating trustful acts to affected consumer i.e. self-admittance of breach, self-correcting behavior and prompt remedying of a consumer. The Singaporean agency reduces inherent risks arising from such behaviors borne by businesses, i.e. bad images and creditability loss that are high enough to prevent them from acting in a favorable way to a consumer, by assuring them with an avenue for mitigating penalties and directions regarding breach. This corresponds to the interview with data protection officers in Singapore on motivation for notifying or not notifying data breach to affected consumers.

The absence of a similar formal venue provided by the FTC in countering high risks involved does not purport to encourage businesses in performing such trustful actions after the breach was discovered. The FTC, by directing respondents to establish a formal channel for receiving independent third parties’ reports on data security flaws, has further indicated that its approach relies heavily on these third parties in determining business trustworthiness, rather than leaving the matter to be resolved between consumer and business parties within an ongoing and direct relationship. This underlines the notion of trustworthy businesses under the U.S. fragmented approach in contrast to the trust relationship notion under the Singaporean regime.

On the ground, organizations in U.S. and Singapore shared the common view by relating privacy with trust and the organizational relationship with individuals becoming a factor when determining post-breach responses to affected individuals. By contrast, the evidence found through the FTC and PDPC cases suggests the fewer and lesser degree of trustful behaviors demonstrating by the U.S. respondents in comparison with post-breach responses from their Singaporean counterparts. This disparity indicates that the regulatory design and enforcement styles could play significant role in nurturing this trustful post-breach behaviors towards individuals. As in the PDPC case, the law and enforcement when infusing right value and motivation based on trust to meet organization’s interest could allow the organizational trustful behaviors to be rendered.

Therefore, as to the question of how divergent regulatory designs and the agency implementations provide different accounts from trust relationship and cooperation perspectives, this study argues that the answer lies in the translation process from the law in the book into the law in action: that is, how can trust and cooperative values embedded in the law be transmitted into business logic with which the business decisions have been made. In that process, the regulatory design together with the agency interpretation can construct a proper environment of assurance and openness to risks, and infuse trust attitudes and motivations into the legal climate for businesses to take into account when complying with law.

The Transplant and Translation

In my view, the lessons from U.S. and Singaporean approaches to data security protection and its implications for trust relationship and cooperation are relevant to the case of Thailand. The situation of data security breach in Thailand harms individual rights to personal data guaranteed by the Thai constitution. Despite the emergent threats from widespread data security breach, the personal data protection bill has not yet been passed to regulate business conduct, resulting in loss of trust in both government and businesses. Individuals also receive no remedies for damages caused from the breach. This has led to the question of how to optimize a platform for protecting individual rights to personal data while also promoting trust relationship and cooperation among actors in Thailand.
For the purpose of this dissertation, in transplanting the lessons learnt from U.S. and Singapore to data security protection in Thailand, it would be beneficial to deconstruct the designs and implementations into the basic elements: (i) platform or avenue refers to a construction or formal structure that provides assurance to actors in navigating the space; (ii) legal actors—individual or consumer actors, business actors and agency actors—those who perform and interact with others according to the roles and character designated to them under the law; (iii) flow and force refers to the movements resulting from the interactions of actors within the space; and (iv) the space refers to unregulated areas, gaps and ambiguities, either intended or unintended as created by the law, which are open to an actor’s improvisation. It is also helpful to refer to functions of law as instruments in constructing an environment for trust and cooperation among actors in two fundamental ways: assurance and openness. Trust and cooperation are discussed in this dissertation in two modes: an attitude affixed on actors in action; and a motivation or interest convincing actors in action. It is also inevitable to look into the similarities in the platforms, actors, forces and space to ensure that the transplant will find a way to connect with and be welcomed by the soil of the native land and its preserved values.

This dissertation assumes that despite the presence of right and non-right basis of personal data protection in different jurisdictions, these issues have similarities in that (i) data security breach issues present breaches of trust between consumer and business parties in the information relationship; (ii) an individual actor’s performs based on attitudes of trust or distrust, and one’s capacity to trust when making a decision regarding data privacy and security; (iii) the institution takes consumer trust into account when performing an act that risks countering its own profits or interests; (iv) the aim of regulation is to cultivate the right actions, which means action of business actors in favor of consumer interests.

The main considerations for transplanting are whether the transplanting ideology, concept and values would be well-received and yield desirable outcome on different soils. Therefore, the survey of the established platform, actors’ attitudes and behaviors, flows and force of openness of space is needed to ensure the viability and the smooth translation into the Thai landscape. This study found that there are choices of legal platforms under the established consumer protection regulations and the upcoming personal data protection bill. As for actors’ attitudes on trust and behavior in data sharing, individual consumers generally trust businesses in processing their data. Not only do individuals have low awareness of data privacy and security, but so do the businesses that have thus far not developed a culture of responsible personal data practices.

Despite the press reports on the recent large-scale data breaches involved popular social media platforms and Thai major breach incidents, leading to individuals’ withdrawal of trust in data sharing with businesses, forces from the press and public vigilance have played a limited role in putting pressure against the business and government, or in educating and raising awareness on the issues. Lack of information transparency is a major hurdle that causes the problems of information inequality in individual-business relationship, as well as the lack of transparency of a government investigation in the public domain. The space in Thai Society remains open for new values that align with democratization and individualism amidst authoritarianism, patronization and collectivism displaying in the background.

The condition of the Thai landscape therefore casts light on to the regulatory design that corresponds to the considerable needs of increased information equality between business and consumer in any transaction, and the increased transparency in government investigations against unreasonable business practices, which would raise individual and public awareness on data security and privacy. That said, the right design should promote the sense of individual control on personal data while also persuading business attitudes and behaviors to be more
accountable towards consumer trust. Examining the U.S. construction of a mechanism for self-control and the Singaporean mechanism for infusing businesses with the motivation and attitudes for trust relationship allows the study to propose considerations for the design of data security protection in Thailand.

B. A Research of Interests and Motivation

Privacy is an Elephant in the Dark Room.

My inquiry into privacy law began with some questions: What is privacy? If it is real, what does it look like? I have a general sense of what ‘privacy’ means, as I believe others do, but the meaning given will vary from one individual to another. Privacy is a subjective, of personal interests. How law can address privacy as a right is a challenging task in that such rights have to acquire some objective meaning without losing the subjective interest in it.

The frame to look at privacy is proposed by Solove’s understanding privacy (2008) in which clusters of today’s privacy problems can form a pragmatic approach to form legal rights. The problem-oriented approach could bring us to the needs of legal protection, but there remain some doubts on how it can prepare the law for the unimaginable future privacy problem. Further, today’s common theme of data privacy problem is somewhat agreed, but also varies by cultural norms that defines privacy boundary and interests at individual society level. For instance, what is perceived as privacy problem by a society may not be an issue for another. Should law and the attempts of legal harmonization provide a solution by elevating the status of an issue to become more common privacy problem?

A dichotomy of private and public space of privacy are widely discussed among scholars. But with the assistance of technology, any expression and forms of existence are data that links to the data subject. How such a distinction made by law can still relevant and effectively address the nature of privacy issues that blurs the physical boundary of space present another challenging aspect to tackle what we call privacy.

Tracing Privacy from A Relationship Thread: How it works on the ground

Privacy nature of being subjective, fast-changing in time and crossing limited bound of space makes an ambitious goal for law alone to properly tackle it. I, therefore, take a sideway and look back to the threads that weave the fabric of privacy and its very meaning. Such threads are relationships that involve decision of trust and distrust, which I refer to as trust relationship. Besides the spontaneous characteristics of trust relationship that goes as privacy goes, its internal force and function regulates behaviors of parties inside the relationship. My research motivation is to explore and start as a point of inquiry on this alternative way to address privacy from trust relationship, how law can find a way to connect and reestablish on it. So, a legal design could set toward better privacy, not to hinder it.

For the clarification purpose, not a definite conclusion, I view privacy as a two-way process of controlling information about oneself that involves expression of one’s meaning to the other, and at the same time allowing values held by another person or society to inform and readjust one’s own behavior in calibrating the intended meaning to others. From this view of privacy as a process or means to exchange values through the relationship, privacy is not a static space. This fabric and its edge, hold together by subject’s insecurity force, gives the form or the body aggregating values and meaning, so-called self-identity, self-image or persona. Data privacy clings on this notion for it refers to data identified by or with the subjects that are part of the bigger collages.
This research looks for this thread in a more tangible form of data privacy, organization-individual relationship and evidence of organization’s worldview through the privacy professional on the relationship of trust which matters to organizations’ responses to individuals after data breaches.

Tracing Privacy from a Legal Mold: How Law Treats It by Language and in Action

To understand how a legal design can promote trust relationship and privacy, it is to examine how law thinks about privacy in the first place. What are those ideal, images, characteristics of privacy and the expectation for the business and consumer to perform their roles regarding privacy. I assumed that today’s law and the agency interpretation provide factual evidence or descriptive account of what privacy is. As also being adhered by actors, law molds privacy normative, future-forwarding account of what privacy should be.

I applied outsider perspectives to analyze the legal design from the language, context of application, objectives and principles, established venue and structure of the relationships among business, regulator and individual actors to map out the characteristics drawn by the key privacy regulations, identified by scholars in the U.S. and Singapore. I found the diverged ideals and values of privacy grounded on the self-control in U.S. and the trust relationship in Singapore. The key regulators’ interpretations, the FTC and the PDPC has added more characteristics to the presence of privacy in both jurisdictions.

I borrow the lens from U.S. privacy scholars, Hartzog & Richards on the current view of U.S. privacy characteristics of individualistic approach forming around the independence, self-reliance and transparency in democracy and consumerism. They contrast this approach with the dimension of social relationship of trust, which they advocate for the inclusion of honesty, fiduciary to the way law addresses privacy issues in U.S. In part of Singapore, my inspiration has found on the Singaporean “no vision of privacy” and the consistency in the way in which the term ‘privacy’ has not been found in the law, but in the language of trust. Privacy scholars in Singapore shared similar view on this, but have not emphasized the relationship of trust that works behind the absence of law, and protect privacy interest in a formless, non-right basis. If Singaporean design could enhance better privacy through trust relationship, it could provide a substantive basis for the U.S. trust relationship approach to reflect on.

To the question of how law can promote trust relationship and better privacy, I put forward in sharp contrast with the U.S. that the Singaporean trust relationship approach, based on interdependence and social relationship, describes how privacy works from a human dimension to inform intersubjective notion of privacy in the information relationship. It also highlights the interdependent nature of the individual in society and the relevance of the law in the information age.

Where Both Ends Meet: Tie a Knot versus One Loose-End

Besides the evidence of privacy speaking from the thread of trust relationship and the thread of law, how and where both ends meet is a question to explore in the U.S. and Singaporean approach. The meeting point is a starting point for exchanging and transforming privacy meanings, which could provide an opportunity for a more uniformed practice of privacy law.

This research looks into the organization’s perception of individual privacy in U.S. and Singapore, how this threads of law and trust relationship speak to their perception, and whether it sounds enough to get interested in initiating proactive privacy practices towards individuals. It is noticing that organizations are the key actors who realizes privacy by passing on these threads in terms of direct experience towards individuals.
So, the answer to the starting question of how law can address privacy as a right without losing the subjective sense of privacy, keep up with the fast-changing nature and crossing physical border could be found inside the organization worldview and practices, in which law has choice to meet it and ties the legal language in tune with their operations, motivates them to deliver better practices. Or, law could stay and lead the ideal, disconnected, and depends on its command-and-control in forcing better privacy. What if the ideal defined by the privacy as a right becomes the hurdle towards proactive privacy practices itself. While the non-rights basis which ideals have not been affixed allows expanded protection of privacy interests. I chose to study the case of Singapore to see the possibility of this non-right basis where trust relationship has a chance to surface.

**Thailand as an Elephant in the Dark Room**

Thailand’s dual ideals are the destination of transplanting privacy lessons from U.S. and Singapore: privacy rights and privacy non-right based on trust relationship. Besides, its conditions of low privacy awareness and lack of organization culture of transparency also present the way to think about the limits faced by each approach when applied specific setting and a way for both to work in a complementary with each other. Privacy materialism and spiritualism does not necessarily mean to collide but works to converge in privacy reality.

**C. Research Design, Methodology, Materials**

_i. Comparative Law Methodology_

This dissertation approaches from a holistic viewpoint, applies the comparative law methodology, and the law interpretative analysis to examine the research question of how data privacy law can promote trust relationship. From a comparative lens, it aims to explain how divergent regulatory designs and implementations by the agencies provide implications for the emerging organizational trustful behaviors towards individuals in response to data breach.

The comparative law method provides an instrument to compare the similarities and differences as to the legal design and operationalization in the U.S. and Singapore through the selected data security breach cases. The analysis was made on the following points: the regulatory design and platform, the agency’s interpretation of reasonable data security practices and recognition of post-breach behaviors, the organization worldview and demonstration of post-breach behaviors observable from actors in both jurisdictions. The similarities and differences, convergence and divergence of these aspects found in the post-breach behaviors of organizations reflect back to divergent legal ideals and concept behind their operationalization in different societies where notion of individual privacy pervades and is being transplanted.

The methodology paved way for the assessment of innovative legal choices and functions of data privacy, based on rights and non-rights bases, devised by each jurisdiction to tackle today’s data privacy problems, and to protect individuals from data breach. The lessons learnt from the U.S. and Singapore broaden the way we understand privacy as shaped by the law and offer choices for better legal design for privacy and trust relationship in Thailand. On reflection, the specific conditions in Thailand also allow us to see through the potential limitations and complementary functions of the U.S. and Singaporean approaches.

_ii. Evidence and Materials_

This dissertation collected the evidence from the following materials: the legal statutes, legislative history, interpretative notes, guides, court decisions, regulator decisions relating to data
breach, government statements, news and publications, reports from the government website and local media, scholar publications and the data from the interview memoranda with data privacy professionals in Singapore. The core materials are as follows.

A. Language of law as Evidence of Legal Perspectives on Privacy Ideals

The language and contexts of FTC Act and related privacy regulations and the PDPA provisions provide materials for understanding legal perspectives, which serve as molds to shape different characteristics of privacy and values preserved by the law. The contextual analysis is made from the objective, purpose, principle, structure and gap of law. Based on the evidence found in the language of law, which does not only contain facts but also normative voice, the analysis in chapter II puts forward the claims of different ideals set by the laws on privacy values, images of and the relationship between businesses and consumer actors, and different accounts from trust and trustworthiness.

B. FTC and PDPC Decisions on Data Security Breach

The study examines the case materials of the FTC and the PDPC decisions on data security breach in Chapter III and Chapter IV. The following case materials are included: (i) the FTC decisions including complaints, and the settlement orders categorized with "Data Security" brought under the FTC Act section 5, and published on the FTC website until February 2018, comprising of 68 cases; (ii) the PDPC decisions determined under Section 24 of the PDPA and published on the PDPC website until February 2018, comprising of 32 cases. These cases involved organization's inadequate security practices for preventing unauthorized disclosure of personal data, regardless of whether actual disclosure was made or not, and whether the breach caused from the insider or outsider attack. The term does not exclude cases where the breach of privacy involved.

Chapter III examines the FTC and PDPC data security cases up until February 2018. The cases were selected from the criteria of similar causes of breach and nature of respondent businesses, details of which provides in chapter III. For the purpose of this chapter, the PDPC cases on the breach of individual consent section 13 are included to compare with the similar breach incident characterized by the FTC as data security issues.

These selected cases are categorized into three groups, as follows:

Group A. Cases of Outsider Attack: the FTC Re: Twitter, the PDPC Re: Orchard

Group B. Cases of Insider Breach: the FTC Re: Eli Lilly, The PDPC Re: Debt Counselling

Group C. Cases against Platform Actors:

(i) platform acting on behalf of another in Vision I properties and Social Metric;
(ii) platform acting on its own behalf i.e. data reseller and data brokerage.

The analysis identifies differences as to how the FTC and PDPC interpret “reasonable data security practices” which provides different implications for the notion of consumer, trustworthiness, recognize organizational responses after the breach, how they characterize the business actors involved in data processing, and assign them with different roles of a principal and a intermediary as well as distinct liabilities thereof.
Chapter IV further investigates the post-breach behaviors demonstrated by the organizations and recognized by the FTC and PDPC in these decisions. The purpose of this chapter is to look into the types, degree and consistency of these behaviors and how they were recognized by the PDPC and the FTC. Then, the evidence found on the organizational desirable post-breach responses i.e. breach notification and remedies will be examined with trust relationship lens to suggest that relationship of trust could be another force driven behind these organizational beyond-compliant trustful behaviors.

C. Secondary Sources: Interview Excerpts from Data Privacy Professionals

The study examines the organization’s perception on privacy and their practices in the U.S. and Singapore based on the interviews of data privacy professionals, excerpted from the book, Privacy on the Ground (Bamberger and Mulligan, 2015), and the CLTC project memo regarding the role of DPOs in enhancing trust relationship through the data breach notification in Singapore.

The interviewees from Singapore are 17 data privacy professionals in the organization operating in Singapore. Ten interviewees have the formal title of data protection officers (DPOs) of the organization; the others have the title of regional privacy officer, regional director of the public policy or privacy legal consultant, or the informal DPOs by default. Ten interviewees have other titles in the organizations such as auditor, chief information security management, CEO, COO, legal. Interviewees ‘organizations provide financial products for business and consumer, consumer brand, digital and technology products and educational service. There are ten global firms, one regional firm, three cross-bordered firms and three local firms.

The interview excerpts are examined with the case analysis in chapter IV to understand the post-breach responses and the indication of trust relationship influence behind the beyond-compliant behaviors of organizations in U.S. and Singapore. The excerpts are also used in Chapter V to provide some evidence in support of organization’s privacy perception and their decision-making on post-breach responses in Thailand.

iii. The Overview of U.S. and Singapore Data Security Breaches Landscape

In selecting the U.S. and Singapore for the case studies and applying lessons to Thailand, the table below provides a contrasting view of the U.S., Singapore and Thailand’s legal, social and political landscapes and data security breach. The unique legal designs and approach to data privacy based on the U.S. consumer protection and the Singaporean trust relationship form a good landscape for the studies and lessons for the legal reform in Thailand.

<table>
<thead>
<tr>
<th></th>
<th>U.S.</th>
<th>Singapore</th>
<th>Thailand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal System</td>
<td>Common Law</td>
<td>Common Law</td>
<td>Civil Law with Common Law</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tradition</td>
</tr>
<tr>
<td>Political System</td>
<td>Democracy</td>
<td>Authoritarian</td>
<td>Post-Authoritarian</td>
</tr>
<tr>
<td>Social Orientation</td>
<td>Individualism</td>
<td>Collectivism</td>
<td>Collectivism</td>
</tr>
<tr>
<td>Data Breach Situation</td>
<td>Major cases against tech provider - FTC as a key</td>
<td>Major cases against the traditional service provider</td>
<td>Recent cases against telecom service provider</td>
</tr>
</tbody>
</table>
regulator under section 5 and related consumer protection provisions. -PDPC as a key regulator under the PDPA -Consumer Protection on Advertising and Consumer Contract - Personal Data Protection Bill

<table>
<thead>
<tr>
<th>Privacy and Security</th>
<th>Constitutional Rights Origin of privacy concept</th>
<th>Non-Constitutional Right Transplant</th>
<th>Constitutional Right Transplant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative Individual Attitudes</td>
<td>High Distrust</td>
<td>High Trust</td>
<td>Relatively High Trust</td>
</tr>
<tr>
<td>Freedom of Press</td>
<td>Full</td>
<td>Restrained</td>
<td>Limited</td>
</tr>
<tr>
<td>Level of Threats from Technological Innovation and individual engagement</td>
<td>Complex</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

| C. Literature Review |

I. Conceptualization of Privacy Rights: Finding a Common Value?

How to define privacy and conceptualize privacy as a right fuels endless debates by privacy scholars. A non-uniformed view accelerates as privacy finds legal landscapes of different jurisdictions. (Solove, 2008).¹ Scholars propose ways to approach data privacy from the property and public goods (Schwartz, 2003; Acquistiti, 2014).² Others in EU found human-right basis of privacy. A more nuanced approach views privacy depends upon the specific situational context in which it operates and applies. (Nissenbaum, 2010).³

Data privacy regulations or personal data protection laws of each jurisdiction passed on different privacy values. The EU General Data Protection Regulations clearly ground privacy on the human rights basis of the EU 1995 directive on personal data protection. US decisional privacy inherits from a democratic polity and cultivation of the democratizing process (Schwartz, 1999)⁴. In Asia, Greenleaf’s Asian Data Privacy (2014) provides remarks on the resemblance of data protection laws in the regions, which have been developed into certain characteristics departed from the U.S. and EU approaches.⁵ Ess’ 2005 in the comparative study of Thailand, Japan and China, argues that data protection laws in these countries pursue the aim of advancing international commerce development rather than a nation's intrinsic goods and democratic

---

polity. The plural views conveyed by data protection laws across regions and different legal characteristics could obstruct in a significant way to the free flow of data in international business and commerce.

Greenleaf’s (2014) viewed Singaporean personal data protection law as a set of procedural rules for collection use and disclosure of personal data. Greenleaf comparative study of data protection law in the regions found on the data protection principles, without discussion on the philosophical aspects or conceptualization of privacy from sociology and compliance view, allowing this dissertation to take on the values of privacy preserved behind a set of procedures. Chesterman (2014) views data protection law in Singapore does not follow the individual subject right protection approach. Its aspiration rests upon addressing the technology problem, as a “future proof” and “technology neutral”, and driving its status to become a trusted hub for data processing business. This has led to the so-called pragmatic approach, which Chesterman described the aspect of striking “a right-based approach of EU with the laissen fair sectoral patches approach of US, with focus on how to deal with ever-expanding data available instead of whether to collect it in the first place.” Privacy has not been in the language of the legislation, or the vision of the country. Chesterman refered to Lee Kuan Yew’s speech, dated 20 April 1987, emphasized how very personal matters “who your neighbor is, how you live, the noise you make, how you spit or what language you use” will be taken care of by the government. This dissertation aspires by this ‘no privacy vision’ to enquire on the possibility that those similar to individual expectation of privacy from right-basis, or even the social values and interests beyond, may receive protection in the language of no privacy but trust relationship.

By asking how law promotes trust relationship, this dissertation examines whether trust relationship is a right frame, right angle to look into data breach and privacy, thus forming a basis for regulatory design for a jurisdiction. Through the cases of U.S., Singapore, Thailand, it draws the power of regulatory design that construct a proper environment for privacy to thrive through the trust relationship. In the selected jurisdictions of U.S. Singapore and Thailand, can the language of trust relationship spoken by law and enforcement actions can turn the data breach situation involved risk and uncertainty and loss of trust, to be an opportunity to promote individual-organization trust relationship?

This way privacy as rights serves as a reminder of underlying and already-existing relationship in the society and as by-products rather than the ultimate ends. This dissertation explores characteristics in a regulatory design based on trust relationship in which functions encourages organizations to reintegrate individual user experience as trust in its corporate logic, thus rendering socially desirable behavior in response to the breach.

---

10. Id. at xii, fn 3.
II. Privacy as Trust, Social Relationship, Contextual Privacy

Privacy law scholars, Helen Nissenbaum, Ari Waldman, Woodrow Hartzog and Neil Richards integrate social relationship and its context into the way of understanding privacy and design of law for better privacy.

Waldman’s ‘Privacy as Trust’ (2018) studies individual perceptions based on trust when sharing of personal data. He argues that to save privacy from extinction, the law should put stronger trust norms for trust when there is data breach. He claims that stronger trust norms will mitigate risks and encourage individuals to share more data and rebalance the power to individuals.11 ‘Privacy as Trust’ approach builds on the implications from Bamberger & Mulligan (2010) on the evidence of an organization’s concern on consumer trust, and takes on the Nissenbaum's contextual integrity, which, in the context of information sharing such matters as “who, where and when”, determines individual privacy and the norm. However, ‘Privacy as Trust’ omits the trust relationship aspect as found in Hartzog & Richards’ arguments on trust relationship and privacy, and further raised the lack of clear doctrinal legal approach, or the use cases in the latter.12 In response to Brunton &Nissenbaum’s recent work on ‘Privacy Obfuscation’,13 Hartzog & Richards claim that the ‘privacy individualistic approach’ as they found in Nissembuam’s proposition does not protect social relationship of trust. This relationship they claim as of fundamental value to be preserved for a society in their effort to strengthen laws on privacy from trust relationship perspectives, in which values of honesty, sincerity and fiduciary determine basis for legal principles.14 Hartzog & Richards raised concerns on the Nissembuam’s recent proposal on privacy obfuscation as a deterioration of the trust environment in society and a discouragement of hope on legal measures to tackle privacy issues.15

This dissertation places itself in this view of privacy laws from social relationship of trust perspectives, which focus primarily on the private relationship between organizations and individuals in personal data treatment and post-breach responses. It supplements existing discussions from an organization’s worldview of trust relationship that conditions organizational post-breach responses upon individual experiences and the interpretation of organizational response to a data breach. My predisposition on privacy, to some extent, overlaps and departs from privacy law scholars whose frames to initially examine the issues have been borrowed for this dissertation.

A Frame and Deviation

First, my view of privacy as a mechanism or process of control over information about oneself sits on the convergent point between Richards & Hartzog and Waldman’s perspectives. This means not only does privacy change the relationship as Waldman argues, but also the relationship itself also influences how an individual behaves in a way congruent with what would be interpreted by other persons or by a society’s norm to convey self-interests and self-expression

---

12 Id. at 5.
15 Richards & Hartzog, Privacy Trust Gap, supra note 14.
that forms an identity. My position also casts doubt on the mitigated risks as a result of a stronger trust norm as claimed by Waldman. I would agree if that refers to the perceived reduced risks by individuals, which encourages them to share more personal data. However, if that is what ‘Privacy as Trust’ aims to achieve, it can be argued that the law serves as an assurance, a trusted system, on which individuals can continue to share data. And, in contrast to what I refer to as an individual-organization trust relationship, the latter speaks to the direct and ongoing relationship in which an action of a party is motivated by the trust of the others in maintaining this relationship. I discussed this issue further in Section III.C on Regulation and Trust Relationship. It is to me that privacy protection needs to be addressed not from society as a whole, as Waldman argues, but at the individual unit of a relationship to really fulfill its legal purpose. Also, it is this trust relationship that allows protection not limited to an individual’s expectation from the time of data sharing to the time of breach.

Indeed, all the views from Waldman, Nissembuam, Richard and Hartzog are put together to complete a full frame for understanding privacy in my proposal to reframe privacy as a process of exchanges of meaning in a relationship in which it itself regulates the parties’ behaviors toward maintaining trust.16

In the end, Richards & Hartzog’s commentary asks why we need to build a forest to hide ourselves whilst the law still has a chance to revive trust relationship. The law as an instrument for promoting trust and a trust relationship will be discussed in privacy and security regulation in Section III.

This dissertation is framed based on trust relationship axis as closest proxy to privacy and what is a real stake in which law could align with when thinking of privacy rights. It merely looks into organic “means” of how privacy is shaping and reshaped based on individual trust and distrust decision in the ongoing and direct relationship between parties, even behind the corporate shield or a seemingly inorganic system. Trust relationship is privacy in operation. This dissertation does not aim to define values of privacy itself as trust or trust relationship; better privacy protection is the by-product of this trust relationship process. Relationship basis would bring a common ground to think about privacy in the making, the individual decision, and behaviors that transcend into organizational logic operated by the human behind organizations.

III. Trust Relationship as a Regulating Function of Privacy

This dissertation borrows Hardin’s definition of trust encapsulated relationship where a party in a relationship is motivated to act for the interests of the other party to maintain trust despite risks involved in performing such act.17 This ongoing, direct relationship between the parties that provides basis for a party to behave in a trustful way to the other party differentiates it from the notion of risk-taking and trustworthiness. Trustworthiness, which is often mentioned in privacy, is a quality pertains to an individual or a system based on one’s assessment. Such trustworthy character could be measured from a distance, from a third-party’s view, not a party in a relationship. (Cheshire, 2011)

16 Privacy-as-a-process is an attempt to control and readjust a self-image or self-meaning; an exchange within the relationship. Identity – a body of meanings, is more static, a result of the process of self-meaning-making.

Trust is an act of a person who exposes to a certain degree of his /her vulnerability to the control of another person in deciding the outcome. Therefore, a situation involving risks and uncertainties allows trust to emerge, and repeated act of risk-taking is essential for forming a trust relationship (Blau 1964; Holmes and Rempel 1989; Cheshire 2010). An act or decision on trust is only relevant where uncertainty and risk are present together; that is when some judgment is needed responsively to those unknown factors and possible outcomes. (Cheshire, 2011). In that way, trust act interrelates with control and risk-taking. After decision has been made, either it be trust or distrust, things are more certain in that way. (Luhmann,1979) Both trust act and risk-taking act are similar in that they seem to be counter-knowledge or counter-intuitive. The risk taker however does not need prior direct relationship experience between actors. Besides, unlike trust, the consequence of risk taking act is also found unreciprocated. (Cheshire, 2011). Similarly brought into privacy discussion are creditability and reputation, which relies on assessment of third party. Although, it could provide alternatives to relational trust when dealing with risk and uncertainty, and create image of high trustworthiness, perceived lower risks that leads to more cooperation (Cheshire, 2011).

Trust and cooperation are related concepts. Trust is an element in establishing cooperation, which in turn leads to productive societies. (Robert Putnam, 1995) However, other views put forward that trust is needed only when individuals are not trustworthy. Trust built into a relationship also gives a forward-looking view into the future cooperation. Trust may not require at first for cooperative interactions but growing important as relationships continue. Cooperation therefore is the decision to return trust, rather than keeping entrusted items. (Cook et. al, 2005) In compliance with law, trust and cooperation becomes relevant in explaining a party behavior to fulfill legal duty, coordinate with authorities or voluntarily perform beyond the legal duty. The quality of willingness in initiating such act in contrast to following the instruction or command to the agency or regulation distinguishes trust act from cooperative act.

In the information relationship, data sharing involves allowing personal data to be under the control of the other person or entity, being vulnerable to security threats and exploitation of the person with whom data is shared. For the situation of data breach, a party who is entrusted to process data needs to expose to a certain degree of vulnerability and takes risks in disclosures of one’s own mistake or fault to the party of such breached data. For corporations processing individual personal data, these risks are apparent as it concerns a violation of law, bad reputation and following lawsuits and loss of consumer trust. Eventually, lack of mutual trust could lead to the deadlock situation, where parties involved are reluctant to share data or disclosure of breach and remedies to one another. The literature suggests that lack of mutual trust between exchanging parties needs a unilateral risk-taking act of one partner to break the pattern. (Cook, Cheshire and Yamagashi, 2005.)

To the question of how law can promote trust relationship, this dissertation borrows the lens from trust relationship literature by perceiving trust relationship as the fundamental characteristic of information relationship. Risk-taking opportunity and exertion of will are the crucial part in forming as well as maintaining trust in information relationship between organization and individual parties. In a situation of data breach, it focuses on how a regulatory design and implementation of jurisdiction could speak to the existing trust relationship and provide risk-taking opportunities for organization party to act on trust in protecting individual interests in a relationship.
As the role law comes into play with the organization-individual trust relationship in privacy protection, the assurance provided by law could work to support and enhance trust relationships between business and consumer parties. Law can serve as a structural arrangement for avoiding or mitigating risk for parties to initiate trust act. A caution is that overreliance with assurance system could replace the relational trust between parties. Culture also forms a context of privacy and the low-risk and high-risk averse becomes a critical factor that governs the choices made for relying on system or relational trust. In observing the choice of regulatory design of data privacy in different contexts of U.S., Singapore and Thailand, it is foreseeable that culture pervades in the country and organizations’ culture developed around privacy and trust plays a significant role in how such choices will be made. Such commitment on values and context in privacy could mean varying level of organization’s commitment to render individual party experience or consumer trust from privacy practices, and to be perceived as a trustworthy party to the individual party within the relationship and/or the public. That said, a choice of a regulatory design between seeking to promote trust relationship or building a system of assurance would depend on the context and values committed by organizational behaviors in a particular jurisdiction. Strong legal mandate and narrower gap for risk-taking would be necessary to force organization to act in a trustworthy way in some jurisdictions. For others, the opposite and subtler forms of guidance and voluntary basis could be more desirable and found more persuasive for organization to render better privacy practices.

This dissertation does not provide an in-depth view of the privacy culture of organizational behaviors. It captures a glimpse of possible convergent worldview of organizations on trust of individual party that becomes a factor when determining response to individuals after the breach. In that way, it is conceivable that trust relationship could become a common factor, not just in language, that drives organizational behaviors across jurisdictions for proactive privacy practices, regardless diverse privacy concern and interest. It casts light onto a legal design that could tap into the organization’s perception on trust relationship, in which post-breach responses are part of internal risk management functions, to activate their desirable trustful behaviors to affected individuals in responses to data breach.

At this converging point of trust relationship and assurance of law, the process in which the language of law is translated into organizational logic and influence the way they make sense of post-breach responses, though not examining thoroughly in this dissertation, is hoped to inspire the future research.

**IV. Ambiguity in Data Privacy Laws, A Construction of New Meaning**

Ambiguity is the nature of privacy, agreed by scholars and practitioners. (Schwartz, Solove, Hartzog) Defining what is the personal data or identifiable data brings problem and methodology to be sought out by scholars. (Schwartz, et al. 2011). This dissertation does not deny the necessity of those definitions, but take an opportunity of privacy ambiguous nature and the lack of clarity from law at this moment to examine what could be in the benefit of doubt and confusion.

Essentially, sociolegal scholars Edelman (1992) and Talesh (2012) put forward that the inherent ambiguities contained in procedural rules on data processing would allow a business actor to construct the new meaning of law deviated from the original meaning. Speaking from trust lens, such ambiguities contain the risk and uncertainty components, allowing trust decisions
to be made and could be reciprocated by the other party. A unilateral risk-taking act of one party could crack the deadlock situation caused from the lack of mutual trust and keep the activities continue. (Cook, Cheshire and Yamagashi, 2005.) Data breach incidents could cause individuals becoming reluctant to share data with organizations. Bamberger & Mulligan’s Privacy on the Ground (2015) found that legal ambiguities in the area of privacy law could be an innovative means to reveal the practical meaning of privacy right as developed by data processing businesses in different contexts of the institutions. Reframing of privacy in align with actual business perception could lead to better policy outcome.

Indeed, the benefit of doubt and confusion shared as part of privacy experience right now allows a reinterpretation and a party’s act on trust to correct the situation to take place. Privacy law could be part of this reinterpretation and corrective behaviors, depending on whether such activities would fit or collide with the ideals and values advocated by the law. Following this view, the dissertation attempts to bring onto the surface the existing function of organization-individual relationship of trust, established in organization business and commercial practices before the pervasion of privacy. It asks whether this function is still relevant and to what extent it could be repurposed by the law for remedying breach of privacy.

To the question of how law can promote trust relationship, the dissertation takes the challenges and struggles faced by law and policy makers—due to these intangible, fast-changing, subjectivity, less-than-clear, non-physical confined nature of the privacy issues—to observe the creative solution lawmakers and regulators have sought outside the conventional way of applying force and the command-and-control of law. How law engages in this part of this reinterpretation of data breach and encouraging corrective behaviors is discussed in this dissertation.

V. Privacy on the Ground: Organization as a Meeting Point of Privacy Worldview

How does privacy on the ground works inside organizations in compliance with the law? Bamberger & Mulligan (2015) ‘Privacy on the Ground’ examines these key questions: (1) how organization perceives privacy; (2) what drives organizations to adopt privacy-proactive or beyond compliant practices; (3) the role of law in shaping an organization’s meaning of privacy; and (4) other factors that influence the process of meaning-making. The interviews conducted on the chief privacy officers of the U.S. based firms, identified by peer as leaders in privacy fields. They worked for the firms in major sectors such as health, financial service credit, and the unregulated sectors; half of those in technology sectors. The study points to an asymmetry between the fragmented legal system in the U.S. and the more streamlined practices on the ground developed by organizations. In proposing that privacy law aligns with corporate practices on the ground, the study views the success measured from the agreement of privacy management approach among corporations through procedural criteria, which that demonstrate greatest promise for vindicating the expansive definitions of privacy that society demand.18 The interview with nine U.S. CPOs found the corporations relates individual privacy with consumer trust.

18 Bamberger, Kenneth A. and Mulligan, Deirdre K., Privacy on the Ground: Driving Corporate Behavior in the United States and Europe (MIT 2015) at 11.
Perception of privacy is framed in terms of consumer concerns and business values in an ongoing relationship.

As with data security breach notification, the study conducted on seven information security officers demonstrated all organization participants’ fear of losing consumer trust on the brand and reputation from notifying breach to the public. From consumer perception, the 2007 survey conducted on US consumers also reveals the implications of the way in which that breach was communicated to them with the increased trust in the organization. The study called for introducing a more effective and uniform breach notification, which strikes a balance between ensuring a proper manner of communication as a remedy and not creating a too burdensome duty, resulting in increased operating costs for organizations.

This dissertation applies these questions from the Bamberger and Mulligan’s study to the interviews with the data privacy professionals in Singapore in the CLTC project memorandum. The small size of seventeen participants and the varying in their titles and the level in the organization provide limitation to the full comparison of two studies. However, the dissertation casts the light on whether similar worldview and practices on privacy are found on the ground of Singapore, as compared to the more established privacy culture in U.S. It is hoped to identify some common mechanism that drives individual privacy proactive organizational practices among different societies, regardless of diverse privacy values and interests. Besides, it observes the alignment between the legal ideals and the organization practices that could indicate some successful compliance.

The central focus of this dissertation was to examine an alternative approach to enhance personal data protection by promoting trust relationship as evident in the objectives, principles and characteristics of the Singaporean legal framework and the regulator’s decisions.

Singaporean contexts of non-rights privacy protection, the transplant of personal data protection paraded by international standards and the international business hub in Asia have created a unique site for an understanding as to how privacy norms take shape and the legal adaptability to introduce this concept in harmony with social changes.

V. Conclusion

Putting together, arguments in this dissertation situate where theories on trust relationship intersect with regulatory compliance with an aim to better understand how a law can motivate organizations to act on trust to individual affected from data breach without the requirement of law. Law could provide some degree of assurance as to the meaning of compliance, legal consequences from non-compliance and leave space where organizations can exert their will and their discretion to protect the individual privacy interests in form of individual experience.

20 Id. at 4, 15, 18.
21 Id. at 26.
22 Id at 30. From the 2007’s CSO study, a uniform standard of data that applies to all security breaches would ensure equal amount of information received by consumers, which allows the same opportunities for them to protect themselves.
Conventional command-and-control model forces organizations to comply with legal mandate, violation of which jeopardize an organization’s reputation and result in hefty fine. The element of voluntariness or willingness necessary for trust-building is subsumed by such force, thus resulting in cooperative action rather than act on trust. A self-regulation approach switches legal role to perform a subtler function of infusing specific values into the legal environment for organizations to internalize in practices. When such values align with organizational decision-makers values or logic, less effort or enforcement is needed to force socially desirable behaviors from organizations, thus voluntariness to act on trust is possible.

This dissertation explores trust-enhancing mechanism, where the law could leave some opportunity for organizations to initiate an act on trust for protecting the individual interest in a relationship. Such repeated act on trust would prevent the declined mutual trust between the organization and individual parties necessary for the free flow of data on balance with protecting privacy. It will employ privacy rights as a tool for generating trust in the information ecosystem and preserve human resources of individual well-being. While system trust or a legal assurance is indispensable in a particular jurisdiction lacking mutual trust, dependence may not lead to the desired outcome as compared to a cooperative force led by the enforcement agency. The latter could enhance trust in a certain period after operation. However, when reliance on enforcement and it fails, distrust attitude could increase. A more balancing approach striking a balance between of level of assurance and gap for business discretion could set the right motivation business operator to cooperate and exert trustful act that contributes to a sustainable system.

How can law promote trust relationship? The author examines the roles of law in leaving the unfinished gap for trust relationship to fill in the function of post-breach remedies towards individuals in the context of data security breach. In this gap, law in the language and action could assist organizations to take risks in delivering desirable post-breach behaviors by assuring with right view from the organization’s interest in trust relationship and assured them with favorable conditions when trustful behaviors have been delivered.

A comparative study of data privacy law implemented in the different context of society, cases of U.S., Singapore, and Thailand, put forward implications for the role of trust in information relationship and the possibility of finding a common language speaking of privacy through the lens of trust relationship. This commonness on the ground transcends cultural barriers and privacy shield of right and non-right basis, and finds a meeting of mind between legal ideals, organization’s worldview in the reality of organizational practices. The findings would contribute to a convergent point in trust relationship and regulatory compliance in the theme of data security privacy and security. It also brings about visualizing example and application of trust relationship to regulatory design that supports the proposal to reframe privacy from trust perspectives.
Chapter 2

A Comparative U.S. – Singapore Data Security Regulatory Landscapes: Privacy Legal Ideals and Characteristics

Chapter Abstract

This chapter addresses the question of how law promotes trust relationship and cooperation by examining the similarities and differences in the regulatory designs of the U.S. Section 5 of the FTC Act and the Singaporean Personal Data Protection Act, which have implications for trust relationship and cooperation. The comparative analysis focus in terms of how each design provides a platform and venue purported to promote trust and cooperation among relevant actors. It found significant divergences in the following areas. First are in the platforms, the basis of Section 5 of the FTC Act and Section 24, which confine the scope and values of protection. Second are the principles that shape a venue of interactions by predisposing actors with certain attitudes and characters, roles and relationships in their interactions with others. Third are obligations and duties between business actors, which creates motivations and drives for forming and maintaining trust relationship and cooperation. Fourth are powers of the enforcing bodies, tools and strategies employed for shaping behaviors of business and individual actors.

The Singaporean design illustrates the platform and venue that embraces the interrelated nature of information relationship in data processing businesses: the PDPA basis and principles posit that individuals rely and depend greatly on reasonable judgment of business parties to protect their interests in personal data, thus the design and enforcing body reinforces such ideal by creating assurance and motivation for encouraging businesses to directly initiate trustful act to individuals in resolving data breach issues while being cooperative with the Commission. By contrast, the U.S. FTC design rather casts towards the ideal of self-reliance and being autonomous: the current fragmented mechanism of Section 5 does not provide a direct venue or platform for trust relationship to stem between businesses and individuals. The unclear roles and obligatory boundary between businesses acting as data controller and data intermediary towards each other and individuals leave much ambiguities and uncertainties to these actors in checking on others as part of control. The FTC strategies under the restraint of section 5 cast only on the level of adequate and truthful information disclosures and discovery relies on third party such as media and independent researcher group. In Chapter 3, the author examines the implementations of the U.S. and Singaporean regulatory designs through cases analysis which provides further evidence on divergent approaches based on trust relationship and cooperation.

Chapter Introduction

Emerging threats to personal data from advanced cybersecurity attacks plus weak data security governance has exposed individuals to greater risks of identity theft, financial losses, reputational and emotional distress resulted from unauthorized disclosure of personal data. Organizations with data leakage also risk losing consumer trust, business reputation, and following enforcements and lawsuits. Due to the emergent and widespread impact from data breach transcending across boundaries, regulators call for the right approach to tackle this issue commonly encountered by most jurisdictions.
Despite the influence of the EU’s General Data Protection Regulation (GDPR) being a leading comprehensive model adopted and followed by several jurisdictions, the regulatory designs of U.S. and Singapore’s personal data protection portray distinct approaches deviated from the EU that are worthy of investigations. In general, instead of human-rights based approach to privacy and personal data, the U.S. borrows the consumer protection regulations and existing sectoral regulations to guard personal data and privacy and security from unfair exploitation. The FTC as enforcing body employs contract and information disclosure as measures to tackle businesses with unfair and deceptive conducts to personal data treatment. The FTC consistent interpretations and directions through cases, after years of enforcement, has emerged into certain standards of data security practices for businesses, so called The FTC Common law by Solove and Hartzog. Taken together, the applications of the FTC Section 5 to data privacy and security has developed a not straightforward platform and venue to personal data protection, marked by the fragmented relationship between parties and thus unevenly distributed duties toward businesses of different roles in data processing chain, and significant reliance on outsiders such as media, independent third parties auditors and researchers, to check on trustworthiness and credibility of businesses operating in the market.

Singapore’s Personal Data Protection Act (PDPA) represents an economic-driven approach to personal data protection with the clear goal of reinforcing trust in data processing businesses. Individual privacy, though not being recognized as rights in the Singaporean Constitution or in the making of the PDPA, has been regarded and protected in the light of such goal and framework of the PDPA. Its objectives, principles and language of the PDPA, as amplified by the PDPC’s interpretation, move towards the direction of encouraging individual-business trust relationship as part of accountability. The mechanism found in the PDPA all points to reinforce the direct relationship between individuals and businesses with the PDPC overseeing from a distance. The legal predisposition and ideals of Singaporean regulatory design is different from U.S. and the EU in that the right to privacy dissolves into the right to personal data, in which ideally individuals are expected to be able to depend on organizational reasonable judgment, or trust that they will respect individual privacy in organizational performance. In the author’s view, this approach makes a deliberative choice to bypass the controversy and endless discussion of what privacy is and the extent of right cloaked by abundant and subjective meanings of this term. Thus, it enables the author to unveil and observe privacy necessity or real needs that are not fueled by the demands of privacy activists and legal scholars.

This chapter is outlined as follows. First section provides an overview of the design of U.S. and Singaporean regulatory landscapes to personal data protection: Part LA focuses on the design of the U.S. FTC section 5 and relevant FTC regulations and Part LB focuses on the equivalent functions found in the PDPA. Both parts walk through these following questions: what forms the basis of “reasonableness” interpretation, what are conditions for their applications specific to nature of organization, activities and relationships with individual and other business actors, and what are values protected. Second section puts forward the divergent approach between the U.S. and Singapore’s regulatory design as to the platform, venue, attitudes and motivations, and role of the enforcement bodies. Deduced from there are the distinction as to ideal and characteristics of both designs for data security protection, which illustrates how varying aspects of trust relationship and cooperation performs as part of legal mechanism in a regulatory design. The finding leads to the understanding that the legal basis forms different images, characters and
relationships carried out by actors when performing and interacting with others. Therefore, in designing a trust-driven or trust-enhancing mechanism, it is in the very beginning that the law, either in plain text, objectives or principles, communicates to business actors of its desirable trustworthy image and values behind business-individual trust relationship in order to establish right motivations for businesses to act on individual trust regarding their personal data.

Section I: An Overview of U.S. and Singapore Data Security Protection Regimes

Part A. The U.S. Consumer Privacy Protection Regulations and the FTC: A Fragmentary Approach

I. An Overview

The Federal Trade Commission (the FTC) is a key regulator and enforcer in the area of U.S. consumer data privacy and security protection. The FTC regulations empower the FTC to investigate businesses whose conduct is against reasonable data security practices. Section 5 of the FTC Act prohibits the unfair and deceptive act in commerce and grants the FTC with powers to bring administrative or juridical claims against conduct it believes in violation of this Act. The FTC has consistently applied Section 5 to unfair and deceptive data security practices by businesses.

Since 2002 until this date\(^{23}\), the FTC has brought 70 data security cases based on unfairness and deception claims. In these cases, the FTC alleged the respondent companies that their failure to provide reasonable data practices during the collection, use, transfer, storage or disclosure of personal information relating to their business activities, allowed unauthorized access to consumer personal information.\(^{24}\) The FTC pursues action against the alleged practices on case-by-case basis rather than rulemaking.\(^{25}\) The Commission’s interpretation of whether a certain act is unfair or deceptive, and therefore unreasonable, has emerged into a common-law-like standard of practices adhered by businesses.\(^{26}\)

Besides Section 5 of the FTC Act, the commission has authority to bring actions against business practices in violation of the GLBA, the FCRA and the COPPA. These specific statutes require the covered entities to put in place proper safeguards to consumer data and specific obligations to comply when handling the protected data.\(^{27}\) While FTC Act does not allow private

---

\(^{23}\) As of April 30th 2018.
\(^{24}\) The number represents cases published on the FTC website tagged under category of “data security”. Respondents companies vary across industries, ranging from software developers and IoT providers, manufacturers, retailers operating web-based e-commerce, technical service providers, financial-related product and service providers to data brokers. The claims were brought against companies regardless of size and position in the business chain, either SMEs or multinational companies, upstream, intermediary businesses. In these FTC charges, size of breach varies from hundreds to millions of personal data being compromised at a single incident or multiple attacks. Type of information includes sensitive credentials, SSN, DOB, data on health and financial-related activity that could lead to information injuries such as identity theft, economic loss and physical harm and loss of reputation.

\(^{25}\) The FTC asserted that it has discretion to enforce against unfair practices through individual enforcement action rather than rule-making. Its interpretation of reasonableness standard, therefore, is based on case-by-case basis. (FTC’s Opp. Br. at 20, 22).


\(^{27}\) The scope of protected data under Section 5 of the FTC Act covers broad range of consumer data relating to commerce. As Section 5 generally prohibits unfair and deceptive act or practice in or affecting commerce, it does not limit the scope to specific type or format of data relating to commercial practices, but include all consumer data where failure to provide proper safeguard would create unfairness and deception to consumer as well as adverse effect on market competition.

The FTC defines “Personal Information” as individually identifiable information collected or received directly or indirectly, from or about an individual consumer. This typically includes information as follows; (a) a first and last name; (b) a
rights of action for affected individuals, those are available under the FCRA and COPPA. Most FTC cases however ended up in settlements between the FTC and the alleged businesses, with prohibition of further violating conducts, with requirements for implementing mandate comprehensive privacy or security program (the MCPSP), violation of which would trigger the FTC to file the claims with the court.

II. Basis for Reasonable Data Security Practices under the FTC Regulations

The FTC stated that “reasonableness” as a touchstone of its approach in information security. In the 50th data security action, it stated that a company’s data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.28

A. Reasonableness under Section 5 of the FTC Act: Unfair, Deceptive and thus Unreasonable

Section 5 of the FTC Act prohibits acts or practices in or relating to commerce that are unfair and deceptive. An act or practice is unfair if it causes or is likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves, and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(m). In exercising unfairness, authorities under section 5, the three-prong test must be met: (a) there is an unfair act or practice which has caused or is likely to cause injury; (b) there is substantial injury to the consumer; and (c) consumers themselves cannot reasonably avoid such an injury, which is not outweighed by countervailing benefits to consumers or competition.29 Applying to data security realm, the benefits of society come from free flow of data, innovation and capital formation.

The FTC has also been empowered under section 5 to bring a claim against a deceptive act or practice, which is a representation or omission that misleads or is likely to mislead the consumer. Such misleading representation, omission or practice of a company shall be material from an ordinary consumer understanding in particular circumstances of such practice. A failure

physical address including name of street, city or town; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other government-issued identification number; (g) a financial institution account number; (h) persistent identifiers associated with a particular consumer or device such as such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address; (i) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information (D-Link, Trendnet, Uber); (j) credit or debit card information; (k) credit report information; (l) an authentication credential, such as a username or password; or (m) any communications or content that is input into, stored on, captured with, or accessed through a computer including but not limited to contacts, emails, SMS messages, photos, videos, and audio recordings (Twitter, Snapchat).

Other statues provide specific protection to certain kind of consumer data. Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), also protects customer information of financial institutions. And, Sections 604 and 607(a), and 682.1(b) of the FCRA protects consumer report or consumer information derived from consumer reports for a business purpose.


29 The FTC always mentioned how simple, low-cost, and easily accessible and available of tools to prevent possible threats on practice in comparison with possible losses to consumers and society. In LabMD case where multiple attacks compromised the lab results of consumers, the FTC asserted that it was likely to pass the cost-benefit test if the incident occurs for second-time. From this, it can be inferred that the FTC perceived that the harm arises from both incidents was much likely to outweigh the costs of prevention. Otherwise said, it will be easier to for the FTC to hold multiple leak incidents unreasonable data practice. However, the agency has not yet adopted quantitative tools for measuring actual economic loss, i.e. estimated damages occurred to individuals besides its consideration of volume of data being compromised and number of individuals affected. Only in certain cases where the fraudulent charges were placed against the banks as a result from the breach that the economic losses were measured by the agency and stated in its complaints.
to honor any direct or implied representation made on its data security practice will constitute an actionable deceptive practice.

(i) Substantive Baseline from the FTC’s Unfairness Claims.

In the FTC’s response against Wyndham’s motion to dismiss, it further stated that “unreasonable data security practices are unfair.” (FTC’s Opp. Br. at 17). A substantive baseline for reasonable data security practices, deduced from the unfairness claims on the FTC, has evolved. There are common grounds in the FTC findings in cases. It finds a certain company’s practice unfair, and therefore unreasonable when a company fails to employ preventive measures against commonly known threats of security attacks despite the availability and accessibility of academic and technical resources for avoiding such harmful consequences on personal data. Further, it considers whether ordinary consumers without technical knowledge would have any ‘reasonably available’ means to be aware of security flaws and be able to help themselves.\(^{30}\)

Cognizable Injury. Unsettled issues remain on the type of injury, ‘actual’ versus ‘likely’, which is sufficient to provide basis for the unfairness claims against companies and considered as cognizable injury by the court.\(^{31}\) The current Commission led by Commissioner Ohlhausen has taken a more reserved interpretative approach on the substantial injury element out of the three-prong test; the agency laid claims based on the evidence of actual unauthorized disclosure rather than foreseeable data leak from poor data security practices.\(^{32}\) This means a company’s failure to provide adequate data security practice by itself without actual unauthorized access may not be sufficient to meet injury element of second prong under unfairness claim. Another ongoing issue is the recognition of objectively concrete and tangible injuries as opposed to intangible ones. Emotional injuries and reputational risk alone may not be independent basis for unfairness.

---

\(^{30}\) the FTC has brought the unfairness claims based on the company’s failure to provide take reasonable steps to secure its data practices during collection, use, transfer, storage or disclosure of personal information relating to its business activities, which allows unauthorized access to consumer personal information. For instances, the FTC's alleged unreasonable practices includes the offerings of products with security flaw built-in function that caused extensive collection of data on consumer behavior on the internet or tracking of private communication and sensitive financial data on the user's screen without consumer knowledge (FTC Matters concerning Compete, Upromise). The misuse of personal information occurs when, for examples, the company exploits such data by sharing with unauthorized third parties. (FTC Matters concerning Vision I properties) The unreasonable data security practices occurred due to improper data storage, for example, when data was stored without proper encryption (cite case), a company failed to assess vulnerabilities of its system or updating software to prevent well known security attacks (cite). In many cases, the company failed to limit employee or its service provider's access to data stored in the network, or failed to ensure compliance with internal procedure by having employee's training or contractual arrangements with third parties. Storing data without proper deletion and retention of database longer than necessary also considered unreasonable data security practices. (cite cases) It is also unreasonable if the practices do not encrypt the data or provide adequate means of protection from interception during data transmission. (cite cases). For IoT manufacturers or software developers, the lack of adequate code review or tests before distribution of products could result in the unreasonable and inappropriate functions on collection, use, transfer or disclosure of personal information. (cite case)

\(^{31}\) As for whether the mere “likely injury”, as opposed to realized injury, is sufficient to trigger an unfairness claim, there are still debates among the commissioners. On one side, the majority of the FTC in Wyndham case, Commissioner McGlenny and Brill, has made clear that the cognizable injury does not limit to “actual or tangible” harm, but “likely and intangible” injuries, which was opposed by Commissioner Ohlhausen.

\(^{32}\) However, in the Internet of Thing recent case of D-Link, the FTC dropped the claim after D-Link filed the motion to dismiss in which it argued that FTC lacked of evidence on direct and actual harm to consumer besides the claim of inadequate security safeguards in D-Link camera products. This was supported by Chairwoman FTC Commissioner Ohlhausen in her dissenting opinion blaming on FTC bringing charges upon baseless ground and the lacks of actual concrete evidence of breach or unauthorized access, nor any objective harms such as monetary, or safety and health risks posed to consumers has been found. [http://causeofaction.org/wp-content/uploads/2017/01/D-Link-MTD-2017-1-31.pdf](http://causeofaction.org/wp-content/uploads/2017/01/D-Link-MTD-2017-1-31.pdf). [https://www.cyberscoop.com/ftc-data-actions-ohlhausen-trump-d-link-case/](https://www.cyberscoop.com/ftc-data-actions-ohlhausen-trump-d-link-case/)
claims. This aspect places the limits as to the types of harm recognizable by the FTC to cover merely fraud and similar economic losses, risks to health and safety. Thus, disclosure of private information itself may not be sufficient to trigger claims.

**Whether an injury is substantial.** On substantiality element, among type of informational injuries discussed, those related to monetary, health and safety are often meet substantial requirement while a trivial subjective injury based on speculation and emotion is often disregarded. The FTC in Wyndham clarified that, in principle, the substantiality of claims could be quantified by the magnitude of harm and the number of consumers affected. This means small effects to large number of individuals could be considered substantial. In cases involving sensitive financial data leak which caused the affected consumer cancellation of credit cards and losing their access to checking account until the new cards had been reissued, the FTC considered “Lost opportunity costs and small out-of-pocket costs” of affected consumers falling under substantial injury. Similarly, in FTC Matter concerning TJX, the inconvenience arisen from requesting new SSN and driver license of affected consumer from the leak data was substantial injury. It is noticeable that FTC has never been pursued any action against the company’s practice affecting sensitive personal information of a single individual consumer. From this, it could be assumed that substantial requirement has not been met when one individual affected from the breach.

**Challenges on FTC Jurisdiction.** Despite the disputes raised by respondents on the FTC’s lack of authority, the court in Wyndham affirms the FTC jurisdictions over data security protection under section 5 of the FTCA. In the same case, the court also found that the terms used by the FTC such as “readily available,” “adequate,” “commonly-used,” and “proper” are sufficient without the need to specify any particularized standard for alleging unreasonableness of the respondent’s measures. The court was also satisfied that the FTC demonstrated causality between the alleged unreasonable conducts and subsequent data breach when it asserted several insufficiencies that draw reasonable inferences on the subsequent data security breaches.

---

33 So far, informational injuries that has been recognized by the FTC includes the followings: (a) Deception injury or subverting consumer choice; (b) Financial loss from fraud and indirect financial loss such as deprivation of time and valuable resources on mitigation and reporting, partial or complete loss of otherwise useful asset; (c) Health and safety injury (suicide of affected consumer in AshleyMadison, Accusearch); (d) Unwarranted intrusion injury (Aaron’s computer rental and installation, Trendnet IP camera); and (e) Reputational Injury. The FTC has never brought an unfairness claim based merely on reputational injury even though the breach involved consumer sensitive personal information, as was the early case of Eli Lilly’s email list disclosure of Prozac users. The agency often based the claims upon other indirect and less obvious injuries triggered from reputation loss such as financial harm caused from the disclosure of sensitive information on medical conditions. After all, the FTC Commissioner has emphasized that certain of these injuries have not been independent basis for liability. It is also noticeable that the FTC does not mention disclosure of private information to unauthorized parties by itself as cognizable injuries. Maureen K. Ohlhausen, “Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases,” (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

34 In addition, in FTC v. Bayview Solution and Cornerstone and Company, the FTC’s complaints filed to the court claimed that the disclosure of “extremely sensitive personal information” involved unmasked debt portfolio to hundreds of public viewers had exposed them to potential harms of theft, fraud, invasion of privacy, and loss of job and unlawful debt collection. However, in FTC v. LabMD response, the FTC argued that the law has long recognized that public disclosure of private information by itself an actual concrete harm even in the absence of tangible effects or emotional injuries, or the victim of the breach are unaware of such disclosure.


36 Id. However, the court found that the FTC need not allege the violation of any particularized standard for alleging unreasonableness. As for proving causality, the court satisfied when the FTC did “more than simply assert that a violation must have occurred simply because the data loss incident occurred.” and claimed “several insufficiencies that drawing reasonable inferences in favor of the FTC, led to data-security breaches.
(ii) Substantive Baseline from the FTC’s Deceptive Claims.

A company failing to honor its direct or impliedly representation of data security practice, regardless of security level it had promised, constitutes an actionable deceptive practice. The deceptive acts basis of section 5 has enabled the FTC to bypass the problem of the actual injury element, such as evidential support of actual breach and injury, required under the unfairness test. This so-called “broken promise” or “contract-lite” basis allows the agency to trigger a separate claim against companies believed to deceive or mislead consumer regarding their security practices on consumer data.

The FTC actions against deceptive data security practices covers similar types of acts and practices found under unfairness claims, in the process of collection, use, process, storage, transfer and disclosure of consumer data. There are wide ranges of alleged misrepresentations on data security practices found by the FTC such as misleading representation on: (i) secured data transmission over Internet; (ii) secured online and offline data storage in its network including user credentials, identity, and credit card information; (iii) secured system from well-publicized, commonly-known attacks like the SQL injection and Cross-Site Scripting; (iv) reasonable data retention; (v) user’s control of privacy in sharing personal information, communication and location; (vi) disclose certain product functions or features i.e. non-automatically software updates, extensive personal data collection without consumer knowledge; (vii) screen out impermissible conduct or suspicious party by verification of authentication; (viii) screen out unauthorized access; (ix) user credentials, identity, and credit card information transmission over Internet; (x) Ensure security measures of third-party Service Provider either by contractual arrangements or its implementation of adequate security measures; (xi) maintain channel and process in receiving reports from third party; (xii) ensuring its insider control by implementation of adequate data security policy and practices i.e. strong admin password policy, internal review of email sent out, disposal of personal data, employee’s training and education on

---

37 Misrepresent that it reasonably take reasonable and appropriate steps to secure their products and service from unauthorized access. (D-Link, AsusTek, Trendnet, HTC America, Wyndham, Lookout (URL bypass), Misrepresent security of its network, user profiles of engagers(AshleyMedison).
38 transmission of data over secured connections. (Credit Karma) in encrypted manner (Upromise) Lifelock, Sandra L. Rennert
39 reasonably securely store its database (UBer) passwords in clear readable text (RockYou, Guidance Software) database (LifeLock) NHC (online and offline) Petco (Financial Information in a clear decrypted readable text), Guess (credit card info), encryption (when, in fact, software use a less complex algorithm to protect patient data than a standard encryption such as AES encryption. (Henry Schein Practice Solutions) Valueclicks (not consistent with industry standard); reasonable security protection of user identity (Credit Karma); physical storage and transfer (CBR, LifeLock (fascimile)
40 Fail to employ tools to monitor and prevention against attacks (Guidance Software, NHC) prevent SQL injection attack (Ceridian, ValueClick, Life is Good, Guidance Software), Cross-Site Scripting (Genica Corporation)
41 terms and condition for deleting profiles. (AshleyMedison)
42 misrepresent user control of expiration time of private snap (snapchat) fail to ensure user setting will be honored (Trendnet) Location collection (HTC) user setting choice to keep private message (Twitter)
43 E.g. Fail to disclose adequately software updates not automatically replaced older version (Oracle); fail to disclose some information collected in using certain features (Snapchat, Compete: consumer without special software and technical expertise to discover the extent of collection, Upromise)
44 security measures against misuse and unauthorized access (fail to verify/ control account owner) (Snapchat), fail to verify real purchaser with authentication- URL contains order number (MTS); Misuse of data by sharing with third parties/ sending out billing scams (Sandra L. Rennert); fail to screen users not criminals (Premium Capital Lender, Choicepoint)
45 Notify consumers when someone capture the screen (Snapchat)
46 E.g. Failure to oversee its third party service providers to ensure implementation of reasonable and appropriate security measures. (GMR Transcription, Foru International Corporation, NHC)
47 Failure to ensure contracts with third party service provider and limit access to necessary categories of PI. (Foru International Corporation, Gregory Navone)
handling consumer data, ensure compliance, and monitoring and auditing; (xiii) ensuring user’s data security hygiene practices to business end-users by assessing risks and the implementation of adequate security measures, and educating individual consumer i.e. instruction on creation of passwords.

The misrepresentations could be either direct or implied statement from the privacy and security policy found on the company’s website, CEO speech and elsewhere. Most statements on data security practices were considered “material” enough from the consumer standpoint that could trigger deceptive claims when actual companies’ practices do not meet such promises. As to the standard of security practices, the FTC holds the companies accountable for whichever standard it has promised expressly or impliedly in any statement related to privacy and data security practices. When a company has provided a general promise to provide secured protection, or omitted mentioning specific standard, the FTC assumed they referred to industry standard of data security practices.

(iii) Substantive Baseline from the FTC’s Dispute Settlement Order.

The FTC suggested in the case of FTC v. Wyndham that its reasonableness standard could be clarified under the consent order. From this view, the FTC’s reasonable data security practices shall at least include the measures specified within the mandate written comprehensive privacy or security program (MWCP) ordered by the FTC to business with alleged unfair and deceptive privacy and security practices under section 5. The MWCP shall be reasonably designed to address privacy and security risks related to the development and management of new and existing products or services, and to protect the security, confidentiality, and integrity of personal information. In general, the program must contain administrative, technical and physical safeguards appropriate to a respondent company’s size and complexity, the nature and scope of respondent’s activities, the nature of products or services provided as well as the sensitivity of the personal information.

In FTC orders, comprehensive program shall include the following measures: (a) the designation of employee(s) to coordinate and be responsible for compliance with the privacy program; (b) the identification of reasonably foreseeable risks, both internal and external, that could result in the respondent’s unauthorized collection, use, or disclosure of personal

---

48 E.g. fail to implement policies and procedures in key area including physical security and proper collection and handling of sensitive consumer data. (PLS, RiteAid Pharmacies, Gregory Navone, Goal Financial LLC)

- Appropriate employee training (PLS, RiteAid Pharmacies, Goal Financial LLC, Eli Lilly (fail to provide oversight and assistance for employee with no experience)

- Employee installation of P2P file sharing app to company’s computer network (franklin’s Budget car sales, EPN, )Employee’s use of private email (Twitter), not separate login or limit access to job (Twitter, Lifelock)

- Weak admin password (Twitter)

- Not adhering to its written policy. (Eli Lilly)

- Disposal in a secured manner (CVSMark, PLS Financial Services, RiteAid Pharmacies, Gregory Navone)

- employee’s use of行政 email (Twitter) and not separate login or limit access to job (Twitter, Lifelock)

- False/Misleading monitoring and auditing of internal policy on regular basis (Uber), (Lifelock)

49 E.g. failure to assess risk from user’s network, and measure in place, review or monitor. (Premium Capital Lender), fail to employ detector of intrusion or monitoring system of business client user’s activities (LookOut)

Mislead users in instructing passwords creation (RockYOU), fail to instruct against weak password (Lookout).

50 Whereas most common reference made by the company in its security statement is the industry standard, some statements go beyond such as the “the state of art” security practices as is the case of Nomi Technology. The FTC still held Nomi accountable for failing to meet such higher standard promised although it meets common practice in industry. In such case, the company was prohibited to make false or misleading promise of higher security standard and mandated implementation of comprehensive privacy and security program as same as other cases.
information, and an assessment of the sufficiency of any safeguards in place to control these risks. At least, this risk assessment should include consideration of risks in each area of relevant operation, including: employee training and management, training as required under the FTC order, product design, development and research; (c) the design and implementation of reasonable controls and procedures to address such risks and of regular testing or monitoring of the effectiveness of those controls and procedures; (d) the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of personal information they receive from the respondent, and the requirement of service providers, by contract, to implement and maintain appropriate privacy protections for such personal information; and (e) the evaluation and adjustment of the respondent’s privacy or security program in light of the results of the testing and monitoring required, of any changes to respondent’s operations or business arrangements, or of any other circumstances that the respondent knows or has reason to know may have an impact on the effectiveness of the privacy or security program.

It is noticeable that the obligations under the FTC settlement orders resemble the safeguard requirements for the protection of consumer data under the GLBA applying to the financial institution. In some cases, the FTC placed additional obligations for the respondents to notify consumers of the breach and preventive steps. As in the case of Bayview Solution and Cornerstone and Company, the federal court also ordered the defendants to notify the affected consumers that their information had been exposed and to provide steps they could take to protect themselves from further damage. Whether such disclosure of breach to affected consumer is considered as part of reasonable data security practices will be discussed further in chapter 3.

B. Reasonable Basis under Other Statutory Provisions: GLBA, FCRA, COPPA

The FTC also has authority to enforce against certain data security practices violating reasonable data security obligations provided under the GLBA (the Consumer Privacy Rule or Regulation P, and the safeguard rules), the FCRA (Disposal Rule and internal procedure to screen permissible purpose), and COPPA.

Whereas the specific provisions under the GLBA and the FCRA provides the agency with a more individualized tool against unreasonable practices, the applications of these provisions are limited for those entities subject to the rules, primarily those financial institutions and credit reporting agencies. Therefore, they are not proper means to regulate general businesses. Even when the FCRA equips the agency with sanctioning power to issue monetary penalty for violating companies, previous actions has shown the agency’s reluctance to exercise its power in case involving unauthorized disclosure of hundreds of sensitive consumer information. Though, under the FCRA that provides private right of action to individual, the court satisfied when the

---

51 “Third-party service provider” means any person or entity that is contractually required by respondent or a software provider to: (a) use or receive covered information collected by or on behalf of Respondent or the software provider for and at the direction of Respondent or the software provider, and for no other individual or entity; (b) not disclose the covered information, or any individually identifiable information derived from it, to any individual or entity other than Respondent or the software provider; and (c) not use the covered information for any other purpose.

52 The Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313, or the Privacy of Consumer Financial Information Rule (Regulation P), 12 C.F.R. Part 1016.


injury in fact is the violation of a statutory right inferred from the existence of a private cause of action.\textsuperscript{56} The decision was later vacated and remanded by the Supreme Court.\textsuperscript{57}

\textit{(i) Reasonable Data Security Practice under the GLBA.}

The Safeguards Rule of the GLBA requires financial institutions under the FTC jurisdiction to have measures in place to keep customer information secured. “Customer information” means any record containing non-public personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the company covered by the Rule or its affiliates. Therefore, it applies to information pertaining to individuals with whom the covered financial institution does have a customer relationship. The companies covered by the Rule have an additional duty besides developing their own safeguards to ensure that their affiliates and service providers safeguard customer information in their care. “Service provider” means any person or entity that receives, maintains, processes, or otherwise who is permitted to access customer information through its provision of services directly to a financial institution that is subject to this part.

The Safeguards Rule aims to protect the security, confidentiality and integrity of customer information by setting forth reasonable standards of “Information security program”, which means the administrative, technical, or physical safeguards for access, collection, distribution, process, protection, storage, use, transmission, disposal, or other means of handling customer information. The standards for safeguarding customer information and the elements under §314.3 and §314.4 are similar to the FTC mandate comprehensive privacy and security program included in the settlement orders.\textsuperscript{58}

\textsuperscript{56}Robins v. Spokeo, Inc., 742 F.3d 409 (9th Cir. 2014).
\textsuperscript{57}Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).
\textsuperscript{58}§314.3 Standards for safeguarding customer information.

\textit{(a) Information security program.} You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

\textit{(b) Objectives.} The objectives of section 501(b) of the Act, and of this part, are to:

\begin{enumerate}
\item Insure the security and confidentiality of customer information;
\item Protect against any anticipated threats or hazards to the security or integrity of such information; and
\item Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
\end{enumerate}

\textsuperscript{54}§314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall: (a) Designate an employee or employees to coordinate your information security program. (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures. (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures. (d) Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards. (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

29
The FTC found several financial institutions’ practices violated the Safeguard Rules. These violating acts included: (a) the failure to train employees to handle consumer information properly, including limiting access to consumer personal information in paper files. (Re: Goal Financial LLC, a company marketing student loans, the case where consumer information was sold to third party by employees); (b) the failure to assess risks to its customer information, institute appropriate password policies to control access to company systems and documents containing sensitive customer information, and to encrypt or otherwise protect sensitive customer information emailed by respondents and its service providers using networks outside of respondent’s computer network; (d) failure to take reasonable steps to ensure that its service providers were providing appropriate security for customer information and were addressing known security risks in a timely fashion; and (e) the failure to dispose of consumer information properly as the information was found in dumpsters near the respondent’s office.

Reasonableness under the Privacy Rule

The Privacy Rule or Regulation P of the GLBA requires a financial institution to provide notice and reasonable means for a consumer to opt out before a financial institution discloses nonpublic personal information about his or her to a non-affiliated third party. The FTC has enforced the privacy rule against several companies failing to provide a privacy notice, an opt-out right and disclosure of security practices for consumer, as in FTC cases of Tax Slayer, Goal Financial LLC, America United Mortgage Company, and James B. Nutter & Company. In the cases of America United Mortgage Company and Premium Capital Lender, the court also found violations of the Safeguard Rule and Privacy Rule, section 501-509 of the GLBA, for they fail to provide, no later than when a customer relationship first arises and annually thereafter for the duration of that relationship, a clear and conspicuous notice to customers that accurately reflects the financial institution’s privacy policies and practices. (ii) Reasonable Data Security Practice under the FCRA.

Until the present, the FTC has enforced against several credit reporting agencies’ failure to meet obligations relating to privacy and security under the FCRA. In FTC Matter Concerning ChoicePoint, the agency considered the company’s failure to properly verify the identity of new users and furnished consumer reports to theft, as violations of Section 604 and 607(a) of the FCRA. In FTC Matter Concerning Rental Research Services, the data broker selling tenant screening reports had violated the FCRA by furnishing consumer reports of tenants to a person who did not have permissible purpose, and by failing to provide reasonable efforts to screen the identities and uses of its website’s subscribers who received such consumer personal information. It also failed to establish reasonable procedure for reselling consumer reports only to a person who has permissible purpose pursuant to Section 621(a) of the FCRA, 15 U.S.C. § 1681s(a). These violations of the FCRA also constitute unfair and deceptive acts under Section 5 of the FTC Act.

Downstream liabilities for data broker companies under FCRA.

For data broker companies, in the FTC matters concerning Fajilan and Associates, the FTC found the company furnished consumer reports to hackers that did not have “permissible

59 See the distinction between the definition of “consumer” and “customer” under the GLBA and the additional disclosure requirements for a customer. https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf
purpose” to receive those reports in violation of Section 604, and did not maintain a reasonable procedure to limit furnishing consumer reports in violation of Section 607(a). It further found that the company had failed to implement the security policy, and proper steps to assess, identify and monitor risks for itself, as well as its business end user clients, i.e. the evaluation of the security practices of its clients and conduct training to end user clients.\textsuperscript{60} These failures consequently allowed unverified clients to access at least 323 consumer reports and view reports pulled up by end users in previous 90 days. Similar findings are found in the FTC matters concerning ACRAnet, Inc. and SettlementOne Credit Corporation, where hackers had accessed consumer reports, (694 and 784 reports respectively), from a client’s computer network.

In these three cases, the FTC had issued statements threatening data broker companies with imposing monetary penalties for future violations of the rules.\textsuperscript{61} Interestingly, the agency imposed the alleged data broker companies with implied downstream liability to ensure adequate data security practices of its end user clients. The data broker companies have responsibility for the data leaks caused from computer network of its clients being hacked. It is unclear whether these responsibilities also apply to other players in the upstream of the chain, such as the companies that share consumer reports with these data brokers, which also need to check on the availability of reasonable safeguard measures before sharing information.\textsuperscript{62}

- **FCRA Disposal Rule.**

As for the Disposal Rule, the FCRA disposal rule §682.3 requires that any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Such measures shall include, for example; the implementation of policies and procedures that require shredding of papers or erasure of electronic media containing consumer information, so that the information cannot practicably be read or reconstructed; entering into contract and monitoring compliance with its service provider engaged in the disposal of material and conducting a due diligence review by an independent audit of the disposal company's operations and/or its compliance. And finally, for a financial institution subject to the GLBA, the inclusion of the proper disposal of consumer’s information into the information security program required by the Safeguards Rule. Violations of the FCRA could result in a Permanent Injunction and impose monetary civil penalties, $2500 for each violation, as imposed by the Court.

In the FTC matter concerning PSL Financial Services, the FTC found that the company’s practices violated the disposal rule for it failed to protect consumer report or information derived from consumer report when disposing of them, and to ensure that the information was disposed of in a manner that it cannot practicably be read or reconstructed. These failures could have been prevented by implementing and monitoring disposal policies and procedures, ensuring appropriate guidance or training received by the employees, alerting them to take precaution due to sensitive nature of the information, and providing oversight of the collection and transportation for the disposal. (para. 17). A similar violation of the disposal rule is

\textsuperscript{60} These are, for example, monitoring their use of consumer reports, to detect suspicious activities, or take appropriate action to correct existing vulnerabilities from the known risks.


\textsuperscript{62} The issues worthy for further investigation beyond the scope of this dissertation are as to what conditions trigger the agency’s imposition of downstream liabilities, and whether such liabilities are relevant only to the claims brought under FCRA.
found in the FTC matter against Gregory Navone, mortgage brokerage companies who failed to dispose of sensitive customer information derived from consumer reports in a secure manner creating risks of unauthorized access, which was also deemed unfair under FTC Section 5.\textsuperscript{63}

### III. A Commentary on the FTC Approach: Implied Duty to Third Party and Notion of Reasonable Consumer

#### A. Implied Responsibility to Third Party and Reasonable Consumer

It could be deduced from the previous FTC deception enforcements that the extent of “reasonable and appropriate” data security promises does not limit to alleged company's' internal practices and its employee, but to cover a wide array of practices extended to third parties the alleged company has relationship with. These are, for instances, its third-party service providers, business end-users and consumer. From this view, the FTC interpretation has created responsibility or implied duty of the companies on data security based on their existing relationship.

For service providers, the alleged company has responsibility to ensure the implementation of adequate security policy and practices, provide on-site security review and risk assessment, training and education of security risk and prevention, and ensuring compliance in form of contracts. The company has to ensure that they have adequate security measures in place and able to detect risks for its business clients. As for consumer engaging in its product or service, the company has responsibility to educate and provide adequate instructions to them regarding security risks related to their products and services including making available preventive measures intended for those ordinary consumers without technical background and knowledge, not a sophisticated one, the so-called “reasonable” consumer as in The FTC matters concerning Nomi and Asustek.\textsuperscript{64}

#### B. Undefined Relationship between Business Actors in Data Processing Businesses

The lack of clarity on the agency’s choice to enforce against certain companies and not others casts doubt to stakeholders on the fairness and predictability of the agency’s strategies. It is noticeable that the FTC did not pursue claims against these corporate clients despite the security flaws in their network system that failed to prevention of the foreseeable security attacks. These business end-users also received protection under the Section 5 as consumers.

Furthermore, questions may arise as to whether the agency has taken into account the interrelated nature of data security practices in business reality, where consumer data is not handled only by a single entity, but gone through several processes and multiple entities to fill in the need to provide products and services to consumer. Where a security flaw created by a company might cause the leak of consumer data, other cases may be an accomplice with the recklessness of the others involved in the chain. This view calls into a question of whether or how the FTC enforcement considers this relationship aspect in its discretion and a possibility to fill in the fragments in the system.

\textsuperscript{63}In The FTC matter against the America United Mortgage Company, the FTC found the company failed to provide consumer notice in violation of the privacy rule, and issued Permanent Injunction and the monetary civil penalties for violation of FCRA 628 ($2500 for each violation)

\textsuperscript{64}In the Matter of ASUSTeK Computer Inc., File No. 142 3156.
It is uncertain as to what is the rationale of the FTC application of Section 5 to chase after certain business players and motivation created by law for businesses to comply with reasonable data security practices? From the FTC actions, it is neither entity with closest relationship to individual, nor the entity in the best position to control and prevent the damage, or the entity having best economic status to compensate individuals suffered from breach.

These points lead to discussion in Section II on relationship between business players within the FTC design platform and the lack of defined relationship between data controller and data intermediary affecting cooperativeness.

C. Reasonableness Standard of Data Security Practice for Data Intermediary

Several jurisdictions have put forward a specific definition, duty and liability of data processor or data intermediary as distinct from data controller. The data intermediary typically refers to any person who processes personal information on behalf of the data controller, an organization that has a direct relationship with, or collected data from the consumer. Such specific definition or distinction has not been made by the FTC application of law to these entities under Section 5. Therefore, similar reasonableness standards of data security practices are applicable to business party who acts as data intermediary under other jurisdictions.

Until present, the agency has brought several claims against entities considered acting as data intermediary in general understanding. These intermediaries cover service providers and outsourced companies who, for instances, processing sale transaction, and providing authorization services, or carts for checking out process (The FTC matter concerning Vision I Properties). In all cases involving data intermediaries leaked of health information, these data intermediaries were brought under unfairness claims of Section 5. When the breach involves sensitive financial information processed by data intermediaries, who are subject to the FCRA and GLBA, some were charged with deceptive claims and others were charged under unfairness claims, triggered by the violation of these specific provisions.

Undefined Relationship with Data Controller

It is also noticeable that the FTC did not hold the data controller company or the company who hired these service providers to be accountable for the breach, and did not mention in its complaint against the data intermediaries on whether the investigation result had revealed that the data controller companies’ practices was not involved in the breach. Notwithstanding that there were cases where data controller could facilitate the breach by failing to ensure by putting in contractual arrangement of reasonable and appropriate security practices of their outsourced service provider. On that, the agency has not clarified whether the data intermediary has any duty toward its clients, data Controller Company, in secure measures to protect data.

I bring out this point to highlight the lack of distinct definition of data intermediary in the FTC Section 5, which leads to further discussion in part II on distributive liability and assurance. This results in the similar reasonable standard applicable to Data intermediary (DI). Further, there is no specific relationship drawn between DI and data controller, affecting the distribution of relationship between them, and each towards individual consumer.
C. The downsides from reasonableness interpretation under dual basis of deception and unfairness.

The duality of reasonable data security practice created by the FTC interpretation under deception and unfairness claims, or arguably a double-layer of protection to consumer data, raised confusion for businesses in navigating through and compliance with without a clear and streamline clarification. At conceptual and policy-making levels, the FTC’s choice to exercise deception authority on data security over unfairness authority could create significant downsides on the development of U.S. privacy underlying values and way of remedies, the policy-making of agency’s reasonableness standard as well as the norm emergence from compliance.

First, as the FTC recognized deceptive representation itself as harms to consumer choice on products or services without the need of demonstration of other harms, its continuation of exercising deception authority would develop only limited notion of individual rights to privacy and data security in terms of right to get truthful information, informed decision-making ability and protection of promised consumer expectation and control. While others may argue that these aspects form core notions of the U.S. individual privacy values, which rest upon honor of promise, truth, and choices of individual consumption, a full spectrum of privacy values has been turned a blind eye on effect from the disclosure of personal information an individual could be suffered. These are, for instances, loss of dignity, reputation, safety etc. Ignorance on these notions has seen in previous FTC actions under Section 5, and as a consequence, individuals suffered from these uncovered privacy injuries receives no protections or remedies.

Second, adhering to chase after deceptive statements, the agency’s deception action may rather be suggestive to businesses on “what is a reasonable promise” on data security and privacy practices rather than “what are reasonable practice”. By saying so, it refers to the case of Nomi where aiming to achieve high level of security practices, but not yet reached it, could turn against the company itself. The agency’s message could be misleadingly interpreted to discourage the promises of higher security standard in business practices. For businesses considering adopting higher data security standard of practices, besides potential higher investment cost, they bear higher risks of failure to meet the agency’s reasonable practices under deception authority. This may lead to a conclusion of why not just does what their peers in industry do in similar situation.

Finally, the inconsistency of double reasonableness standards applied by the FTC in deception and unfairness claims has raised legal uncertainty, and disrupted the emergence of norms on reasonable data security practices by businesses. While the agency asserted that deception claim is a subset of unfairness claim, it did not reflect such in the past FTC actions. This is supported by number of cases where FTC find the company fail to deliver its promise of reasonable and appropriate security practices to consumer data, but were not charge with unfairness claim.

More than half of FTC decisions regarding unreasonable data security practices were brought under both deceptive and unfair claims. As for the rest, the FTC placed alleged company’s practices based upon either deceptive claims\(^{65}\), or unfairness claims\(^{66}\). There are also

---

\(^{65}\) There are 14 cases based solely on deceptive claims out of 66 cases on the FTC’s website with data security tags; The FTC matters re:Henry Schein Practice Solutions, Oracle, Fandango LLC, Twitter, Lifelock, Genica Corporation, Premium Capital Lender, Life is good, Guidance Software, Goal Financial LLC, Sunbelt Lending, PetCo, Guess, EliLilly, Sandra L. Rennert.

\(^{66}\) There are 18 cases based solely on unfairness claims out of 66 cases on the FTC’s website with data security tags; LabMD, Bayview Solution, Cornerstone and Company, Accretive Health, EPN Debt collector, Fajilan and Associates, ACRAnet,
numerous cases where similar facts of third party unauthorized access and actual disclosure were present, but the FTC chose to pursue under deceptive claim without further unfairness claim. There is a need of clarification and consistent explanation for the FTC’s enforcement choices to better communicate to business stakeholders and reduce uncertainty and confusion in legal compliance.

I revisit these points again in section 2 from trust and cooperative perspectives to address the uncertainty and risks for businesses in navigating through reasonable data security practice emerged from double layer of protection created by the unfair and deceptive test together with the inconsistency of FTC decision to trigger each baseline. I further address these points to demonstrate that the current FTC's enforcement on deceptive claims dilutes the meaning and values of protection derived from unfairness.

**D. Whether such breach notification to consumer is considered part of reasonable data security practices**

There are some cases where the FTC placed additional obligations for the respondents to notify consumers of the breach and preventive steps. As in the FTC cases of Bayview Solution and Cornerstone and Company, the federal court also ordered the defendants to notify the affected consumers that their information had been exposed and provide steps they could take to protect themselves from further damages. Though, these FTC orders lacks further explanation and are inconsistent with the other cases with similar factual circumstances where the FTC did not order respondent companies to notify breach.

In other instances, the FTC complaints recognized the fact that notification to consumer and remedial actions had been done by the alleged businesses. However, this is without much clarification from the FTC on the significance of such action to the agency; whether they found these actions plausible, and what could be the consequences therefrom. So far, as the FTC message is not clear on what are plausible and what are beneficial from remedial actions to consumer, there are fewer incentives for the businesses to initiate the remedies to consumer without pressure from the public and media. Even so, the media pressure would work for companies in the spotlight, not all. If the FTC does not address clearly on the positive consequence to businesses from such breach notification and remedy to consumer, it could instead encourage companies to bury the cases and to take no prompt remedial actions for fear of being discovered.

In conclusion, despite these orders mentioned, it is unclear on the incentives or force for businesses to notify breach and remedy consumer. Even though the media can put pressure on  

---

SettlementOne, Credit Corporation, Dave and Buster’s, Reed Elsevier (Lexis Nexis), TJX, Rental Services, American United Mortgage Company, Cardsystem Solutions, DSW, BJ’s Wholesome Club, Vision I Properties.

Among those 17 cases, only 4 cases of Fajilan and Associates, ACRAnet, SettlementOne, American United Mortgage Company also involve violations of FCRA or GLBA; 3 cases of LabMD, Accretive Health and EPN involve health-related data; 14 cases involve sensitive financial data; 10 cases involve massive breach of over a thousand affected customers; 4 cases of LabMD, Bayview Solution, Cornerstone and Company; EPN and US Mortgage involved disclosure of personal information to the public; 7 cases (LabMd, Bayview Solutions, Cornerstone, Accretive Health, EPN, US Mortgage) involved insider breach.

The FTC matters concerning Asustek, Oracle, and Data Broker cases. The FTC also requested disgorgement order as a civil remedial action from the court in the FTC matter concerning Lifelock.

For instances, would the agency consider those facts mitigating the company’s liabilities from breach, and as a result, a less onerous mandate program requirement applicable? Would it make the FTC satisfied and not pursue with further charges against businesses?
some company in the spotlight, those out of public attention can still ignore these responsibilities for fear of discovery of breach. This aspect will be further discussed in chapter 3 and 4.

E. The FTC’s Enforcement Power and Penalties

The FTC Section 5 does not empower the agency to impose penalties for violating businesses in contrast to the FCRA. What could threaten the businesses most would be the mandate comprehensive privacy program attached in the settlement order, parts of which burdens the business parties with third party auditing and reporting obligations to the FTC aside from potential large amount of money suffered by the party if it fails to comply with.69

For the violation of final order of the FTC, the courts have considered these following factors in the past, as well as the agency itself when considering what level of penalties applied: (1) harm to the public; (2) benefit received by the violator; (3) good or bad faith of the violator; (4) the violator's ability to pay; (5) deterrence of future violations by this violator and others; (6) vindication of the FTC's authority. Alternatively, the agency could have expressly clarified its assessment of these factors under 15 U.S.C. § 45(a)(1) in its order and complaints as aggravating or mitigating factors to determine injunctive relief and potential penalties from the violation of its final order.

IV. Conclusion: A Streamlining of Reasonableness under Section 5 with Other FTC Regulations.

Fair, non-deceptive, thus reasonable data security practices under Section 5 as interpreted by the FTC has come closer to specific procedures required under the statutory provisions for protecting consumer financial data from exploitation by financial institutions. These specified measures under the FCRA and GLBA deal significantly with duties to provide adequate and fair disclosure of information and obtaining individual consent before processing personal data. Also found in the FTC settlement orders are those measures similar to the GLBA safeguard procedures for securing the share of sensitive financial data contained in consumer reports, and ensuring of appropriate measures employed by the third-party service provider. What could be an interesting aspect of the FTC applications is when the Commission held data brokers who furnish consumer reports to business clients to be responsible for the security flaws of their end user’s computer system that allowed a hacker to retrieve sensitive data. This interpretation creates an implied liability of an organization for the conduct of other organizations, which is different from the relationship commonly found in other regimes, those between organization and service provider or between data controller and data intermediary. This distinction of U.S. regime from others traces back to the definition of a consumer that does not only refer to an individual consumer, but include a business end user who also receives protection in the similar

69 Section 5(b) of the FTC Act, 15 U.S.C. 45(b) (violations of cease and desist orders issued under Federal Trade Commission Act section 5(b))—Increase from $16,000 to $40,000. Note that for continuing violations, each day is a separate violation. As a result, the maximum civil penalty may be multiplied by the number of days for each violation of the applicable statute or order. But statutory maximums are just that — the maximum civil penalty available under the law. When the Commission seeks any civil penalty (whether in settlement or litigation), it will consider whether the maximum should be mitigated. Past court cases have explained the various factors considered when determining how much of the statutory maximum penalty should be assessed. For example, in imposing a $7 million penalty for violating an FTC order, the district court outlined the factors that bear on this assessment: Courts traditionally have looked at six factors in determining the appropriate civil penalty under 15 U.S.C. § 45(a)(1): (1) harm to the public; (2) benefit to the violator; (3) good or bad faith of the violator; (4) the violator's ability to pay; (5) deterrence of future violations by this violator and others; (6) vindication of the FTC's authority.

way under the FTC Act as an individual consumer does. From this view, Section 5 of the FTC Act may be handy but not a perfectly customized venue for protecting individual privacy and security. When put into contrast with the term “customer” found in the safeguard rule of GLBA, the term “consumer” under Section 5 does not necessarily indicate the ongoing relationship between such end user and the institution. Comparative cases analysis of the FTC and PDPC cases in Chapter 3 further highlights this disparity in actions. It points out different data security obligations of businesses towards individuals, under Section 5 of the FTC versus the Section 24 of the PDPA, which implies different meanings and venue for trust relationship between individual and business parties. This is not to mention the hazy boundary between the role and duties of platform provider and organization under Section 5 that affects their cooperativeness and a shield offered to end-user businesses to not being responsible from poor data security practices.

Part B. Singapore Data Security Governance: A Trust and Cooperative Approach

I. Introduction

This part examines Singapore’s style of cybersecurity governance under the Personal Data Protection Act (PDPA). The Singaporean regime may not be an ideal for promoting individual privacy rights, but would be a good case study for its data protection regulatory design aiming to reinforce trust in data processing businesses and e-commerce. Such efforts are reflected in a regulatory design that provides both a platform and effective tools for the enforcement agency to weave the standard of reasonable data security practices into organizational data governance.

The part is divided into three sections. First section discusses how values of trust and cooperation has been integrated into the Singaporean regulatory design framework and functions performed by the Personal Data Protection Commission (the Commission or PDPC) as enforcement agency. The second and third section introduce the Commission’s interpretative approach to reasonable data security practices, the key strategies and tools with which Singapore’s enforcement agency approaches data security breach cases. Further analysis on the PDPA implementations through selected cases are conducted in Chapter 3.

II. Singaporean Reasonable Data Security Practices

a. The PDPA Objectives and Principles

The Singapore government passed the 2012 Personal Data Protection Act with the goal of promoting trust in e-commerce and becoming a trusted hub of data processing, rather than creating a privacy regime. The law aimed to strike a balance between encouraging free flow of data and protecting individuals from inappropriate use of personal data by businesses.\(^70\)

\[^70\] The PDPA came into full effect on July 2, 2014. It serves as a general law on data protection, which is superseded by specific laws. It also excludes the government agency from its application (Section 4(6) (b)). The law is considered not a pro-privacy regime, as it contains some provision not favored by such pro-privacy regimes. Among other provisions, it allows organization to obtain from individuals based on implied consent, and does not recognize an individual’s ownership of the personal data related to him/her. Singapore’s constitution does not explicitly recognize privacy right.

\[^71\] See section 3 of the PDPA.
Embracing trust as a focal point had a two-fold benefit: all players were familiar with this traditional concept, applied to the emergence of cybersecurity threats to data economy; it also spoke directly to businesses and industry, suggesting that compliance with the Act was in their economic interests. In the recent PDPC’s decision against non-profit debt management, it mentions that the data breach incident may cause members of the public to lose trust in such credit counselling organizations to safeguard their personal data, which may frustrate the larger national credit management efforts. (Re: Credit Counselling Singapore, para. 36 (c))

In pursuit of the PDPC’s objective of promoting trust, the PDPA’s regulatory design embraces principles of accountability and organizational good judgment. Section 11 of the PDPA requires organizations to comply with obligations on the basis of “what a reasonable person would consider appropriate in the circumstances regarding personal data in its possession or under its control.” In enforcing the law, the Personal Data Protection Commission (the “Commission”) has also referred to reasonable care and due diligence standards to determine whether an organization has fulfilled obligations under the Act, including data security obligations set out in Part VI under the title of “Care to Personal Data.” It is questionable, however, that reasonable standard may reflect the Commission’s own expectation of certain organizational response rather than individual expectation of it, or what a reasonable organization would do in such circumstances. In the PDPC’s decision, the Commission is of the view that the organization procedure put in place did not meet the reasonable standards expected of it.

b. Reasonable Data Security Practices under the PDPA.

Data security protection was set out in Part VI of the Act under the title of Duty of Care to Personal Data. Section 24, or protection obligation, provides that “An organization shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.” Organization subject to the protection obligation under Section 24 means any individual, company, association or body of persons, corporate or unincorporated, regardless of whether it was formed or recognized under the law of Singapore, or having its residency, office, or place of business in Singapore. So far, the Commission has found Organization to include an independent consultant, individual data broker and a non-profit charity providing consult to debt management. Protected personal data refers to data, whether true or not, of individual, who can be identified from that data, or from that data and other information to which the Organization has or is likely to have access. It covers data in both digitized and non-digitized form, but excludes business contact information from the governance of PDPA. In compliance with the obligations under PDPA, Section 11 also provides the general principle for organization in considering “what a reasonable person would consider appropriate in the circumstances regarding personal data in its possession or under its control”.

The PDPA establishes distinct obligations and liabilities for business parties acting as a data Intermediary, who is exempted from other duties belong to organization, but still has to comply with protection obligation under Section 24 and data retention obligation under Section 72. Other duties under Care of Personal Data concern accuracy, retention, and transfer of personal data.

72 Re: Data Post Pte Ltd [2017] SGPDPC 10, para. 11.
73 See section 2 of the PDPA.
25. Under the PDPA, “Data Intermediary” refers to organization that processes personal data on behalf of another organization but not including organization’s employee. “Processing” means the carrying out of any operation or set of operations in relation to the personal data, and includes recording, holding, organization, adaptation or alteration, retrieval, combination, transmission, erasure or destruction. From the definition, the characters of organization and its data intermediary under PDPA is similar to data controller and its data processor in EU and UK regime.

The PDPA section 4(3) also emphasizes that an organization having a data intermediary processing personal data on its behalf does not free itself from complying with protection obligations and liabilities arisen from the breach of Section 24. Rather, an organization shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organization itself.

**Self-Resolution and Cooperation among Players.**

In several respects, Singapore’s data protection regime has made considerable effort to encourage organizations and industries to initiate and drive protection of personal data towards the end goal of creating trust economy. Rather than heavily regulating and penalizing companies in violation of the law, PDPA review procedure encourages individual and business parties to seek self-resolution in disputes before filing a complaint with the Commission, and, if self-resolution fails, to request mediation before the case is further reviewed by the Commission. Where other regimes rely heavily on single-handed enforcement agency to impose high penalties and go after the violating companies, Singapore’s cooperative approach reflects a business-centric design, emphasizing effective communication between business players and regulators as well as public vigilance in filing complaints under the PDPA.

### III. The Commission in Action: Tools and Strategies for Data Security Governance

#### a. Broad Power and Discretion

The PDPA provides the Commission with effective tools and sufficient discretion to exercise its power, allowing flexibility in the strategies applied for organizational compliance with security protection obligations. In general, the Commission is vested with broad power under the law to review individual complaints made against an organization’s non-compliant measures. The Commission also has the power to issue directions to ensure that the violating organization has complied with the PDPA: for instance, it can order the organization to stop the collection, use, or disclosure of personal data; to destroy personal data collected; to comply with other

---

75 See sections 4(2) and 4(3) of the PDPA.
76 The PDPC Re: Social Metric
77 See section 27 of the PDPA, Alternative Dispute Resolution—(1) If the Commission is of the opinion that any complaint by an individual against an organisation may more appropriately be resolved by mediation, the Commission may, with the consent of the complainant and the organisation, refer the matter for mediation.
   (2) Subject to subsection (1), the Commission may, with or without the consent of the complainant and the organisation, direct a complainant or the organisation or both to attempt to resolve the complaint of the individual in the way directed by the Commission.
78 The Info-Communications Media Development Authority currently serves the position.
Directions; and to issue a financial penalty not exceeding $1 million upon the Commission’s discretion.79

Directions and Penalties. As of February 15th, the Commission has ruled on 45 cases80 involving complaints of violations of the PDPA across industries, with different causes of breach ranging from insider leak to outsider attack.81 On April 20, 2016, it rendered its first series of decisions on PDPA; five out of nine cases were issued with only warnings.82 Several warnings were also issued in later cases where the breach affected only a single individual.83 In other cases of data security breach, financial penalties were issued against non-compliant organizations. Penalty amounts ranged from $500 to $25,000 in the case of K-Box, which involved a massive leak of 317,000 membership accounts being compromised by the unknown hacker.84 The relatively small financial penalties imposed to the breaching organizations by the Commission in previous decisions suggests that heavy penalty is not a tool for compliance. Effects on organizational reputation and customer trust from being named and published on the Commission’s website and in the decisions are far more concerned by organizations.

Soft Functions and Communication. Section 5 and 6 of the PDPA also empower the Commission to perform other functions, which include raising data protection awareness, advising and consulting with businesses on data protection issues, cooperating with private organizations, conducting research and educational activities for raising individual awareness, and providing supports to organizations in those related to data protection as well as other specific duties assigned under the law. The Commission’s engagement in these activities includes providing educational resources, trainings, and a community network for data privacy officers, appointed by each organization as mandated by the PDPA.85 A Recent public consultation taken place in July-September 2017 regarding the proposed amendment of the PDPA is an instance in which the Commission exchanges and receives feedback from the public and industry, thus enabled them to match their expectation and communicate desirable values and expectation on data security practices.86

Binding and Non-Binding Guides. The Commission advisory guidelines are among reliable resources sought by organizations in compliance. It serves as a guide to the Commission’s interpretation of PDPA provisions and was often cited in the decisions.87 It illustrates scenarios to which these provisions apply in practice. Other non-binding guides from the Commission are, for

---

79 See sections 28 and 29 of the PDPA.
80 As of February 15, 2018
81 Respondents in previous cases were in the following industries: education, professional society, retail, manufacturing, entertainment, finance, transportation, telecommunication, and IT service.
85 According to Section 11(3) of the PDPA, “An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act.”
instance, the “Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data” and “Guide to Managing Data Breaches.” These suggests organizational best practices, recommended by the Commission to follow.

b. Deliberative Interpretation of Reasonable Data Security Measures under Section 24

The Commission’s interpretation of reasonable data security practices has evolved over time as it applied to specific contexts of individual cases. However, certain substantive elements derived from its key decisions in the cases of K-Box, IES, Toh-Shi, and Propnex on the following issues: protected data; reasonableness standard; and a set of obligations of the data intermediary and its liabilities as distinct from the Organization. In the matters following these selected cases, the Commission has continued its deliberative styles of interpretation by making considerable efforts on elaborating its decisional criteria and clarifying specific legal terms with illustrations drawn from the real settings. As found in the Commission’s decisions below, its interpretations fill in vague legal term and many times expand or devise new meanings unfound in the PDPA, for example, ‘sensitive’ data, or the point when a data intermediary turns to be an organization with full responsibility under the PDPA. The consistency of the Commission’s interpretation throughout the three years’ decisions has grown into a standard, relied on by organizations when implementing law into its security governance.

Table 2. Summary of facts and findings of key cases

<table>
<thead>
<tr>
<th>Case No.</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-1411-A213; 20 April 2016</td>
<td>The matter against Institute of Engineering of Singapore (IES) is an early case of cyber attack against the professional community causing unauthorized disclosure of 60,000 members’ login IDs and passwords. The leaked data were posted on the third party website which was accessible by the public. On 20 April 2016, the Commission held that IES failed to provide adequate security arrangements under protection obligation pursuant to Section 24 of PDPA, resulted in the fine amount of S$10,000 imposed on IES.</td>
</tr>
<tr>
<td>DP-1409-A100; 20 April 2016</td>
<td>K-Box and Finantech, the Karaoke chain business and its web-hosting provider, failed to provide adequate security arrangements to protect personal data of K-Box members under Section 24 of the</td>
</tr>
</tbody>
</table>

Despite using the words “adequate” and “reasonable” interchangeably in previous decisions, in the case of National University of Singapore on April 26, 2017, it began to make distinctions between the “adequacy” and “reasonableness” of security measures by addressing separately “(i) whether the Organisation’s safeguards that were in place at the material time were adequate having regard to the volume and type of personal data in question, and (ii) whether the safeguards were reasonable in the circumstances” (National University of Singapore [2017] SGPDPC 5, para. 13).
<table>
<thead>
<tr>
<th>Case No.</th>
<th>Date of Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-1506-A456</td>
<td>21 July 2016</td>
<td>The breach involved 317,000 membership accounts being compromised from the unknown hacker. It resulted in sensitive data of members being posted on the third party website accessible by the public. The Commission issued the fine amount of S$35,000 for K-Box and S$10,000 for Finantech who acted as Data Intermediary of K-Box.</td>
</tr>
<tr>
<td>DP-1603-A661</td>
<td>21 September 2016</td>
<td>The leak incidents caused from data mishandling by Toh-Shi printing staffs, which resulted in erroneous statements including sensitive financial data of 195 Central Depository (&quot;CDP&quot;) account holders being disclosed to other customers (in Toh-Shi I), and 8022 policyholders' statements being disclosed to other groups of policyholders (in Toh-Shi II). The Commission issued Toh-Shi with fine amount of S$5,000 in the first breach incident, and S$25,000 in the second breach incident. Organizations in both cases were not liable for any penalties.</td>
</tr>
<tr>
<td>DP-1512-A613</td>
<td>25 Jan 2017</td>
<td>The leak incident caused unauthorized disclosure of the Do-Not-Call lists containing personal data of 1,765 individual members' searchable and accessible on the Internet. The PDPC, therefore, imposed fine amount of S$10,000 and directions for corrective measures to Propnex.</td>
</tr>
</tbody>
</table>

(i) Protected Data: Personal Data and Sensitive Data

The Commission made clear that protected data under the PDPA includes personal data contained in either digital or hard copy (e.g., printed financial statements and insurance
When determining whether certain information is “personal data,” it considers all the leaked data in combination. In the Propnex case, “personal data” included the combination of full name, home and mobile phone numbers, residential addresses, and personal email addresses contained in the leaked do-not-call list. Information providing indirect access to personal information could also constitute “personal data” under Section 2(1): for example, valid user login IDs and passwords in combination, which could be used to access profile accounts and identify members (IES).

Although the law provides no specific definition of “sensitive data,” the Commission has consistently taken harm approach in finding that the leaked data were “sensitive” in its decisions. That is to consider whether a disclosure of such personal data could lead to harm to individual like identity theft, financial loss, reputation effect and social embarrassment. In Toshi I, it found the leaked printed monthly statements of security account holders mailed out to the customers—containing names of holders, security holdings, transactions, and payment summaries—as sensitive data, since this information could have led to identity theft. The same reasoning was applied in the K-Box case, where the Commission found that the leaked non-financial personal data—comprised of members’ full names, contact numbers, email addresses, residential addresses, gender, profession, and date of birth—were sensitive.

In the second breach of Toh-Shi (Toh-Shi II), the Commission found that an unauthorized disclosure of insurance policy statements—including policyholder names, beneficiaries, insured amount, premiums, and coverage—was “not financially harmful, but socially embarrassing,” and thus involved sensitive data. The relative sensitivity of the leaked data indicates the greater care and higher level of safeguard, and also becomes an aggravating factor when the Commission determines the severity of penalty imposed on the violating organization.

**Totality of Circumstances.** The Commission considered totality of circumstances in its review of an organization’s data security practices. It considered all weaknesses of organizational measures that put individual personal data at risk. Those weaknesses could be found in organizational security systems, organizational policy and practices, or organizational failure to ensure adequate data security measures by entering into contractual arrangements with its data intermediary.

---


90 See *Propnex Realty Pte Ltd* [2017] SGPDPC 1, para. 14. In this case, the Commission determined that the information contained in the Do-Not-Call List, which was in the search result and accessible by the public through the Propnex URL link, constituted personal data. The leaked data included the full names of the individual complainant and her sister, home phone and mobile numbers, residential addresses, and email addresses, as well as internal instructions to the agents contained in the Do-Not-Call List.

91 See *The Institution of Engineers Singapore* [2016] SGPDPC 2. In this case, the Commission found that “anyone with valid user IDs and Password in combination would effectively be able access the entire profile of an IES member and identify him or her.” IES argued that the leaked users’ IDs and passwords were remote from the third party’s access, since the leaked data was posted in “random, unrelated and unlinked” form. The Commission disagreed, explaining that the risk was not remote given possible means of access (i.e., the use of a dictionary attack with automatic scripting to access IES user accounts).

92 See *Central Depository (Pte) Ltd and Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC 11, para. 24(b). In both Toh-Shi cases, Toh-Shi had entered into services agreements with the alleged organizations, which required that Toh-Shi match provided data with the right customer, print, and mail out the statements to customers. In Toh-Shi I, the leaked data—contained in the monthly statements that CDP sent to its customers—was comprised of accountholder information, security holdings, transactions, and payment summary. The Commission considered as “sensitive” financial information involved in the breach.

93 See *K Box Entertainment Group Pte Ltd and Finantech Holdings Ptd Ltd* [2016] SGPDPC 1, para. 42.
Preventability. When determining whether the security practice at issue is reasonable or adequate under Section 24, the Commission considers whether, at the time of breach, the threat was a common one, whether a high degree of vulnerability was involved, and whether the breach was preventable or could have been detected by tools available in the market. If the answers to all of these questions are yes, then the Commission finds that the organization failed to meet its protection obligation under Section 24 of the PDPA.

In the case of IES, the Commission found that IES’s system contained “high severity vulnerabilities” to cross-site scripting attack, a common web threat that could have been detected by a vulnerability scan and patched by tools readily available in the market. IES also lacked encrypted storage of member passwords, security audits, system penetration testing, and contractual arrangements with its vendors specifying security measures to be in place and other specific instruction on implementing its security policy in actual setting.\(^\text{94}\) Taken together the above into its assessment, the Commission found that IES failed to provide protection obligation under Section 24.\(^\text{95}\)

In the case of K-Box, the Commission found that a number of precautionary measures, such as installation of software updates, regular database audits, and adoption of policies against weak passwords and unused accounts, could have helped the organization to prevent the breach. However, K-Box’s practices included a weak administrative password policy, retention of unused administration accounts, an outdated software library, and irregular IT system monitoring or audits, all of which could have allowed attackers to access and compromise its membership database.\(^\text{96}\)

In the case of Propnex, the Commission found that the organization’s vulnerabilities were due to a lack of internal policy prohibiting staff from sharing files containing personal information in the non-protected virtual online system. As a result, the search engine was able to index the leaked link and individual personal data appeared in the search results.\(^\text{97}\)

Likelihood of Causing a Subsequent Breach. It is worth noting that, in the cases of IES and K-Box, the Commission found breach of protection obligation based on a probable cause; security weaknesses which are likely to result in the subsequent leakage of data is sufficient for an organization to breach section 24, without needs of conclusive investigation on the cause and exact time of breach. In the IES case, the leaked login ID and password were posted in a random set by hackers on a third-party website; the Commission did not require evidence that IES member accounts were actually accessed or exploited by the third party thereafter.

Contractual Arrangement with Data Intermediary as First Step. There are a growing number of cases in which the Commission was satisfied with an Organization’s data security practices, and found only its data intermediary liable for breach of Section 24.\(^\text{98}\) Among those cases are two incidents in which Toh-Shi is a data intermediary. The Commission concluded that the organizations in both incidents had “undertaken an appropriate level of due diligence to assure itself that its data intermediary is capable of complying with the PDPA.” Therefore, according to the Commission, it was reasonable for those organizations to have expected Toh-Shi as the data intermediary to take the necessary actions.\(^\text{99}\)

\(^{94}\)See The Institution of Engineers Singapore [2016] SGPDPC 2, para. 30–33.
\(^{95}\)Ibid. It added: "The conduct of vulnerability scans using automated tools like Acunetix is considered industry best practice.”
\(^{96}\)PDPC's decision, K-Box, para. 27-28.
\(^{97}\)PDPC's decision, Propnex, para. 21-26.
\(^{98}\)the Commission also found that the organization fulfilled its obligation, despite its data intermediary’s failure to satisfy Section 24 in Tiger Airways Singapore Pte Ltd and others [2017] SGPDPC 6.
\(^{99}\)PDPC’s decision, Toh-Shi II, para. 27.
In Toh-Shi I, the Organization that hired Toh-Shi to process its customers’ personal data had established adequate security procedures and control; a number of measures had been taken e.g. specifying in contractual clauses with Toh-Shi the necessary actions and precautionary measures to be taken for protecting personal data, issuing the standard of operation (SOP) as well as providing specific protocol on data transfer. In addition, these Organizations in Toshi I and II had conducted annual auditing and on-site visits of the intermediary. Furthermore, the Commission found that Toh-Shi’s staff mainly caused the breach without the involvement of the insurance company as Organization. The organization, therefore, satisfied its duties under Section 24 of the PDPA. From the Commission’s finding in both cases involving Toh-Shi, the incorporation of security protection clause could be a recommending first step, not a complete safe harbor, for Organization to mitigate risks of liability under Section 24.

Non-Excuse of Not Knowing Technical Flaws. The Commission also emphasized that it was the organization’s responsibility to understand the limits of its security measures and mitigate vulnerabilities that came with them when such information was available and widespread on the internet at the time of the breach. Therefore, in the Propnex case, even though the company had relied on its in-house IT team, the Commission believed that it should have understood the limitations of its own implemented security measures—specifically, the inability of those measures to hide the URL containing personal data from the search result.

(iii) Reasonable Data Security Practices of Data Intermediary

Up to this day, the Commission confirmed that under section 4(3) data intermediary refers to any person who de facto processes personal data on behalf of an organization. This means that the actual practice of a person “having access [to], storing and retrieving” personal data make such person a data intermediary. This was the case with Finantech, the data intermediary of K-Box. Applying de facto standard, two external IT vendors hired by IES—one for web and CMS design service including on-demand maintenance, the other for web hosting service—were not data intermediaries under the PDPA. This ruling considered the fact that both vendors were actually restricted access to IES member database. The Commission later confirmed, in the Propnex case, that merely sharing common IT infrastructure between parent and child companies did not constitute evidence that one had processed personal data on behalf of the other. In both Toh-Shi cases, in which there were no contractual terms expressly specified Toh-Shi as data intermediary, the Commission inferred from the actual responsibilities of Toh-Shi under the contracts with the Organization that it was expected to engage in data processing, an act of data intermediary.

Basic Professional and Due Diligence Standard of Data Intermediary.

In the K-Box case, the Commission also set an expectation of “basic professional standard” and “due diligence” in data security practices performed by its data intermediary; where failure to meet this expectation would result in liability of the data intermediary under Section 24 and 4(2). In cases of insider breach, such as both Toh-Shi incidents caused by the organization’s employee, the Commission looked into whether internal data security measures

100 PDPC’s decision, Toh-Shi I, para. 17–18.
101 PDPC’s decision, Toh-Shi II, para. 27.
102 PDPC’s decision, Toh-Shi II, para. 27.
103 PDPC’s decision, Propnex, para. 22–25. The Commission also referred to a Google Support article represented by the organization itself in this matter.
104 PDPC’s decision, K-Box, para. 34
105 PDPC’s decision, IES, para. 24–25
106 PDPC’s decision, Propnex, para. 5.
107 PDPC’s decision, K-Box, para. 37–39.
and procedures that could minimize human errors were in place. In Toh-Shi I and II These include additional review layers, inspection manuals, and technology solutions. It also considered whether staff had actually adhered to the organization’s security policy when handling customer data. The Commission found that Toh-Shi’s staff failed to adhere to its sorting and review procedures, resulting in the errors resulting in the misaligned pages of printed statements containing sensitive personal data of another customer mailed out to the recipients.\footnote{PDPC’s decision, Toh-Shi II, para. 29–34.}

Based on these findings, the data intermediary needs to make sure that available means of security protection—including adequate layers of manual checks by staff, automated tools for review, and staff training on data security—have been sought to mitigate its vulnerabilities or errors that could lead to data breach.\footnote{PDPC’s decision, Toh-Shi II, para. 38(a)–(d).}

C. Aggravating and Mitigating Factors in Determining Breach

Given its broad discretion under Section 39 of the PDPA, the Commission has continuously listed the mitigating and aggravating factors that it takes into account when determining direction and penalties for the breached organizations. This list serves as a guide to the Commission’s views on desirable conditions and post-breach responses for organizations so to avoid aggravated penalties.

(i) Nature of Breach: Size and Type, Recurrence, and Degree of Involvement

In the K-Box case, the Commission weighed the “fairly large size” of the breach—which involved sensitive data of K-Box’s members being disclosed to the public—against the fact that the breach was not due to actions taken by K-Box staff.\footnote{PDPC’s decision, K-Box, para. 42(c), 42(d).} As for K-Box’s data intermediary, the Commission noted that if there was the fact present in this case that the data intermediary had provided an advice to K-Box, but was rejected. Such factual circumstances would matter when assessing culpabilities of the data intermediary.\footnote{PDPC’s decision, K-Box, para. 37–38.} In the Propnex case, the Commission considered the large scale of the public disclosure (1756 individuals’ personal data), the preventable flaw in the organization’s internal file sharing system, and the fact that 96% of records in the leaked list were non-sensitive personal data (e.g. a telephone number or residential address provided without any other personal data).\footnote{PDPC’s decision, Propnex, para. 32(a), 32(b), and 32(d).}

Toh-Shi’s second breach incident, which occurred a short time after the first, resulted in a $25,000 fine—five times larger than its first-time breach penalty. The Commission considered aggravated penalties from the larger number of policyholders affected by the second breach (8,022 policyholders, as opposed to 195 affected parties in Toh-Shi I) in addition to the social embarrassment aspect that the disclosure caused affected policyholders. The Commission also found that Toh-Shi could have prevented the breach with a better system of security auditing in place.\footnote{PDPC’s decision, Toh-Shi II, para. 38(a)–(d).}

(ii) Cooperation with the Agency during Investigation

Whether or not the respondent is forthcoming and cooperative with the agency during investigation has been established as mitigating and aggravating factors in assessing penalties and directions. In only a few cases, including the case of K-Box and Finantech, has the Commission found respondents neither cooperative nor forthcoming during investigation. These

\footnotetext[102]{PDPC’s decision, Toh-Shi II, para. 29–34.}
\footnotetext[103]{For an organization like Propnex, which relied on its own in-house IT, the Commission expected its IT team to understand the limits and risks of the security measures they had employed, in particular when the knowledge on limits of such tools on security protection is available on the internet, so as to minimize the inherent risks.}
\footnotetext[104]{PDPC’s decision, K-Box, para. 42(c), 42(d).}
\footnotetext[105]{PDPC’s decision, K-Box, para. 37–38.}
\footnotetext[106]{PDPC’s decision, Propnex, para. 32(a), 32(b), and 32(d).}
\footnotetext[107]{PDPC’s decision, Toh-Shi II, para. 38(a)–(d).}
uncooperative acts are incomplete response and plain facts of the breach incident submitted seven months after K-Box’s receipt of the Commission’s request. Most cases like Propnex case, the Commission found that organization respondent was cooperative and forthcoming during investigation of the breach, which also includes when it first admitted the breach to authorities.

(iii) Fair and Prompt Response to the Affected Individuals

The Commission also considered whether or not the respondents provided fair and prompt response to the breach and corrective measures toward affected individuals. For instances, the Commission was satisfied that K-Box made a website notification a day after becoming aware of the breach, and issued corrective measures within a month of the discovery. IES emailed a prompt breach notification to all IES members a day after discovery of the breach, informing them of the hacking activity on the site and of the measures IES had taken to minimize damages. These were disabling access to the portal member site, resetting IDs and passwords, and removing numbers and addresses from its database. In both Toh-Shi cases, the Commission was enough satisfied with Toh-Shi’s corrective measures after the breach that it did not issue further directives. In Toh-Shi I, the Commission noted that Toh-Shi had added additional layers of checks i.e., security supervisor, document barcode system, including technology solution to reconcile printed statements to prevent repeat of incident. In Toh-Shi II, it conducted a review of its staff training procedure and staff adherence to Standard Operating Protocol (SOP), and improved its tech-solution to prevent errors in manual sorting process. In Toh-Shi II, the Commission considered as mitigating factors the company’s notification and apology to three affected victims which included vouchers of $100 for each, as well its retrieval of the wrongly delivered documents.

IV. Singaporean Data Security in Times of Changes: New Apparel, Same-Old Vision

Despite tremendous changes taking place in technology realm and the cybersecurity legal landscape in Singapore affecting the PDPA applications, its original visions, key concepts and principles has continued to sustain yet been adjusted to be compatible with the more demanding international standards such as the EU General Data Protection Regulation.

The Personal Data Protection Commission has continued to bridge the gap between legal ideals and organizational practices, paving the pragmatic path of implementation for organizations to internalize into their data security practices. The new cybersecurity law, the Cybersecurity Act of 2018, does help clarifying the intention of the PDPA as a general data protection law applicable to all businesses. This is in contrast to the Critical Information Infrastructure (CII) sectors, namely energy, water, transport, health, government, information communication, media, security and emergency services, and banking and finance, which are subject to a more onerous duty under the new law and the Cyber Security Agency of Singapore whose responsibilities is to tackle the national-level emergent threats.

The proposed PDPA amendments emphasizes the original visions of the PDPA towards trust relationship and cooperation while making formal substantive changes to meet the

114 PDPC’s decision, K-Box, para. 42(f), 43(c).
115 PDPC’s decision, Propnex, para. 32(c), 32(f).
116 PDPC’s decision, K-Box, para. 42(a), 42(b), 43(a).
117 PDPC’s decision, IES, para. 39.
118 PDPC’s decision, Toh-Shi I, para. 21, 24(e).
119 PDPC’s decision, Toh-Shi II, para. 32, 38(f).
international demands. The proposed PDPA amendments on individual consent requirement allows businesses to automatically obtain individual consent for legitimate legal and business purpose when such business objectives are made available by organizations. This change, if accepted, would favor businesses and make it harder to breach consent requirements under the PDPA.

Another major shift according to the amendment proposal is the introduction of mandatory breach notification regime, replacing the current voluntary basis. Despite the outlook of a more stringent approach to breach notification, the proposed technology and post-breach remedies exceptions do allow organizations to not notify breach to affected individuals when the leaked data is intelligible for those who obtained, and when the remedies and prevention has been sought to eliminate the potential risks to affected individuals. This proposed mandatory regime would be triggered only when it is likely that harm would occur to affected individuals, not in every situation. The Commission has employed this risk-based approach in determining breach and applying aggravating penalties when breach incidents had impact on individuals. The proposed timeframe for notifying breach to individuals is “as soon as practicable”, leaving much room for organization to exercise discretion. The PDPC mitigating and aggravating criteria that require “prompt” responses are stricter in this sense. The proposed mandatory breach amendment and its exceptions are therefore a change in form and default functions, which affirm and elevate the status of PDPC’s criteria previously employed by the Commission in making decisions. It is noteworthy that the Commission retain power to order otherwise for the benefits of public.

The PDPC also proposed an inclusion of reporting duty to the Commission when the breach involves 500 individuals or more, as a separate criteria and duty to notifying individuals. The Commission refers to this threshold as “significant” breach despite disagreements of the industry and commentators. The Commission claims that it will better provide directions to organization as to how to remedy the breach, but this proposal would also benefit the Commission in collecting the data point and conduct further investigation against organizations that tries burying the incidents. The amendment, however, reflects the needs of cooperative efforts from organization to uncover incidents involved wider public. This also speaks to the existing PDPC mitigating criteria consistently applicable to the circumstances when organizations admitted of breach in the first instance and being cooperative in investigations.

In addition, the proposed amendments, which assign a duty to notify individuals of breach to Organization, not Data Intermediary, has pointed to the relationship basis upon which organization’s duty and liabilities arise. The proposal clarifies that Data intermediary only need to inform organization when being aware of breach, thus leaving the duty to notify affected individuals to organization. The Commission has already mentioned this line when considering the breach of section 24 and the mitigating and aggravating criteria applicable throughout the cases. This amendment therefore points to the underlying trust relationship and cooperativeness approach found in the PDPA objectives as implemented by the PDPC.

From the author’s view, the proposed amendments on breach notification further highlight the venue always encouraged by the Commission throughout the decisions. That is for organizations to opt for self-correcting, remedying and mitigating risks to affected individuals after the breach, so that they will not have to notify breach to individuals according to the new proposal. Or at least, organizations will have to try their best efforts to mitigate impacts from breach before notifying so as to not alarm affected individuals, which could put organizations at risk of losing reputation and consumer trust. Thus, this approach draws out the relationship between organization judgments in handling breach and affected individual’s satisfaction. When
organization breach response is unsatisfactory, the PDPA empowers individuals with abilities to lodge a claim against organizations that does not do enough to mitigate impacts and offer satisfactory compensation or remedies to individuals. The proposed amendments expect organization to rely on their honor codes and reasonable judgment as to how they solve data breach and post-breach responses, yet ready to demonstrate such evidence to the PDPC when needed. Following the original visions of the PDPA of promoting trust, the proposed amendments and PDPC implementations through cases has instantiated trust relationship and cooperation approach in the Singapore’s unique ecosystem.

Section II: A Comparative Analysis of Design Platform for Data Security: Implications for Trust Relationship and Cooperation

A. Individual-Business Relationship within the Platforms of FTC Section 5 and PDPA Section 24
   i. The Implied versus Direct Approach to Data Security.

   The FTC approach to apply Section 5 in protecting security of personal data has never been a straightforward way. It needs expertise in applying fair and non-deceptive basis to the data security and privacy practices of businesses in order to communicate the substantive baseline for reasonable data security practices to business. These indirect implications derive from the FTC’s consistent interpretation through its enforcements against unreasonable practices and listed reasonable practices found in the settlement orders entered into with businesses. Due to the current fragmented FTC regulations, which pose limits as to the scope, obligations, and tools for the enforcement against different business players, there is an attempt of the FTC to streamline the interpretation of reasonableness under Section 5 to align those of the GLBA and other FTC regulations.

   Singapore’s Personal Data Protection Act provides in a direct and positive manner of the duty for businesses to provide safeguards to individual personal data under Section 24, compliance of which requires meeting the reasonable person standard, a general principle of the PDPA. The PDPC has consistently illustrated specific examples of reasonable and unreasonable practices of business parties acting as Organization and Data Intermediary through advisory guidelines and individual cases before the PDPC.


      - U.S. Notions of Informational Duties, Trustworthy Business and Consumer Independence

      Informational Duties.

      The scope of Section 5 of the FTCA has placed significant constraints to the FTC regarding the way to approach data security issues and shape business behaviors. The objectives and fair and non-deceptive principles of Section 5 could end up addressing data security protection only on the level of informational duties, rather than addressing a full spectrum of substantive safeguard measures to protect consumer security interests on personal data.

      The FTCA objectives are to protect consumer choice and fair competitive market. Thus, data security protection is relevant to the extent that it falls within such frames. That means to prohibit certain data security practices that deter such objectives for the purpose of ensuring a
well-informed decision and availability of choices for consumption. For the purpose of maintaining a fair ground for business competition, data security protection matters only when it affects the transparency of information disclosure on policies and practices of businesses relating to products and services.

The fair and non-deceptive principles of Section 5 also raise a number of issues when applied to data security protection. First, the duality of FTC’s reasonable standards of data security practices found on deception and unfairness claims raise confusion and legal uncertainty for businesses in navigating through that disrupted the emergence of norms on reasonable data security practices by businesses without a clear and streamline clarification. The FTC has authorities to enforce fairness and deception on an independent basis, which means “deceptive” practice is not necessary lead to unfairness conclusion as in theory. In practice, the FTC does not clarify its choices on why sometimes when similar facts presented it put forward only unfairness claims without further deceptive claims against certain company’s practices.

Second, the FTC’s overreliance on exercising the deceptive claims against broken promise could dilute the meaning and values of data security derived from unfairness basis. As the FTC recognized deceptive representation itself as harms to consumer choice on products or services without the need of demonstration of other harms, its continuation of exercising deception authority would develop only limited notion of individual rights to privacy and data security in terms of right to get truthful information, informed decision-making ability and protection of promised consumer expectation and control. While others may argue that these aspects form core notions of the U.S. individual privacy values, which rest upon honor of promise, truth, and choices of individual consumption, a full spectrum of privacy values from the disclosure of personal information has been neglected. These are, for instances, individual loss of dignity, reputation, safety etc. Ignorance on these notions has seen in previous FTC actions under Section 5, and as a consequence, individuals suffered from these uncovered privacy injuries receives no protections or remedies.

Furthermore, actions based on the deceptive statements can be misled to suggest to businesses on “what is a reasonable promise” rather than “what are reasonable practice” on data security and privacy. As in the FTC case of Nomi where higher standard of promises on state of art security level could turn against the company itself when its security measures meets industry standard but fail to deliver as promised. This could result in discouraging businesses to consider adopting higher data security standard of practices beyond their peers, as they also bear higher risks of deception claims aside from higher costs of investment.

To those ends, reasonable data security practices within the scope of Section 5 centralize on establishing informational duties for businesses to provide adequate and accurate disclosure to a consumer to make an informed choice. Data security and privacy is a part of products and services in commerce. Thus, it conveys values of transparency that form a perceived trustworthy character of business in U.S. perspectives.

A Trustworthy Business in U.S. Notion.

From the view of trustworthiness, being trustworthy business in U.S. notion is measured from acting in a transparent way of providing accurate and adequate information disclosure. This notion of trustworthiness that contains information transparency has been carried forward by the FTC and applies within the context of data security and privacy.
This notion is consistent with cognizable injury from company’s broken promise under Section 5. A false and misleading representation by business, either expressed or implied, already cause injury under Section 5 by undermining transparency and subverting choice of consumer. It follows for violating businesses that the untrustworthiness impinges on their character arisen from deceitful and non-transparent acts on information practices. In this sense, perceived accountability acquires from being accountable for any misunderstandings and when the bad surprise occurred to the consumer from the unlearned and unexpected when making choice of consumption. Less emphasis is made on what happened following the breaches.

*FTC Informational Injury.*

Besides affecting to the choice of consumption and fair competition, harm to privacy and security and harm to personal data by themselves remains uncertain. They stand on a loose ground unless they can objectively and concretely demonstrate in the forms of monetary and threats to consumer health and safety, thus considered Informational Injury by the FTC. For instance, the unauthorized disclosure of personal data by itself may not be sufficient to prove harm and injury occurs to an individual unless accompanied with above mentioned consequent threats. Unfairness basis of Section 5 also requires that harm is substantial enough considering the magnitude of harm and the number of consumers affected. This means that small effects to large number of individuals and those related to monetary, health and safety often meet substantial requirement. It is not the intended scope of Section 5 to guarantee data security protection at an individual level. For instance, data breach caused to an individual may not be substantial enough regardless of how sensitive personal information is, and deceptive data security statements found to be material by minority of consumer might not be enforced by the Agency whose primary concerns has placed on the ordinary consumer understanding.

- *Having Control of Choices as Consumer Independence.*

Empowering consumer with choices of consumption has been the key to an ideal of competitive market, the pillar of Section 5. It follows that the disclosure of information is a mechanism integrated into Section 5 to promote informational equality between business and consumer, aiming to meet the ideal of informed consumer choice becomes main force that drives market demands and shapes business behaviors. Information transparency therefore becomes the integral values promoting together with the decision-making ability of consumers. When importing this *ideal of control and choice and fair and transparency information* mechanism and values into data security and privacy realm, such importation carries the notion of privacy and security in term of one’s ability to control by having choices and decision-making ability to consumption, with abundance of information beforehand. That imported meaning paints a consumer’s image as being rational for they know what is best for oneself based on one’s being intelligible in discerning overloaded information disclosed to them. Whether this image aligns with a consumer’s perception of oneself in the market and behavior in consumption of products affecting one’s privacy and security is another issues raised by scholars. Regardless of those, under Section 5 of the FTC Act, privacy and data security has been informed by self-control through decision-making through consumption that brings the sense of individual empowerment and freedom.

- *Singaporean Notions of Duty of Care, Trust Relationship and Consumer Dependence*
Duty of Care to Personal Data.

The PDPA subjects organization’s data security obligations and retention of personal data under the duty of care to personal data. Wide range of substantive and procedural measures fall under this protection obligations, which focal point is not limited to information disclosure duty. Having reasonable person standard as general principle for compliance with, the PDPA paves way for objective values in a society to take part in what a reasonable person would do in a particular circumstance regarding personal data treatment. That means what is reasonable for an individual acting in business capacity and for board members in a corporation could be varied due to availability of resources, capacity, professionality and expertise. In the author’s view, this reasonableness principle brings out the human aspect behind the corporate shield to be considered when determining what is sound for organizational judgment to comply with the PDPA regarding data security practices.

- Trust and Dependent Relationship.

Having reasonableness principle applied, the PDPA predisposes that an individual relies on a sound or reasonable judgment of a business party to regard any individual concern with personal data including security and privacy aspects. That premises draws on a dependent relationship between an individual and a business actor who is supposed to be able to put themselves into consumer shoes while exercising judgment with better preventive capacity and expertise based on information and resources they have beforehand. That means business actor have to foresee potential issues that goes beyond individual expectation and exert right actions in a particular circumstance. That provides a contrasting ideal with the U.S. notion of consumer empowerment and independence because the PDPA is tailored in that a consumer can depend and trust on business reasonable judgment to cover broader types of harms and measures to address individual concerns in handling personal data. These are beyond FTC informational injury and duty to information disclosure.

- Inadequate safeguard measures.

Pursuant to Section 24 of the PDPA, the organization has obligations to implement reasonable safeguard measures to protect personal data. This covers wide ranges of measures against threats i.e. contractual arrangement, technology solution, implementing internal policy and practices and employee trainings. This security protection obligations apply to both Organization and Data Intermediary. Failure to comply with the provision occurs when there is inadequate measure putting in place; it does not need an actual unauthorized access or disclosure of information to breach Section 24.

- Empowering Consumer through Compliant.

There are many procedural designs of the PDPA that amplify consumer voice in negotiating with the business to receive satisfactory remedial actions after the breach. First is an individual right to make a complaint to the Personal Data Protection Commission after failure to reach and solve the issues with a organization party. Second, the PDPA offers a mediation procedure between the disputed parties, allowing number of cases to be settled between parties at this stage before it goes under the Commission’s full review and investigation. During the PDPD review, if there is the factual evidence that business party had taken right actions toward individual such as promptly notifying affected individuals of breach and proper remedies, the Commission will
apply mitigating factors and thus issuing only warning or small amount of penalties to the
breached organization.

- **Trust Relationship in contrast to U.S. Trustworthiness.**

The implications for trust relationship, found in the PDPA approach makes a sharp contrast
to the U.S. notion of trustworthiness based on transparency and integrity found in information
disclosure. The PDPA trust relationship grounds on the ideal of dependent ability of business,
substantiated by a cultivation of acts on trust in business decision-making and behaviors to
protect individual interests in such relationship. Trust relationship in this sense refers to the
character of a relationship, which in an ongoing and direct, whereby a party finds the interests of
the other as motivation in his/her interaction with that party. Put simply, protecting interest and
trust of the other motivates the action of a party. In personal data treatment, a motivation of an
act of a business party could be individual’s privacy and security interests in such personal data in
the control of a business party. The direct and ongoing information relationship basis forms a
legal obligation and liability for Organization in PDPA, who is designated to act on trust in
delivering extensive duties regarding data protection toward individuals as compared to partial
provisions applicable to Data Intermediary.

Act on trust refers to an act which the party initiating such act is motivated by the other
party’s relationship interests and risks countering his/her own interest in gaining trust from such
act. (It is not the same with acting without expectation, for such risk-taking act of a party is
motivated with belief to gain trust from the other as a result from protecting the other’s interests.)
These acts on trust are such as notifying individuals of breach and remedial actions which also
risks disclosing the breach, revealing poor organizational practices to the individuals, following
bad reputation, benefit losses and lawsuits. The PDPC does not make it mandatory obligations,
but encourage directly at Organization, not Data Intermediary, to perform to individuals. As
further examined in the PDPC implementation in Chapter 3, such extensive duty of
organizations ceases when the ongoing and direct relationship fades away as there is no further
purpose to sustain such relationship, and the other player has become closer proximity to
individuals in term of data control. (See, PDPA Decision Re: Social Metric).

Therefore, the aspect of “trustworthiness” in the PDPA’s design connotes the underlying
dependent nature of relationship, substantiated by real acts of risk-taking to protect the other
interests where trust performs as a motivation for such initiating party. In this sense, it differs
from notion of trustworthiness surrounded the FTC Section 5 approach, which refers to a quality
as perceived and measured by others from the transparent act in disclosing information to the
other. Such FTC section 5 prohibitions creates business obligations to disclose information in an
accurate and fair manner, and when doing so, such disclosure found a basis to find fault on such
business for breaking promise given. Information disclosure under section 5 speaks from
obligatory position rather than itself a motivation for remedies voluntarily made to the individual
party. Even when businesses risks choosing to disclose information more than necessary in the
way that counters their interests and understanding that they have to be accountable for those
statements, the U.S. trustworthiness does not contain the elements of an ongoing and direct
relationship, and exchange of trust as motivation to act for the other as the PDPA do. The
accountability in U.S. notion also accounts for information disclosure and statements given by a
party as promises in the past and at present, but not carry forward onto the future interests or
what is unexpected or not relied on by the other party at the time such promise has been
made. The PDPA accountability rather cast light onto how to act in a responsible way with due efforts in remedying breach and impacts.

B. Platform for Distributive Liabilities and Cooperation among Data Processing Businesses.

The U.S. design of Section 5 and other FTC regulations do not clearly distinguish between the role of Data Processor or Data Intermediary and its relationship with a Data Controller, an organization with principal responsibilities in collection, use and disclosure of personal data. The Singaporean PDPA design, by contrast, follows other models which defines the roles of Data Intermediary (DI) and Organization as well as legal relationship between them. The divergent approach provides the implications of how a distribution of liabilities within a regulatory design could bring in mutual interests and cooperative perspectives on regulatory compliance.

- The unclear distributive system of the FTC.

Section 5 of the FTCA does not establish the clear basis to determine when a business party acts as Data Controller and Data Intermediary, thus resulting in the blurry scope and extent of the obligations and liabilities among business parties involved in data processing business. The design of Section 5 governs any business party offering a product or service to an end user in the market to have duty to conduct a fair and non-deceptive act to consumer. Thus, it seems to drift beyond the scope of Section 5 to regulate the conduct of businesses in the upstream, such as the wholesaler and other resellers, not offering a direct service or product to end users. Such presence of fragments in the design of Section 5 is significant when applying to breach, data sharing and nature of data processing businesses for any leakage at any point in the data sharing stream could render all efforts of prevention become fruitless. Unless there is a clear norm following among players in the data sharing businesses or a clear command of law on their relationship and liabilities to one another, it is difficult to envisage their incentives to cooperate in data security practices in the presence of Section 5 approach.

- PDPA’s Distributive Liability, Assurance and Cooperation.

Unlike the FTC approach, the PDPA carves a clear role and venue for business players acting as Data Intermediary and Organization to interact with each other. This turns out to be a seamless web of liabilities for whoever comes into contact with personal data either by processing, having in possession or control of such data. These liabilities also hand down as data have been transferred from one party to another party in data sharing and processing businesses. The PDPA assigns Organization, either business-to-business or business-to-consumer, with a principal role regarding the protection of individual data and overseeing practices of its data intermediary. Organization has more extensive and direct obligations towards individuals pertaining to personal data compared to its data intermediary whose obligations is limited to data security and retention, thus play a secondary and indirect role in towards individual in data protection. A clear instance is that the PDPA specifies that an organization is liable for any unauthorized disclosure of personal data caused by its data intermediary, unless it can demonstrate reasonable efforts on its part to ensure and oversee the data intermediary to proper treatment to personal data. As further illustrated in Chapter 3 in the PDPC’s implementation, whether an organization and a data intermediary comply with Section 24 on reasonable data security practices will be determined separately. A data intermediary is not always found breach together with an organization when it can prove reasonable practices and advice has been provided to the
organizations, thus not facilitating the breach. From this view, the legal relationship between organization and data intermediary established under the PDPA aligns with the interrelated information relationship in data processing business, where there is an area of shared responsibility and a mutual interest to cooperate between parties in order to prevent breach and to comply with the PDPA so as to avoid the Commission’s investigations and penalties.

- A Perspective Line for Cooperation as Assurance.

Cooperation is necessary in data processing businesses because consumer data is not handled by a single entity, but gone through several eyes and multiple entities involved before delivering products and services to a consumer. Personal data is susceptible to breach; human error, a system security flaw, or an accomplice with the recklessness of others could lead to a data leakage, undermining the whole point and efforts of data protection. In the author’s view, incentives to cooperate is evident in reality, but the matter as to how a regulatory design could emphasize on these incentives and draw a perspective line for businesses to find mutual interests in cooperative acts is a question for a regulator. Speaking from assurance perspective, the PDPA’s clear perspective line of scopes of liabilities between business players do assure businesses with certainty on ways of interactions, and the risks and consequences arisen when navigating through this path. On the contrary, the Section 5 path does not provide enough assurance for those involved in data processing businesses to be cooperative in compliance because of the unclear cue and command for interactions, hazy scope of duties and relationship between them. All of these does not point to the area of shared responsibility among them that will encourage them to find mutual interests in cooperation.

C. Relationship between Enforcing Body and Businesses: Specific Commands and Cooperation.

- PDPC’s Variety of Means to Engagement, Broad Discretion and Informal Approach.

The Personal Data Protection Commission (The PDPC) empowered with broad discretion and tools under the PDPA to issue the binding and non-binding guidelines with recommendations for businesses to adopt into their practices. Among those, a model clause of data protection equivalent to industry standard, for instance, is recommended by the PDPC to be entered into with a data intermediary. This has found to be effective means to preliminarily identify who is a data intermediary of organization, to establish the private liabilities between them, and recognize the industry standard to accelerate a more uniformed business practice. As found in Chapter 3, the PDPC refers to these guides in decisions and form criteria in determining breach and penalties, which urges and motivates businesses to follow and cooperate in adopting these measures in absence of legal mandates. Apart from issuing of guidance, the PDPC performs a more neutral role of a mediator as requested by the disputed parties, before it conducts further reviews of complaints and issues decisions.

- Broad and Non-specific FTC’s Direction and Means.

Even though the FTC has similar functions with the PDPC in providing guides for businesses to reasonable data security practices, a venue for communication between the FTC and businesses under Section 5 appears to be more constrained by means of directions given by the authority. The FTC can exercise power to discontinue prohibitive unfair and deceptive business measures, but lacks an authority to specifically command violating businesses to adopt certain practices in compliance with law. Even though its dispute settlement agreements with businesses allow the
agency to specify certain specific data security practices to be reasonably implemented in the Mandate Comprehensive Privacy or Security Program, these measures have raised issues on the due process and beyond the FTC authority by businesses. From cooperative perspectives, the design of Section 5 disallows specific commands and directions to be communicated to the businesses, thus the FTC is unable to urge them with illustrations on what are desirable pre- and post-breach measures or direction so as to pursue in implementations with the FTC.

\textit{v. Reliance on Insider versus Outsider: Trust Resources for Breach Discovery and Common Protection}

- \textit{The PDPA’s Reliance on DPO as Trust Point.}

Section 11 of the PDPA mandates every organization to appoint at least one data privacy officer (DPO) as part of its openness obligation. The DPO contact shall be made available to the public. This is another indication of a direct venue established for individuals to report the breach incident directly to organization before the DPO passes the issues to relevant departments, such as security and IT, auditing and compliance and legal to get involved, or elevates to the decision of organization’s directors and board members. The proposed amendment to DPO qualification to be a C-level employee demonstrates the importance of this position. Chapter 4 provides supporting evidence on the evident role of DPO as organizational internal compliance, a trust and cooperative point within the organizations where the internalization of the PDPA and all resources pool together.

- \textit{The FTC’s Reliance on Outsiders.}

Rather, the FTC approach relies on outsiders such as independent researcher group and media to discover and report data breach scandals. Even though Section 5 does not express so, the FTC found a company’s unreasonable security practices, among others, from its failure to establish a proper channel for third-party report of breach. \textit{(Re: HTC, Re: Lenevo\textsuperscript{121})}. When consistently applied by the FTC to the cases, these findings suggest an implied duty to establish a specific venue to receive third-party breach report.

In the matter of Fandango, the FTC in alleging the respondent with unreasonable practices found that, among others, the lack of “clearly publicized and effective channel for receiving security vulnerability reports. Their reliance upon its general customer service system resulted in the security vulnerabilities issues not being escalated to a proper team for further review.\textsuperscript{122} In the matter of HTC\textsuperscript{123}, the FTC in alleging the respondent with failure to employ reasonable security in its customization devices found that, among others: failure to “implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.”

The FTC also made reference to the research and publications on cybersecurity threats at the time of breach as evidence for the respondent’s foreseeability and preventability of such threats. Failure to respond and employ available measures to prevent the risks results in the unfair and an unreasonable data security practices. In the matter of Lenovo, the FTC in alleging the respondent with unreasonable practices found its failure to update or stop selling computers with

\textsuperscript{121} In these cases, the company and its customer service mistakenly ignored warnings from third party researchers, and thus failed to elevate claims to the security team of the company.

\textsuperscript{122} The FTC matter Re: Fandango, Para. 17.

\textsuperscript{123} The FTC matter Re: HTC America.
vulnerable program preinstalled after receiving the researcher reports placed consumers at risks from exploitation. Risks became higher when security researchers and bloggers published such vulnerabilities and way to exploit two months after the respondent becoming first aware of its vulnerabilities. Similar FTC mentioning on security professional warning about risks are found in the compliant of the matter of Reed Elsevier.

All of these evidence points to considerable reliance and weight given to the role of outsider parties in the discovery of a breach and suggest the standard of reasonable security measures to be employed by the companies. The independent parties has become an integral function of public vigilance who conducts a review of informational disclosure by businesses on behalf of consumers under FTC application of Section 5 to data security and privacy protection.

vi. A conclusion.

This chapter demonstrates the characteristics of the trust-relationship and cooperative basis to data security regulatory design of the Singapore’s Personal Data Protection Act in contrast to the notice-and-choice model of the U.S. Section 5 of the FTC Act. Those divergences are found in the following areas: (a) platform for individual-business relationship; (b) distributives liabilities among data processing businesses; and (c) the structural relationship between the enforcing body and businesses. First, trustworthy businesses in the U.S. design speaks from the transparency viewpoint of information disclosure made by business to consumer. Thus, informed choice purported to empower a consumer with control and independence in their consumption evolves the notion of U.S. privacy and security. By contrast, trustworthy businesses in Singaporean design speaks from the underlying relationship and interactions between the business and individual parties motivated by trust of the other. Thus, dependency on trust of the others in protecting relationship interests informs the Singaporean notion of individual privacy and security. Second, the Singaporean design of distributives liabilities among data processing businesses brings in cooperative perspectives of players in compliance with the law in contrast to the uncoordinated approach of U.S. Third, the Singapore’s variety of means to the Commission’s engagement, broad discretion and informal approach provides certainty and assurance to businesses which induces cooperation, which lacks in the broad and unspecified directions of the FTC. Finally, the aim for the PDPA is for organization to resorting trust resources within the organization for breach discovery while the FTC relies on outsider and independent group for vigilance. Chapter 3 continues to further examine these aspects in the enforcement actions.

---

124 The FTC matter Re: Lenovo, Para. 22.
Chapter 3
A Comparative U.S. and Singapore Data Security Breach Enforcement

Chapter Abstract

This chapter continues to approach the question of how data security regulation can promote trust relationship and assurances from the case enforcement perspectives. By examining the selected decisions on data security breach issued by the U.S. Federal Trade Commission (the FTC) and the Singaporean Personal Data Protection Commission (the PDPC), the decision analysis found the convergence and divergence in the U.S. and Singaporean enforcement approaches which have implications for trustful and cooperative organizational behaviors in both jurisdictions. Despite convergence in criteria adopted to determine reasonable data security practices of businesses, the divergences are found in their interpretations of the following areas: (i) the scope of application; (ii) the extent to which reasonable standards are applicable to different types of business actors; and (iii) how both agencies recognized the respondent’s intent and attitude involved in a breach and their post-breach responses in their decision-makings. This chapter highlights the evidence found in the agencies’ decisions that align with the venues constructed from the regulatory designs in Chapter 2: the U.S. and Singapore approaches to data security diverge as to how they set focal points on trust relationship and assurances, not just in principles but the implementations by enforcing bodies through enforcement actions.

Chapter Introduction

The following decisions demonstrates that the PDPC has continued to draw out the clear legal relationship between business actors of different roles through contracts and de facto behavior, thus creating a web of liabilities and a principal-and-agent like relationship between the principal business actor and its data intermediary. In such characteristic of relationship, these business actors are clearly informed of their roles in terms of the beginning and end, the nature of shared and separate responsibility towards other businesses and individuals regarding reasonable data security practices. The absence of those found in the FTC approach, which remains silent on the distinctions between the characters of data controller and its data intermediary as well as relationship between them. This results in the inconsistency as to choices made by the FTC in initiating actions against certain businesses and disregarding of others, as seen in the selected decisions. The departure of the PDPC’s approach has paved different paths open to different choices and motivations for these business actors to interact with individuals. This sheds light onto the characteristics of trust relationship and cooperation as part of mechanism adopted by the enforcing bodies in regulatory implementations.

In addition, the PDPC consistently recognized the positive attitudes and post-breach responses from the breaching organizations towards the affected individuals and the agency, as mitigating or aggravating impacts for the penalties and directions imposed against organizations in these selected decisions. These criteria provide assurances for organizations that their trustful acts, i.e. self-admittance of a breach and cooperation with the PDPC, and prompt notifications and remedies towards affected individuals, are desirable and will receive favorable consideration by the agency. In doing so, the PDPC could mitigate some inherent risks and uncertainty from rendering such acts borne by organizations. In the FTC’s selected actions, these acts have not
been formally recognized or guaranteed with favorable conditions by the agency despite the fact that some respondents performed those trust behaviors. Rather, the FTC order directed the organizations to establish a proper venue to receive reports from third party groups, and found their failure to react to the reports they received to be unreasonable data security practices.

This, taken together, emphasizes how the discrepancy between the PDPC and the FTC’s interpretations further shapes the different venues for trust relationship and assurances under the U.S. and Singaporean approaches. The PDPC encourages individuals to rely on “prudent business parties” in handling their personal data, purported to promoting trust in information relationship, in alignment with the principles of due care and reasonable person standard under the PDPA. The FTC’s approach under section 5, however, relies on the outsiders to check on the transparency and trustworthiness of businesses in support of consumer protection.

The first section of this chapter provides an overview and different landscapes of data security issues brought before the FTC and the PDPC taken into account in selection of cases for this study. The second section provides a comparative analysis of the FTC application of Section 5 to data security issues in comparison with the PDPC’s actions under Section 24. The analysis demonstrates the divergence and convergence in their interpretations of reasonable data security practices, which gives rise to implications for trust-enhancement and cooperation, to be discussed in Chapter 4.

Section I An Overview of Landscapes on Data Security Issues Before the FTC and PDPC

The FTC and PDPC enforcements on data security are against similar weaknesses in data security practices of businesses. Causes of data breach are from both insider leakage and outsider attack. The weak organizational practices range from data mishandling by employees, weak password policy and failure to limit access to individual personal data. Some of these existing vulnerabilities in the organizational internal control also invite malicious actors to intrude and exploit for further misuse. For instance, when the failure of a company to detect and patch its security systems against common threats allows hackers to access and obtain personal data, especially sensitive financial personal data.

A. Meaning of “Data Security Breach” to Cover Intent and Inadvertent Act

For this chapter purpose, data security breach covers both intentional and inadvertent misconduct on personal information by business actors. Intentional breach refers to when a business deliberately or willfully disregards the law and exploits personal data for its own benefit. Inadvertent breach refers to when a business unintentionally, but recklessly disregards in treatment of personal data. For the PDPC, making such distinction on the intent involved in a breach is significant when assessing whether the issue falls under Section 24 or Section 20 and 13. Section 24 governs data security breach, or so-called under the PDPA as the breach of protection obligation. Section 20 and 13 governs the consent breach, which serves as functions close to privacy breach commonly understood. Such intent in breach also matters when the PDPC distinguishes when a business actor acts as the organization and data intermediary for determining the liabilities arising therefrom. For the FTC enforcement, such distinction is insignificant under Section 5, which applies to business conduct regardless of the intent involved in a breach or whether the issue is a data security or privacy breach.
B. Selection of Cases

The selection of cases for the analysis conducted on decisions regarding data security breach, made by the FTC and PDPC until February 2018, 68 and 32 cases respectively.

All cases from the FTC and PDPC were divided into 8 groups according to three criteria: (i) whether the causes of leakage are from the outsider (O) or insider (I); whether the respondent’s business size is large (L) or small and medium (S); and whether the business model is business-oriented (B) or consumer-oriented (C). Then, each from the FTC and the PDPC within the same group is selected into comparison based on similar breach pattern found in the factual circumstances, such as, the leak caused from the CC email, or both involved credentials were stolen.

Based on the above criteria and the availability of cases falling under each from the FTC and the PDPC, these selected cases are categorized into three groups as follows.

**Group A—Cases of Outsider Attack:**

O-L-C  Twitter v. Orchard (Employee’s credentials stolen by hackers)

O-L-B  N/A (no PDPC case in this category)

O-S-C  N/A (no PDPC case in this category)

**Group B Cases of Insider Breach:**

I-L-C  Eli Lilly v. Singapore Debt Counseling (CC: email address)

I-S-B  Lookout v. Data Post (Employee breached internal policy)

I-S-C  GMR v. GMM (unencrypted file sharing)

**Group C—Cases against Platform Actors**

I-L-B  Platform Acting on Behalf of Another: Vision I properties v. SocialMetric

O-S-B  Platform Acting on its Own Behalf:

---

125 Large-sized organization means an organization with more than 400 employees, and small and medium sized organization means an organization with less than 400 employees.

126 In Re: Orchard Turn Development, the PDPC made reference to the FTC matter against Twitter as having similar cause of breach.

127 The cases were not examined because of different breach circumstance. Lookout involved one customer’s employee exploiting the easy-to-guess password and bypassing to accessed the tax forms of other customer’s employees whereas the PDPC Re: Data Post concerns the printing companies acting as a data intermediary of the bank, and the erroneous process caused two bank statements sent to the wrong bank’s individual customers. The fact provides that breach notification and corrective acts were made by Lookout 1 months after the incidents to its business customers whose accounts may be viewed. In Data Post, individual who received the statements of other individuals notified the bank, which promptly reported the PDPC and MAS about the leakage.

128 Despite the similar breach pattern, GMR is a consumer facing, but more oriented to business customers and involved the leakage of transcript containing health information. Other candidates of the I-S-C category, The FTC Re: Upromise and Re: Compete, are eliminated because of the breach involving intentional excessive collection of data from users to business clients—already discussed in the I-L-B. The breach in FTC Re: Genelink concerning the unrestricted sharing of health-related personal data with its service provider is not compatible with the PDPC cases in the I-S-C category; Re: Spear Security and Re: Eagle Eye (Condominium security service), Hazel Florists (Gift shops), Smiling Orchid (Food caterer with the restricted). However, it is noted that all the Singaporean respondents in this category provided prompt and corrective remedies and mitigating penalties applied. All did not notify breach to affected customer (ranging between 0-1 individual except in the case of GMM that affected 190 individuals.) All FTC cases falling under this category did not demonstrate breach notification or remedies.
Data Reseller and Data Brokerage

The selected cases represent the best match within each group. The study examined comparatively the criteria of the FTC and the PDPC in determining “reasonableness” of the respondents’ practices and the agencies’ recognition of post-breach behaviors. The finding suggests divergent criteria taken into account by the FTC and PDPC. The respondent’s post-breach responses, organization actors’ intent and the existing relationship basis plays significant role in the PDPC’s decision-making. These similar criteria are less significant in the FTC’s decision-making.

C. Points of Observation

In these selected cases, I observed the following points in the PDPC and the FTC’s interpretations:

i. Activities falling under the scope of application: commercial activities, business activities, non-commercial activities and non-business activities.

ii. Recognized injuries and harm: financial and non-financial harm, personal harm and harm to the public.

iii. The defining and distribution of liabilities between involved business actors: how obligations begin and end, triggers, separate and shared responsibility.

iv. Recognition of Trustful Behavior: self-admittance of breach, prompt breach notification, prompt correction and remedies towards the consumer, which I refer to as “Trustful Behavior”.

I investigated whether the respondents in the selected cases delivered such acts, and how the agencies regarded and interpreted such acts in their decisions. In Chapter 4, I borrowed the lens of self-regulation, compliance and trust relationship to interpret the meaning of such acts, and their implications.

Whereas the first and second points define the extent of protected right, the third point clarifies how the laws distributes obligations among business players, thus shaping their behaviors and relationship with individuals. The fourth point demonstrates how the FTC and PDPC different recognition on positive business behaviors towards individuals after breach could assure and motivate business behaviors into certain directions in breach responses.

D. The Analysis: The Intersection, Diffusion, Overlapping of the Interpretations

Based on those observation points from selected cases, the analysis found the intersections, diffusions and overlapping of the PDPC and the FTC’s interpretations. These decisions demonstrate that their interpretations converge on similar criteria applying to determine reasonable data security practices notwithstanding different basis of Section 5 and Section 24. However, there are diffusions as to the nature of regulated activities and how to determine reasonable standard for the business acting on its own behalf and for on another’s behalf, the organization and data intermediary. There are also significant differences between “consumers” who receive protections under the FTC, which also includes business end users versus the individual subject of protection under the PDPA. This has led to a contradictory result as to which actors’ certain actions will be brought against the reckless data security practices. Last but not least, there are divergence as to the formal recognition of the trustful behaviors by the
mitigating and aggravating criteria developed by the PDPC, in contrast to the absence of formal recognition found in the FTC decisions.

Section II A Comparative Analysis

A. Cases of Outsider Attack

The following decisions of the PDPC re: Orchard Turn Development\textsuperscript{129} (“Orchard Turn”) and the FTC re: Twitter (“Twitter”) demonstrate the applications of reasonableness standards under section 24 of the PDPA and section 5 of FTC Act to similar facts on the weak credential practices of organizations that led to the consequent hacker attacks and the unauthorized disclosures of personal data. The comparative analysis sheds light on the trustful behavior from respondents’ responses after the leakage, and how they were recognized by the PDPC and the FTC in assessing breach, directions and penalties.

I. Summary of Facts and Findings: The FTC re: Twitter and the PDPC re: Orchard Turn Development

The matters of Orchard Turn and Twitter share similar facts and findings: (i) both companies collected personal information directly from users; (ii) both were attacked by unknown intruders who obtained the valid admin passwords, and used them for gaining access administrative control of companies’ servers, putting the whole consumer database at risk of being compromised; (iii) security measures adopted by both companies at the time of breach were found unreasonable by the agencies due to the weaknesses found in employees password storage and practice policy which caused the breach incidents; (iv) the attacker used such control in conducting fraudulent and malicious acts, open to further exploitation by other attackers i.e. disclosure of the fraudulent reset passwords to the public, creating fake tweet from prominent user accounts sending fake blast email containing phishing link from Orchard Turn; and (v) both cases involved large database of user personal data.

The differences in both cases are on following points: (i) the nature of businesses of social online networking platform versus a retail mall; (ii) type of personal data accessed by attackers: the non-public information of Twitter user including private post and message, an email address, IP address, telephone number, and username for any user blocked account whereas in Orchard Turn, leak data involve subscriber data including a subscriber’s name, email address, birthdate, and membership registration date; (iii) how the breach was discovered by the public after the hacker’s fake tweets from user’s account versus by the in-house organization discovery of bogus loyalty program emailed to subscribers; (iv) the involvement of data intermediary in Orchard Turn versus Twitter in-house data security team; (v) the civil penalties imposed in Orchard Turn in contrast to no penalties imposed for Twitter.

II. The Case Analysis

\textsuperscript{129} PDPC decision re: Orchard Turn Developments Pte. Ltd. [2017] SGPDPC12, Case No: DP-1512-A612.
(a) The Intersection of Reasonable Standard: The Baseline and Aspects of Safeguard Measure

Reasonableness Does Not Mean a Perfect Security Protection. In Orchard Turn and Twitter decisions, the FTC and the PDPC do not imply perfect data security protection for their “reasonableness” standard. Rather, their mutual goals set towards organizations to have proper measures in place to protect consumer personal data, and that reasonable efforts have been made by respondents to seek available tools in the marketplace for preventing common cybersecurity threats at the time of a breach.

In the FTC’s response to public comment in the Twitter case, the Commission recognizes that “there cannot be perfect security and that data breaches can occur even when a company takes reasonable precautions to prevent them.” It also affirms the position provided in another response that the measure itself may not be a perfect warrant of no breach, but make a second breach more difficult.\(^{130}\)

These statements from the FTC were referred to by the PDPC in the Orchard Turn case whereby it further emphasized that the mere fact of a successful outsider attack itself does not constitute the breach of section 24, but merely serves an evidence that points to potential flaws in an organization’s safeguard measures.\(^{131}\) In addition, the PDPC provides that the fact that the system was being compromised by certain tools or technique may not be as important as to how the organization has paid due efforts to protect its collected personal data from threats from an outsider or insider. In the final analysis, the PDPC puts forward that it was not prudent for an Organization like Orchard Turn to deliver the said data security practices on personal data.\(^{132}\)

The Physical, Technical and Administrative Aspects of the Safeguards Measures. In Orchard Turn decision, the PDPC’s interpretation of reasonable data security measures under Section 24 also covers data retention and disposal practices by organizations. From this view, the coverage of PDPC data security protection involving physical, technical and administrative measures, equivalent to those found in the reasonable implementation as required by the Mandate Written Security Program (MWSP) of the FTC settlement orders as well as the GLBA safeguard rules for financial institutions.

In Orchard Turn decision, a number of weak technical measures were found to increase risks of personal data exposure to cyberattack, i.e. the transfer and duplication of personal data to a server that was connected to the internet and retained that data longer than necessary.\(^{133}\) The weak form of administrative measures against admin password sharing together with mandatory periodical changes of password demonstrate less than reasonable efforts to ensure the safeguard...
of the personal data set by reasonably anticipating, identifying and rectifying the technical security vulnerabilities at an early stage.

In the Twitter case, from 2006-2009, the weak administrative and technical measures on safeguarding users’ personal data taken together, failed to prevent unauthorized administrative control of the Twitter system. Among others, it failed to (a) implement sufficient administrative password policy on using hard-to-guess passwords instead of common dictionary words or similar ones to those used for accessing websites; (b) prohibit storage of a password on personal email accounts in plain text; (c) disable admin passwords after a number of unsuccessful attempts to login; (d) provide a separate non-public login page for employees; (e) enforce regular password changes, i.e. every 90 days; (f) limit employees’ access to non-public user information based on needs in performing their jobs; (g) restrict administrative access by other means such as granting access to specified IP addresses.134

Accordingly, both agencies’ view has converged as to their interpretation of baselines and aspect of measures covered by reasonableness standard as applied to organizational actors by both agencies.

(b) Divergence: The Intent Baseline Drawn between Security and Privacy Breaches

Deceived Consumer Choice as a Trigger for FTC’s Both Privacy and Security Actions. In Re: Twitter, the FTC alleged Twitter’s misrepresentation was based on two counts of similar factual circumstances: the first claim was on the deceptive statement of privacy policy regarding protection of non-public user information; the second claim was on company’s failure to honor the consumer’s choice in keeping their information private; therefore, making privacy choices appear to be illusory or deceptive.135

Despite arising from the same basis of deceptive acts, the second claim casts light on the security attack by a hacker that led to a breach of privacy promise, an additional layer of protection granted by Twitter in accordance with the user’s preference setting. This notion of privacy values deriving from consumer choice was emphasized by the FTC in making a response to public comment. It provided that: the non-public user information at issue did have value to Twitter users, especially the information which users deliberately designated as private.136 In this sense, the FTC’s meaning of privacy breach involves breach of the promise on deliberate choice made by consumer for such information to be private, whether it is intentional or unintentional.

Intent or Inadvertent Breach as Determinant for Security or Individual Consent Breach. The PDPC clearly makes a distinction between intentional and inadvertent misuse of personal information; the first would lead to issues under individual consent breach Section 13 whilst the latter would lead to breach of protection obligation under Section 24. Without clear evidence on willful disregard of user’s preference setting, it is unlikely that the facts appeared in Twitter would raise a separate issue under the PDPC’s interpretation of consent breach. And so, even though subscribers in

134 The FTC re: Twitter, complaint, para. 11.
135 Id. para. 13-17.
136 The FTC Letter in Response to Commenter Mr. Hale, In the Matter of Twitter, Inc., File No. 092 3093, Docket No. C-4316, para. 3: Further, the Commission believes that the nonpublic user information subject to unauthorized access as a result of the breaches described in its complaint did have value to Twitter users, especially the information users deliberately designated as private.
Orchard Turn had tailored their personal preferences to particular types of emails from the department store, the case would not present the issue of privacy or consent breach under Section 13 and 20.

For the PDPC, whether or not a user’s account and personal data were actually accessed or disclosed to an unauthorized party is not a condition for triggering the liabilities from a breach of section 24; it is an issue which matters only when determining mitigating and aggravating factors. That is why the Orchard Turn case did not indicate whether subscriber accounts were further accessed or disclosed without user’s consent by hackers. The FTC, however, would find such factual circumstances significant as a proof of injury element necessary to trigger unfairness claims under Section 5.

While intent involved in breach does not matter for the FTC in bringing actions against broken promises either on security or privacy of consumer data, such factors is employed by the PDPC to distinguish issues of data security from individual consent breach. The latter involves intentional act of organization in exploitation of individual personal data, and is deemed to be more egregious in nature as compared to inadvertent breach.

(c) Divergence in Agency Recognition of Post-Breach Response: Incentives for Remedial Acts

Positive Post-Breach Response as PDPC’s Mitigating Factors. In Orchard Turn decision, the PDPC recognized the fact that breach notifications and warnings of phishing email had been sent out by Orchard Turn to affected consumers on the day following the incident.\(^{137}\) The PDPC also considered these organizational behaviors as mitigating factors in determining the direction and penalty; the Commission found the organization had been cooperative and forthcoming in providing timely responses to the PDPC during the investigation, promptly remediating breach after learned about the incident. It was also satisfied with other corrective measures to improve organization’s IT security by purging all the personal data residing on the hacked server and subsequently putting in place a policy where the personal data will be removed from the server after a standard period of 14 days.\(^{138}\)

Positive Post-Breach Response Not Mitigating FTC’s Liabilities. In Re: Twitter decision, however, certain facts regarding breach notification, admittance of breach, or the action taken after the breach incidents had not been recognized in the decision, order, or complaints issued by the FTC. The fact that Twitter publicly disclosed the breaches shortly after the discovery had been raised by an individual commenter to the FTC proposed settlement with Twitter. The Commission, despite agreeing on its importance, clarified that such disclosure of breach does not relieve the company of liability for false or misleading statements previously made concerning its information security.\(^{139}\)

These divergence as to the FTC and PDPC’s recognition of post-breach responses towards an individual provide implications for assurance and incentives to shape organization behaviors towards individuals regarding self-admittance of breach, initiation of apology, remedial and corrective actions towards consumers, to be discussed in part III.

\(^{137}\) The PDPC decision re: Orchard, para. 8
\(^{138}\) Id. para. 40, para. 41 (d) and (e).
\(^{139}\) FTC Letter to Commenter Alex Radocea, noting that Twitter “made no claims to be perfectly secure,” had a security policy in place concerning administrative access at the time hackers gained administrative control of its system, and publicly disclosed the breaches shortly after they occurred. The Commission shares your view that a company’s prompt disclosure of a breach is important. However, such disclosure does not relieve the company of liability for false or misleading statements previously made concerning its information security.
B. Cases of Insider Leak: Email Disclosure of Sensitive Personal Data

Insider leakage of personal data is commonly found to be the cause of data security breaches under several FTC and PDPC decisions. As in the cases of Eli Lilly\(^\text{140}\) (“Lilly”) and Credit Counselling Singapore (“CCS”)\(^\text{141}\), the leaks were caused from simple errors during an employee’s sending out of email communication, which resulted in the disclosure of sensitive health related information in Lilly and financial information in CCS, to the members within the email groups.

The comparative analysis sheds light on the agencies’ interpretation of similar organizational practices under different standards of Section 5 of the FTC Act and Section 24 of the PDPA on the following issues: (i) the scope of application; (ii) aspects of harm and injury protected under reasonable standards; and (iii) how organizational responses after the breach were recognized and taken into account by both agencies in assessing breach, directions and penalty in decisions under section 24 of the PDPA and section 5 of FTC Act respectively. This analysis, when applied with trust and cooperative lens, provides implications for meaning of privacy and security from in relation to trust derived from the agencies’ interpretations including motivations for reinforcing of trust relationships between organizations and individuals.

(i) Summary of Facts and Findings: The FTC Re: Eli Lilly and the PDPC Re: Credit Counselling Singapore

The facts and findings in both decisions are similar in that: (a) these issues were considered data security breach by the agency of each jurisdiction; (b) the leakage caused from an employee disclosed individual email addresses to other members in the same group; (c) the leaked data were email address and found to be personal data of sensitive nature in such specific context of leakage; (d) these practices were found unreasonable due to lack of adequate review measures and internal control of organizations; and (e) both organizations were considered as large-size companies holding large volume of personal data.

The facts and findings in both decisions are different as to: (a) the commercial nature of Lilly versus the non-profit organization status of CCS; (b) health-related products of Lilly versus financial consultant service of CCS; (c) an application of misrepresentation and deceptive principles of the FTC Act versus the reasonable standard of the PDPA; (d) no penalties issued for Lilly versus relatively large amount of financial penalties imposed on the CCS; and (e) the mandate written security requirement program ordered in Lilly versus no further direction given considering the satisfied post-breach responses of CCS.

(ii) The Analysis of Re: Eli Lilly and Re: Credit Counselling Singapore

(a) The Diffusions as to Regulating of Noncommercial-Related Activities.

The FTC authority under Section 5 is limited to “any act or practice in or affecting the commerce”. Even though certain types of corporation are exempted from its application, the court applied section 5 to de facto commercial acts of those exempted organizations. Therefore, having

\(^{140}\) In the FTC Matter of Eli Lilly and Company, File No. 0123214.

\(^{141}\) The PDPC Decision Re: Credit Counselling Singapore, [2017] SGPDPC 18 Case No. DP-1610-B0261
the status of a non-profit organization may not guarantee a total exemption from the FTC reach under section 5 regarding data security breaches. 142

Unlike the FTC Act, the provisions of the PDPA apply to any individual or entity regardless of their business or non-business nature that falls under the definition of “organization”. 143 The case of CCS is an example of a non-profit organization, which is, without exemption, obliged to comply with reasonable data security protection where failure to do so would trigger liabilities under section 24. 144 It is also noteworthy that the PDPC did not apply a more lenient standard or mitigating penalty with the fact that CCS having non-profit nature.

Such distinction due to the scope of Section 5 and Section 24 implies the diffused grounds for the protection of personal data and its values arising from such protection. The FTC anchors on the commercial-related nature of activities and the effect it made on the market mechanism i.e. consumer choice, notice and consent while the PDPC recognizes a broader range of activities including non-commercial activities of an organization’s actors in its protection of individual personal data.

(b) The Diffusions in the Aspects of Harm and Injury Protected: Reputation and Embarrassment

Both agencies found the breached personal data were of a sensitive nature considering the context of the leakage of members’ email addresses which disclosed specific information concerning health or financial status belonging to members of the group. However, such findings were based on different reasons; the FTC’s basis is on the promise of confidentiality to consumers, whereas the PDPC pointed to the embarrassment, social stigma and effects on reputation due to the disclosure of an indebtedness status that leads to moral judgments by others on such individuals.

The FTC’s complaint does not explain further in Lilly as to why such medical information of Prozac users is considered sensitive. The Commission merely referred to the privacy and confidentiality clause of Lilly which had promised confidentiality of collected information, and later the breach of that promise. As implied from there, the finding of sensitive nature is based on the promise Lilly exchanged with consumers for obtaining such information from them. The FTC press release shares the opinion of J. Howard Beales, III, then Director of the FTC’s Bureau of Consumer Protection, about the sensitivity of data and the seriousness of consumer trust breach: “Even the unintentional release of sensitive medical information is a serious breach of consumers’ trust,” and “Companies that obtain sensitive information in exchange for

---


143 PDPA Section 2(1), “organisation” includes any individual, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore.

144 Before the case of CCS, PDPC in its early enforcement has held Institute of Engineering of Singapore (IES) liable for the breach of member personal data from an outside attacks to member account database.
a promise to keep it confidential must take appropriate steps to ensure the security of that information.”

In Re: CCS, the PDPC made it clear that the aspects of harm covered under section 24 included harm to affected individuals in forms of financial loss, embarrassment and harassment by an illegal debt collector. These aspects of harm led to the agency’s finding that the leaked email list is of a sensitive nature, and therefore greater care was needed during the handling of these data. The PDPC further elaborated that it took into account the nature and context of the follow-up email in finding the leaked email addresses sensitive data. The leak indicated the indebted financial status of individuals on the list who are “either currently facing financial debt, or was previously in debt, and that the individual is obtaining, or had previously obtained, assistance under the DMP scheme to pay off the debt.” Besides, by citing opinions of foreign commissioners, it is implied that PDPC concurred with the views on actual and potential harm which occurred to individuals from revealing their indebtedness status and the consequences on a person’s life regarding ‘social stigma, discrimination or tarnished reputation, moral judgments about the individuals and their spending, financial choices, earning power or about their character generally’. It is also noteworthy that the PDPC in assessing breach and direction found that potential and actual harm, injuries and hardship, serious reputational damages and embarrassment had aggravating impact on the breach.

Interestingly, the PDPC raised the aspects of public trust when assessing the breach and direction given to CCS. According to the decision, the Commission found that the breach posed threats to the general public trust on a larger credit system, and therefore resulted in aggravating factors when determining penalties for CCS. This illuminates the objectives of the PDPA on protecting trust in data processing businesses.

The cases of Lilly and CCS demonstrate different aspects of harm from the unintended disclosure of sensitive personal information as recognized by both agencies. The FTC finds its protection limited to the breach of consumer expectation arising from the promises given and relied on by individuals. Thus, FTC does not extend protection to other impacts from the breach beyond such expectation. The PDPC interpretation, by contrast, provides a broader and more

---


146 The PDPC Decision Re: Credit Counselling Singapore, para. 23, “Accordingly, the personal data that was disclosed in this case was not ordinary personal data but “sensitive” personal data. As will be elaborated on below, when it comes to the protection of “sensitive” personal data, organisations are required to take extra precautions and ensure higher standards of protection under the PDPA.”

147 Id, para. 19. The Commissioner restated that: disclosure of an individual’s indebtedness to other third parties could lead to harm to the individual because it could result in social stigma, discrimination or tarnish his reputation. These are real possibilities that can affect a person’s life. Hence, the confidentiality of the individual’s financial information should not be treated lightly. [the] presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.” The PDPC referred to foreign Commissioner: It is also worth pointing out that the Office of the Privacy Commissioner of Canada (“OPC”) has taken the position that “a simple reference to an outstanding debt, even without disclosing specific details about the debt, is personal information”. [para. 21] In Hong Kong, “[information] showing the financial problems of a customer such as default in payment is commonly recognised as sensitive data, and should therefore be handled with extra care (para. 22)

148 Id. para. 36 (a).

149 Id. para. 36 (c) the data breach incident may cause members of the public to lose trust in such credit counseling organizations to safeguard their personal data, which may frustrate the larger national credit management efforts.
straightforward venue to recognize intangible loss from self-embarrassment and reputational effect on individuals including those direct, potential and actual harms, which also trigger aggravating penalties under Section 24. In doing so, the PDPC interpretation allows social values to inform the values of privacy and security of data in addition to the market-defined values of it.

(c) Divergence in Agency’s Recognition of Organizational Post-breach Responses: Breach Notification and Other Remedies

In Re: CCS, the PDPC considered the responses of the organization after the breach incident in assessing penalty and direction given to the CCS. The desirable responses from CCS being recognized by the PDPC as mitigating factors are: (a) its cooperative actions during the investigations and the admittance of its mistake without delay, (b) the prompt breach notification sent to affected individuals, as well as an apology and an offer to delete the leaked email upon individual request, (c) CCS internal investigation conducted on the admin staff, and implementation of further steps to prevent future data breaches, such as undertaking a refresher course at organization-level on compliance with the PDPA, and a software replacement scheduled two months after the breach; and (d) no further breach reported.150

In FTC Re: Lilly, by contrast, neither the FTC’s complaint nor settlement order recognizes Lilly’s responses after the breach incident. Notwithstanding, the concurring statement of Commissioner Orson Swindle mentioned Lilly’s cooperation and responsiveness including its willingness to correct the mistakes after the breach. The statement provided considerable respect and empathy for Eli Lilly regarding the unfortunate and unintended disclosure, despite its longstanding efforts to protect privacy while also encouraging other firms to follow desirable practices adopted by Lilly. It reads: “Lilly should be respected for its long-standing efforts in development of its privacy practices, its acceptance of responsibility for the internal failures that resulted in the alleged violation of its privacy policy, and its willingness to take appropriate steps to correct those mistakes. I appreciate the company’s leadership in cooperating with us to improve its security measures, and I believe the firm will fully carry out its commitments under the proposed order. Lilly’s responsiveness and its efforts to improve corporate privacy practices can be a model for others to follow.”151 The concurring statement addressed the same organizational responses after the breaches, which were formally recognized and considered as mitigating factors by the PDPC.

With those mitigating factors, there is no further direction given to CCS, but still a relatively high penalty amounting to S$10,000 for CCS, compared to the highest amount of S$30,000 imposed for K-Box. On the contrary, no penalty was imposed on Eli Lilly, but the Mandate Written Security Program (MWSP) included in the settlement order required Lilly’s compliance with reasonable data security obligations. While violations of the MWSP resulted in fines of $16,000 per incident together with other auditing duties in accumulation could be sufficient for prohibiting and discouraging future incidents from continuation and recurrence, these duties do not ensure fair and prompt remedies from a breach to be provided to the affected consumer thereafter. This is in spite of that consumer would have expected fair and prompt post-breach remedies based on the promises of privacy and security made to them by the companies.

Lilly’s post-breach responses were not formally recognized, or taken into account in determining breach and penalties in the FTC’s decision-making, except a separate view in a

150 The PDPC decision re: CCS, Para. 37.
concurring statement provided by Commissioner Swindle. By contrast, these similar post-breach responses found in CCS were recognized by the PDPC as aggravating or mitigating factors in determining penalties, the criteria the PDPC at its own discretion developed under the PDPA. The divergent approach taken by the FTC and PDPC has implications for the emergence of norms on desirable post-breach behaviors and the incentives provided to an organization regarding the admittance of a breach after its discovery, and the initiation of prompt corrective and remedial action towards an affected consumer, together with cooperation with an agency during the investigation. The FTC’s disregard of desirable post-breach organizational responses may discourage the emergence of such norms on the prompt admittance of a breach and preventative correction and remedies to be provided to affected individuals.

C. Cases Relating to Platform Providers

This part discusses two types of data breaches relating to platform providers. The first type concerns misuse of personal data involving the platform, which processes data on behalf of the other business party, which I refer to hereafter as “the platform acting as data intermediary”. The second type concerns intentional and inadvertent leakage of personal data involving data platform acting for their own business purposes, which I refer to hereafter as “the platform acting on its own behalf”.

(i) The platform acting as data intermediary: The FTC Re: Vision I Properties and the PDPC Re: Social Metric

As discussed in the previous chapter, the FTC Act section 5 and the PDPA establish distinct obligations, liabilities and nature of relationships among business parties acting in different capacities. Such divergence has been evident in the implementations of law by the FTC matter against Vision I properties152 (“Vision I”) and the PDPC decision Re: Social Metric Pte Ltd153 (“Social Metric”).

The case of Vision I brought into contrast with the case of Social Metric has demonstrated how the FTC and PDPC have different basis to pursue claims on business actors for unauthorized disclosure of personal data of consumer. In Re: Social Metric, PDPC did not hold the merchants who hired Social Metric liable under section 24 for the unauthorized disclosure of personal data relating to their social media campaigns, in which Social Metric processed on the merchants’ behalf. Besides, as will be analyzed, the case highlights on the PDPC establishing boundary and relationship between the merchants and their platform providers in a manner similar to the principal-agent relationship, and has clarified its use of intent basis to distinguish data security issues brought under section 24 from the breach of consent under section 13.

The FTC case of Vision I Properties is among the few instances that actions under Section 5 have been triggered against the platform providers acting as intermediary for the merchants. A contrasting rationale between the FTC and the PDPC is seen in this case where the retail merchants who used the cart services of Vision I Properties to process consumer payments

152 In the FTC matter of Vision I Properties, LLC, et al., File No. 042 3068
153 PDPC decision re: Social Metric Pte Ltd, DP-160-4712; DP-1604-4713; 27 November 2017
were not enforced by the FTC, and even received the protection from the unfair basis under Section 5 enforcement.

Overall, the PDPC’s interpretation establishes the delegation structure and distributive mechanism of liabilities among business actors performing different roles in data processing businesses. The absence of a similar formal structure and mechanism under the FTC approach raises uncertainty as to the choice made by the agency to accuse unfairly of some actors with unreasonable data security practices. The analysis of these selected cases from both agencies puts forward that the PDPC’s mechanism provides incentives for a party acting as an organization and data intermediary to cooperate in protecting personal data. Implications for cooperativeness are to be discussed in the end of this chapter.

a. Summary of Facts and Findings

The facts and findings in the FTC matter Re: Vision I appear to be similar to the PDPC decision in Re: Social Matric in many aspects: (i) they both carried out the collection of information from individual consumers as part of a service provided to the merchant clients; (ii) they were later found by the agencies to act beyond the agreed scope and purposes of service agreements in exploiting individual personal data.

The differences lie in the fact that Social Metric did not intentionally abuse personal data by retaining them longer than necessary on a website, but Vision I Properties intentionally rented out personal data to the marketing companies.

b. The analysis

(i) Divergence in Distributive Liability Mechanism for Business Actors of Different Capacities

Who is accountable for breach?

In the case of Vision I Properties, the FTC sought unfair contract as a basis for determining unreasonable data security practices of Vision I Properties. It found that the inadequacy and conflicts of information provided under the terms of the cart service agreements entered between Vision I—a cart service provider—and retail merchants—its end users of the licensed software, constitute an unfair act and unreasonable practices under Section 5 of the FTC Act. From the FTC’s view, merchant customers of Vision I Properties were unfairly treated under the ambiguous contract and the reselling data practices of Vision I under Section 5. Thus, it appears that personal information of individual purchaser only receives indirect protection from this interpretation of the FTC. This FTC did not mentioned further as to why it did not exercise authority under section 5 against these retail merchants for broken promises against individual purchasers on their data security given under the privacy statements or the failure to ensure reasonable security practices of Vision I to their consumer data.

In Re: Social Metric, the PDPC implies that it would be unfair to hold the merchants liable under Section 24 and 25 because the discontinued relationship with individuals at the time of the breach. To illustrate that, the PDPC distinguished between two situations: first when the platform provider acted as a data intermediary for other businesses; second, when it acts in its own capacity as an organization under the PDPA. Such distinction is significant for PDPC in
determining obligations and liabilities assigned to a party under Section 24 and 25. The PDPC’s assessment found that Social Metric, at the point of collection of personal data carried out on the behalf of its clients for the marketing campaigns, therefore acted as a de facto data intermediary for its clients. The act of Social Metric in posting individual personal data of its clients on the website was likewise conducted in the capacity of a data intermediary.\(^{154}\) However, the PDPC found that Social Metric acted in its own capacity as Organization regarding the retention and disclosure of personal data posted on the website after the marketing campaign ended. Such data retention was a longer time period than was reasonable, and that Social Metric could no longer be considered a data intermediary in relation to such activities. The PDPC provided that: “Had the period of retention been shorter, and Social Metric stayed as a data intermediary.”\(^{155}\)

For the organization that hired Social Metric for a marketing campaign, the Commissioner further clarified that: In the premises, it would not be logical nor fair if the PDPA imposes a continuing obligation on Social Metric’s clients. Since Social Metric had failed to carry out what it was supposed to do, that is, the disposal of the personal data after the marketing campaigns, it bears the risk for whatever happens to the personal data that was held in its hands after the marketing campaigns were over. This highlights the point when the organization’s liability under section 24 ceases. The data intermediary turns into Organization itself and have a principal responsibility on safeguarding personal data at the point when it deviates from the original purpose of the assignment or the scope of duties under the contract.\(^{156}\) In the author’s view, the PDPC’s interpretation here reminds the nature of a principal-agent relationship, where the principal’s liabilities for its agent’s actions apply only when such acts are performed within the scope of the assigned duty, and not against the principal’s interest.

Put into analysis with Re: Social Metric, the case of Vision I Properties would lead to a different outcome if it appeared before the PDPC. The agency would consider Vision I Properties as acting as a data intermediary on behalf of merchants regarding its processing of personal data before 2003, and then later turning to act for itself after 2003 with regard to the rent of personal data for its own profit. Applied with the PDPC’s rationale from the case of Social Metric, Vision I Properties shall take full responsibility for the intentional misuse of personal data, which breached the individual consumers’ consent. The retail merchants in Vision I, however, shall not be relieved from the obligations and liabilities to ensure reasonable data security practices during their continued using of cart services from Vision I in order to facilitate their individual purchasers. That means that the PDPC would hold these merchants for their failure to ensure Vision I Properties’ proper treatment of personal data for the practice before 2003, in addition to holding Vision I Properties itself as an organization for intentionally breaching individual consent for the practice after 2003.

**What is the relationship between Merchant and Platform Provider and Duty arising therefrom?**

Secondly, despite section 5 of the FTC Act being silent on the specific relationship and duties between the platform provider and the retailer, as is the case of Vision I Properties, the FTC settlement order provided a glimpse of duties similar to those of the PDPC’s interpretations on the organization and its data intermediary. These duties are the contractual arrangements between the parties to ensure that adequate safeguard measures have been put in place, as well as

\(^{154}\) PDPC decision, Re: Social Metric, para.17.

\(^{155}\) PDPC decision, Re: Social Metric, para. 26.

\(^{156}\) PDPC decision, Re: Social Metric, para. 18, 24.
the platform provider’s duty to provide advice to its merchants about the treatment of individual consumer data.

Conclusion. The cases of Vision I Properties and Social Metric demonstrate the FTC’s lack of a formal venue established for delegating obligations and distributing liabilities among business actors of different roles in the data processing business. This gives a contrasting picture to the PDPC’s interpretation, which enhances the delegation system and distributive mechanism embedded into the design of the PDPA. These system and mechanism contours the area of shared and separated responsibilities in the principal-agent-like relationship between an organization and its data intermediary, and underlines that the organization are principal actor in protection of individual personal data. As in the case of Social Metric, the obligations and liabilities carried by the business party acting as an organization ceased, and were completely transferred to its platform provider to take on the full risks involved in safeguarding personal data.

As will be discussed in the end of this chapter, the analysis puts forward the implications for cooperative attitudes between business actors arising from the Singaporean approach to data security, which are absent in the U.S. approach. The Singapore’s platform casts an organization actor to play a principal role with direct responsibility for protecting individual trust by governing its data intermediary’s practices. With a clear limit on its responsibility set by the PDPC’s interpretation, this prevents organization actors from endless liabilities on personal data, even when they have already taken due efforts in safeguard personal data whilst in their control. At the same time, the PDPC ensures that the safeguard obligations will be transferred in a fair and seamless manner to another party who is in better control of data, and therefore should be accountable for the breach. The FTC’s unspecified scope and duty between these actors fails to provide reassurance in the above respects to all the parties involved as to when they will fulfil the safeguard obligations under section 5 of the FTC Act.

(ii) The Cases of a Platform Acting on its Own Behalf: Data Reseller and Brokerage Services

a. Cases of Data Resellers and Inadvertent Breach: The FTC Matter Concerning Fajilan and Associates, ACRAnet, Inc. and SettlementOne Credit Corporation

i. Summary of Facts and Findings

In matters concerning security breach incidents involving data broker companies, Fajilan and Associates, ACRAnet, Inc. and SettlementOne Credit Corporation, the FTC had imposed downstream obligations on these data broker companies to ensure that their clients had adequate data security systems in place to protect personal data. These companies were not only found to be in violation of the FCRA by furnishing consumer reports to persons without permissible purposes, but also the FTC further found that the disclosure of hundreds of consumer reports to hackers were due to the companies’ failures. These included: failure to implement data security policy for itself as well as its end user clients; failure to properly assess risks and to implement

---

reasonable steps to address those risks i.e. evaluation of the security practices of its clients and the provision of training to end user clients; failure to monitor their clients’ use of consumer reports, detect suspicious activities, or take appropriate action to correct existing vulnerabilities from the known risks. It followed from these cases that the FTC issued statements, which threatened to impose monetary penalties for future violations of the rules by data broker companies, as empowered under the FCRA.

ii. The Analysis

The PDPC has not yet rendered the decisions on a similar situation of inadvertent data breach of a data broker due to its failure to properly verify the users with whom they share individual personal data. However, if the cases of Fajilan and Associates, ACRAnet, Inc. and SettlementOne Credit Corporation appeared before the PDPC, the result would be different. The Commission would find the data brokers not as a data intermediary but acting on its own behalf as an Organization under the PDPA. The users of platforms who are business clients would also be considered as Organizations under the PDPA, who are obliged to provide reasonable safeguard to personal data in their possession. From thereon, the clients whose systems were hacked will breach their obligations under section 24 if they did not provide adequate data security protection of personal data. The disclosures of the personal data to an unauthorized party by the data platforms due to failure to provide a proper screening procedure would also trigger the platforms’ liability under section 24.

The relationship and duties between an organization and another organization, unlike between an organization and a data intermediary, have not been specified in the PDPA or the PDPC interpretation. Contrasting this with the FTC’s downstream liability in the cases at issue, the FTC seems to assume more onerous duty and liability for data platforms, which are, to ensure proper and adequate safeguards of their ordinary business end-users regarding personal data, and also to be deemed liable for the weaknesses of these end-users’ data security systems that have led to the attacks from malicious actors.

This brings another contrasting point between the FTC and the PDPC enforcement against data brokers. The upstream data broker businesses would fall under the definition of an “Organization” which has obligations on safeguarding personal data under the PDPA. Those companies, however, are not within the range of the FTC, whose focus is at the end of the stream with the points of contact with end-user, either it be the business or individual. This means that the upper stream platforms who share the data with the data broker companies will not be triggered under the FTC section 5, but can still fail additional safeguard obligations under FCRA or GLBA.

b. Cases of Data and Debt Brokerage: Intentional Misuse of Personal Data

This part discusses cases of intentional misuse of personal data by business parties whose main purposes are to make profits from the rent and sales of these data to third parties. The FTC cases concern debt brokers posting unmasked individual debt portfolios on their websites, Re: Bayview Solutions and Re: Cornerstone,158 which were accessible by the public. In Singapore, the first case that came before the PDPC concerns an individual data broker reselling personal data to third parties without the individuals’ consent.159

159 PDPC decision re: individual data broker, [2018] SGPDPC1 Case No DP-1701-B0485
i. **Summary of Facts and Findings**

The facts and findings in the FTC matters against Bayview Solutions and Cornerstone appear to be similar to the PDPC re: Individual Data Broker in many aspects: (i) all are data brokers selling information of individual consumers for profits; (ii) individuals were unlikely learned about the data in the respondents' possession; and all involved in intentional disclosure of sensitive personal data of individuals without authorization.

The differences are of the following facts: Bayview Solutions and Cornerstone disclosed consumer debt portfolios by posting them on the public accessible website containing the unencrypted, unmasked, sensitive personal information of more than 28,000 consumers viewed at least 340 times (in Bayview) and 190 times (for Cornerstone). An individual data broker obtained over 30,000 individual profiles including sensitive data including the NRIC number and annual income range to her customers.

ii. **The analysis**

(i) **Use of Intent as Basis for Determining Issues under Security and Privacy Breach**

In alleging unfair acts against Bayview Solution and Cornerstone and Company, the FTC did not distinguish as to whether the alleged acts of these debt brokers were characterized under data security or privacy breach. Although the FTC mentioned that the invasion of privacy is among the consequences from the unfair acts of disclosing “extremely sensitive consumer personal information” publicly, which the consumers were unlikely to know about or give consent to do so. The FTC also found that the defendants had not adequately sought out available alternative means to secure sensitive data, by redacting, encrypting the information, password-protecting the information, or by a means other than a website.

Similar fact found in the PDPC re: individual data broker was clearly characterized as the issue of the consent breach under Section 13 and 20, not the issue on data security protection Section 24. The latter would be a matter involved inadvertent disclosure of personal data. This same basis affirms the PDPC earlier decisions on re: Social Metric and re: Lifelock.

The PDPC also found the guilty conscience of the individuals by trading personal data under her alias and her “premeditated and deliberate” action in violating the PDPA as factors considered for the aggravated penalties imposed to the individual data broker.

Such divergence on the FTC and PDPC on the intent basis was again emphasized in these cases. The intent made no difference under the unfair and deceptive practices of section 5 of the FTC Act, whereas it serves several functions in the PDPC assessment in determining under which provisions the issue will be considered, and distinguishing between an act on behalf of another or an act of one’s own. The intentional breach also found the PDPC’s criteria for aggravating penalties imposed on the organizations.

---

160 FTC complaint for Permanent Injunction and Other Equitable Relief, No.14-cv-01830 (filed on October 31, 2014), para. 25-26. “The consumers whose sensitive personal information and purported debts Defendants have revealed would be unlikely to know that Defendants possess, and are openly disclosing, their information. They therefore cannot protect themselves from the harms and potential harms the disclosures cause, including possible identity theft and concomitant account fraud, invasion of privacy, and job loss.” and “Defendants’ practices also expose consumers to other persons or entities attempting to collect the purported debt unlawfully, even though those entities will not have purchased or acquired the authority to collect the debt. This harms consumers who may end up paying money, but not receiving an enforceable discharge of the debt or any benefit on their credit report from paying the debt. And, it harms debt collectors who may later legitimately purchase those same debts, by making their collection efforts more difficult or impossible.”

161 PDPC decision re: individual data broker, para. 32(b).
(ii) **Business Activity versus Non-Business Activity: Scope of Application**

Under the PDPA, “business” includes an activity of any organization, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his personal or domestic capacity.\(^{162}\) Therefore, regardless of the intent on making profit from such personal data, an individual when acting outside of his/her domestic use of personal data shall be regarded as an “organization” and therefore have obligations to comply with the PDPA. The PDPC considered that acts of an individual data broker in her purchases and sales of the leads were not for personal use or purpose, but business activities.\(^{163}\) This brings a contrasting point to the scope of Section 5 of the FTC Act that places the limits to the acts relating to commerce.

(iii) **Data security issues under an Individual Data Broker: Would it more like a debt portfolio case or the case of data brokers that fail to take care of their client’s computer system leading to security attacks?**

The case of the Singaporean individual data broker is more similar to the FTC’s debt portfolio broker cases where the business actors intentionally misused the personal data without individual consent. The act of the U.S. debt brokers sounds more outrageous because the extremely sensitive information was accessible by any visitors before it was taken down from the website. Compared to the individual broker case, information was sold privately to certain third parties. Still, the FTC disregarded the intent for breach of these debt brokers, but rather looked upon their acts as unfair practices on security protection, which led to the subsequent privacy breach.

If in fact it appeared that the individual data broker case before the PDPC had obtained the consents from individuals pertaining to the resale of such data to third parties, her case would get closer to the FTC cases of Fajilan and Associates, ACRAnet and SettlementOne Credit, those were obliged to screen users with whom they shared information, and to provide secured means of sharing as part of the security protection obligations. Such a screening process was raised in the other PDPC’s decision in the case of the individual consultant who improperly disposed of personal data.\(^{164}\)

In this PDPC individual data broker case, the fact does not present whether this individual broker had safeguard measures in place at the time of the breach. In absence of such a fact, it is not clear whether the PDPC would consider that she also needed to safeguard data in her possession as well as that with whom she shared those data, as found by FTC in the cases of Fajilan and Associates, ACRAnet and SettlementOne Credit.

(iv) **Privacy Harm**

Both agencies raised different harmful aspects of the respondents’ conducts. The FTC in alleging unfair data security practices against Bayview Solution and Cornerstone raised the potential harms accompanying the consumers, whose sensitive data were unaware of the disclosure, including possible identity theft and fraud, invasion of privacy, and job loss, unlawful debt collection. The FTC further raised the consequential economic loss possibly incurred by the consumers and their legitimate debtors, who may end up not being able to collect the debt when the consumers paid out to the illegitimate debtors.

\(^{162}\) PDPC decision re: individual data broker, para. 10.
\(^{163}\) PDPC decision re: individual data broker, para. 9-11.
The PDPC in assessing the breach, stressed the impact on the exploitation of individuals in making profit from sales of personal data, “the very kind of activities which the PDPC seeks to curb, and hence, must be severely dealt with”. In this case of an individual telemarketer selling data, it emphasized on the needs to protect individual interests and safeguard against any harm to the individual, such as identity theft or nuisance calls. The PDPC called for a strong policy against unauthorized selling of personal data.

From this, both the FTC and PDPC considered identity theft as possible harms from the unauthorized disclosure of personal data. However, it is noted that the FTC in addition to the criminal conducts also raised economic impacts to individuals. What the FTC means by the “invasion of privacy” is unclear whether it refers to the information disclosure itself, but the PDPC clearly considered the nuisance calls as harm. This provides implications on the differences of aspects of privacy harms concerned by the FTC. While it is necessary for the FTC in substantiating the unfairness claim, such harm is not necessary for the PDPC compliance-based rule to prove in finding the individual data broker in breach of consent.

(c) Mitigating factors: Personal Hardship of the Respondents

In applying mitigated penalties for the individual data broker, the PDPC considers the fact that she had candidly admitted to the wrongdoing at the first instance and fully cooperated by providing helpful evidence during the investigation. Along with other criteria, the PDPC considered such the financial hardship of the individual data broker and her family in adjusting the fine to S$6000 in reflecting the seriousness of the breach. This further implies the PDPC’s consideration of the status and nature of organization in arriving at certain amount of penalties. Similar criteria are not mentioned by the FTC except in the mandate written security requirement program, which mentioned the level of safeguard corresponding to the nature of respondent’s business.

Part III: The Intersections, Diffusions and Overlaps of the FTC and the PDPC’s Interpretation

The cases analysis in this Chapter demonstrates the intersections, diffusions and overlaps of the FTC and the PDPC’s implementations under Section 5 of the FTC Act and Section 24 of the PDPA as follows.

A. Basis for Reasonableness Standard

There are convergences in the FTC and PDPC’s implementations of reasonableness standards under the FTC section 5 and the PDPA section 24 as to the extent and the level of reasonableness standard applying to business actors. That is, reasonable data security practice does not mean a complete and absolute protection from data breach, but instead implies due effort in providing physical, technical and administrative measures to prevent such security breach from occurring. Examples of reasonable measures illustrated by the FTC and the PDPC through cases includes the readily available tools for prevention of well-known security threats, encryption and the implementing internal policy and procedures for employees.

165 PDPC decision re: individual data broker, para. 33.
166 PDPC decision re: individual data broker, para. 30.
167 PDPC decision re: individual data broker, para 34.
B. Intent as a Basis for Determining Issues and Scope of Application

There are some divergences as to how the actor’s intent involved in a breach is considered by the FTC and PDPC. As discussed in the cases of outsider breach and cases related to platform providers, the intent serves at least three different consideration for the PDPC: first, determining whether the issue falls for the breach of individual consent or data security breach, in which different provisions apply; second, whether the companies involved in the breach acting as an Organization or Data Intermediary; third, how the mitigating and aggravating penalties will be determined. Intent involved in the breach is less significant for the FTC in its assessment of either security or privacy breaches. Both issues have been considered on the similar grounds of unfair and deceptive practices jeopardizing consumer choices. Clear divergence is evident in the cases of data and debt brokerage that involved intentional misuse of personal data by the respondents. The PDPC would find the issue a breach involving individual consent, while the FTC would raise the issue of inadequate data security protection.

Such divergence therefore highlights agencies’ views that give rise to diffused meanings, breadth and depth of aspects of protection on privacy and security basis, to be discussed further.

C. Scope of Application to Commercial and Non-Commercial, Business and Non-Business Activity

There is diffusion as to the scope of applications to non-commercial related activities. The PDPC cases of an insider leak and cases of data and debt brokerage demonstrate that the personal data treated by a non-profit debt counselor also receive protection under the PDPA. An individual acting on business purposes is also considered as Organization, subject to the same obligations as companies under the PDPA. As for the FTC application of Section 5, non-commercial activities provided by a non-profit organization have been carved out from the scope of Section 5.

Such distinction due to the scope of Section 5 and Section 24 implies the diffused grounds for protection of personal data and its values arising from such protection. The FTC anchors on the commercially related nature of the activities and the effect on the market mechanism, while the PDPC recognizes broader grounds for protection beyond market-related aspects to cover social dimension.

D. Aspects of Harm and Injury: Reputation, Embarrassment, Trust

There are diffusions in the aspects of harm and injury recognized and protected by both agencies in the cases of insider leakage involved in sensitive financial and health-related consumer data.

In those insider leak cases, the PDPC also considered aggravating impacts of a data breach incident on the general public trust on the national credit system. This illuminates the PDPA objectives in protecting individual trust in data processing businesses. Similarly, the Director of the Consumer Protection Bureau then referred to the serious breach of consumer trust from the Lilly incidents in terms of broken promises, which the company exchanged with its consumers to protect personal data. Such statement, however, does not link the broken promises and the breach of consumer trust with the effects on individual reputation, stigma or embarrassment from the incident.

Furthermore, both agencies provide divergent reflections on a breach of trust. The PDPC reflects on the real impact on the individual trust and the nation-wide public trust, while the FTC
restricts the interpretation of section 5 to cognizable harm and injury framed by the market definition. That refers only what hurts the market mechanics on information transparency and consumer choice. Breach of trust under the FTC is therefore a breach of trust in the ideal market mechanism.

E. Criteria: Post-Breach Behavior

From the cases of outsider and insider breach, both agencies have divergent approaches in recognizing trustful behavior provided by the respondents to affected consumers. For the PDPC, recognizing these activities, i.e. an apology, admittance of breach, corrective and remedial actions and their prompt responses, and consideration of them as mitigating and aggravating criteria, do serve several functions on providing incentives for trustful behavior of organizations and a venue for correcting prior untrustworthy acts. The cooperation and responsiveness of the breaching organization with the agency are also considered by the PDPC among other criteria, underlying the cooperative attitudes with the authorities. For the FTC, despite similar trustful behavior of organizational responses having been found, these were not recognized or considered as factors in determining breach and order given to the alleged organization. Such divergence therefore implies how differently the agencies embrace trust and cooperation as part of their strategies in enforcement and encouragement beyond compliance behavior, the details of which will be discussed in Chapter 4.

F. Actors and Accountability for Breach

Both agencies have amplified such discrepancies laid by the designs of section 5 of the FTC Act and the PDPA in their implementations. The PDPC’s interpretation streamlines the delegation structure and the distributive liabilities purported by the PDPA. It further improvised a clear distinction between Organization-Data Intermediary characters and the scope of duties and liabilities whilst also ensuring that there remains a mutual interest for them to cooperate and to avoid being investigated by the PDPC.

The FTC’s approach in the case of a platform provider demonstrates that the FTC does not seek to distribute liabilities among business actors by not drawing distinctions of role and relationship between business actors involved in data processing businesses. Therefore, the application of section 5 to a data intermediary in the case of Vision I Properties resulted in the surprising outcome, notably that the merchants, as end-users, also received protection from the unfair act of its data intermediary’s service, and therefore, could not be held accountable for broken promises made to the individual consumer on the security of personal data shared with these merchants through the platform when purchasing products.

The cases of data resellers also demonstrate the limits of the venue constructed by Section 5 to engage the upper stream players to be accountable for the security breach which occurred at the end of the stream. Therefore, the FCRA and GLBA come into play in regulating the financial-related actors in the upper stream to adopt specific safeguarding procedures. Nonetheless, the cases of data resellers illustrate how section 5, when applying to the data platform provider and the business end-users, has created onerous duties for these platforms on reviewing and providing advice on security arrangements to their business clients. This construction of venues for data reseller platform and their relationships by the FTC has been done from a different axis than in the PDPC’s construction. The FTC assumes that business-end users are in the weaker position as compared to the platform provider, so received protection from the unfair acts. The PDPC, however, would deem that both platform provider and the end-
users would each act on their own behalf in profit making from such data shared between them. Therefore, both would equally be separately accountable for inadequate security protection as an Organization, which is not the case of a data intermediary-organization relationship.

**IV. Implications for Individual-Organization Trust Relationship and Cooperation among Businesses from the Enforcement Cases**

The different approaches and mechanisms adopted by the U.S. and Singapore agencies regarding data security breaches provide implications for platforms, actors’ attitudes and forces that altogether form an environment for trust relationship, cooperation and organizational beyond-compliance behaviors. In chapter 2, this divergent approach has been illustrated from legal designs that assign different roles and attitudes to each actor and relationships among them based in the principle levels. That is, the Singaporean legal design serves the ends of promoting trust relationship and cooperation to emerge among players by embracing interdependent relationships, nurtures trust and cooperative attitudes. The U.S. fragmented has not supported those of which but autonomous basis of self-reliance. The findings in this chapter affirm these disparate views as the agencies’ implementations of laws have continued to diverge on the ground.

*Reflection of the principle of care, prudent business and the relationship in data security practices*

The PDPC’s interpretation of reasonable data security practices under Section 24 clearly amplifies the principles of care and the due diligence of businesses in safeguarding individual personal data under the Personal Data Protection Act. The Commission encourages individuals to rely on a prudent organization party who plays principal role on the basis of the ongoing relationship and interests on personal data pertaining to individuals. From the case analysis, I found this ongoing basis of relationship interests highlighted by PDPA decisions in three aspects.

First, such ongoing interest and relationship an organization has with individuals provide the basis for the full obligation and principal liabilities in employing reasonable measures to prevent unauthorized disclosure of personal data. Even when a data intermediary is appointed to handle personal data, organization still has the liabilities if it fails to provide adequate security arrangements, which includes supervising its data intermediary to fulfill the obligations. (Re: Orchard Turn)

Second, despite the PDPA being silent on the organization’s duty regarding post-breach responses, how an organization party delivers desirable post-breach responses towards individuals are taken into account by the PDPC for issuing the direction and penalty for the organization party. Similar criteria for mitigating and aggravating penalties for the prompt breach notification, the corrective and remedial acts towards individuals do not apply to the data intermediary who plays a secondary role to safeguarding personal data. (Re: Orchard)

Third, when such organization’s interest and relationship with individuals cease, as is the end of merchant’s campaign in re: Social Metric, such obligations and liabilities under Section 24 had been transferred from the organization party to the data processor who later acts for their own purposes and became more relevant in such processing of personal data.
From these three aspects observable from the selected cases, I put forward that the PDPC further promotes trust in the organization-individual relationships, reflecting the legal design of the PDPA. By assuring organizations with a more favorable condition of direction and penalties from breach due to the presence of these desirable post-breach responses, the commission reduces risks inherited in these trustful acts of prompt breach notification and remedies towards individuals. Chapter 4 investigates into the types and patterns of post-breach responses from the organizations found in the data security breach cases, and the interview excerpt that clarifies the drive behind these beyond complaint organizational behaviors.

Care principles, prudent businesses and relationship aspects have not similarly addressed by the FTC. The fair information practices resonates with the FTC’s interpretation of unfair and deceptive security practices under Section 5, which has put forward the more objectively protection of market mechanism, i.e. empowering consumer choices through the truthful disclosure of products and services. Market, rather than individual relationship, defines objective interests of privacy that should receive protection. The selected FTC cases did not demonstrate that the relationship with consumer informs the agency’s choice of enforcements or more onerous duty supplied from such basis. Despite some post-breach behaviors appears in re:Twitter and re:Lilly which notified breach incidents to their customers, they did not have much significance to the FTC decisions. Next chapter will investigate the implications for these behaviors as seen in other FTC’s decision regarding data security.

How both agencies’ recognition of these behaviors correlates to the norms on post-breach notification, correction and remedies towards the affected individuals by organizations? Would individual-organization trust relationship be a factor that drives these organizational responses in remedying the breach privacy and gain trust thereafter? These questions will be further examined in chapter 4 with more evidence from the ground.

**Reflection on the Cooperation among Data Processing Businesses**

Both agencies have applied different basis and strategies to pursue claims against business actors involved in the unauthorized disclosure of personal data, as discussed comparatively in the FTC case of Vision I and the PDPC case of Social Metric. In these cases, with much uncertainty remaining from the FTC approach, the clear boundary and the delegation of liabilities between the principal actor and data intermediary have been clarified throughout the PDPC interpretation. As a result, the principal-agent like relationship and liabilities in safeguarding individual data found on the PDPC decisions does not apply to the cases before the FTC enforcement. In the selected FTC cases, the role of merchants which are supposed to be at the front line regarding protecting personal data under the PDPC were replaced by the platform actors who also have further implied obligations to advise the merchants on the reasonable data security practices. The platform actors are more prone to the FTC enforcement rather than the merchants who purchases these products, as seen in the FTC matter re: SettlementOne and re: Vision I.
Case Summary

The PDPC Decision re: Orchard Turn Developments Pte. Ltd. (DP-1512-A612; 6 July 2017)

In the case of Orchard Turn Developments Pte., (Orchard Turn), on 26 December 2015, an intruder had obtained administrative account credentials and gained unauthorized access to the Electronic Direct Mailer (EDM) application on the server used by Orchard Turn for sending out email updates to subscribers. The attacker then sent a blast phishing email that looked like an Ion program update from Orchard Turn to 24,913 subscribers. The link directed the subscriber to the store’s point rewards advertisement page that when clicked further asked subscribers to fill in personal data such as an email address and telephone number for enrolling in the rewards.

Super-E is the service provider for Orchard Turn, based in Hong Kong, at the time of breach incident. It managed the IT system and database stored in the EDM server of Orchard, which comprised of a personal data set of a subscriber’s name, email address, birthdate, and membership registration date. In a day after the breach occurred, Super-E received an alert from the EDM server and discovered that an Internet Protocol address from Egypt had successfully logged into the system and had sent out the phishing email to the Organisation’s subscribers. After discovering the data breach, Super-E disabled the EDM server to prevent further dispatches of phishing emails to the Organization’s subscribers. On 27 and 29 December 2015, the Organization sent emails to the affected subscribers informing them of the phishing email that had been sent out.

The Commission held that Orchard Turn had failed to implement reasonable data security measures to safeguard personal data from two key practices: (i) The daily automatic transfer of personal data stored from the other server to the breached EDM server which connected to the internet, together with the permanent and unnecessary retention of data on the EDM server adding more significant security risks. (para. 15). (ii) the lax safeguard on password policy and practice evidenced by the attacker’s success in his single attempt. (para. 23). In particular, the organization did not prohibit password sharing among admin accounts or require periodic password changes. (para. 24). The same EDM admin password had been used for a year before the incident and was shared between four admin employees, making it difficult to pinpoint the cause of leakage. The organization therefore did not make reasonable efforts to ensure the safeguard of the personal data set by reasonably anticipating, identifying and rectifying the technical security vulnerabilities at an early stage.

On the significant risks, the PDPC suggests that: the fact that the server was accessible from the Internet made it more susceptible to online attacks and external threats, and it was therefore more likely to be compromised. (para. 16). Second, the longer the personal data set was left on the EDM server, the more exposed it was to online attacks and external threats. (para. 17). In the final analysis, it was not prudent for the Organization to keep a duplicate or additional set of personal data on the EDM server for a period longer than necessary. (para. 20).

168 The purpose of case summary is to provide a background for the comparative analysis made in this chapter, not an interpretation of cases or for reference.
After the breach, the Organization purged all the personal data residing on the EDM server and subsequently put in place a purge policy whereby the personal data set on the EDM server will be removed after a standard period of 14 days. (para. 40).

The PDPC found the Organization did not reasonably implement data security arrangements and was in breach of section 24. The penalty of S$15,000 was issued together with the direction. It took into account (a) the large amount of personal data involved, (b) the exposure to further risks and other exploits by the phishing email, (c) the Organization did not make reasonable efforts to put in place proper measures at an earlier stage, (d) the Organization was generally cooperative and forthcoming in providing timely responses to the Commission during the investigation, and (e) the Organization took prompt remedial action after being alerted to the data breach incident, as well as other corrective measures to improve its IT security.

The FTC Matter Concerning Twitter, Inc. FTC file No. 092 3093

The FTC alleged that in the case of Twitter, the deceptive claims under Section 5 were based on two accounts: first, Twitter did not use reasonable and appropriate security measures to prevent unauthorized access to non-public user information; second, Twitter did not use reasonable and appropriate security measures to honor the privacy choices exercised by users.

The Incidents. Between January and May 2009, there were two incidents, in which intruders accessed Twitter’s user accounts without authorization. In January 2009, an intruder used password guessing tool to obtain admin credentials and later accessed non-public information of Twitter user accounts, and tweeted from their accounts. Some reset passwords were posted on the website accessible by the public.

In April 2009, an intruder compromised an employee’s personal email account, and was able to identify the employee’s Twitter administrative password based on two similar passwords stored in the email account in plain text for at least six months prior to the attack. Using this password, the intruder could access non-public user information and non-public tweets for any Twitter user. In addition, the intruder could and did reset at least one user’s password.

User’s Non-Public Personal Information. In addition to a user’s public profile and tweets, Twitter also collects certain information about its users that it does not make public. Such information includes: an email address, IP addresses, mobile carrier or mobile telephone number, and a user’s blocked account. This non-public information can be viewed by the user who operates the account.

Employee accessibility and control of user’s nonpublic information. From approximately July 2006 until July 2009, almost all of its employees had the ability to access and exercise administrative control of the Twitter system, including the ability to reset a user’s account password, view a user’s non-public tweets and other non-public user information, and send tweets on behalf of a user. (para. 7). From approximately July 2006 until January 2009, Twitter’s employees accessed the control through the public login page at twitter.com by entering their administrative credentials. (para. 8). From approximately July 2006 until July 2008, its employees were able to use their personal email accounts for working on company business.

---

170 Full decision available at https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation
Failure to Provide Reasonable and Appropriate Security. Twitter’s measures, taken together, failed to prevent unauthorized administrative control of the Twitter system. Among others, it failed to (a) implement sufficient administrative password policy on using hard-to-guess password instead of common dictionary words or similar ones to those for accessing websites; (b) prohibit storage of passwords on personal email accounts in plain text; (c) disable admin passwords after numbers of unsuccessful attempts to log in; (d) provide separate non-public login pages for employees; (e) enforce regular password changes i.e. every 90 days; (f) limit employee’s access to non-public user information based on their needs in performing their jobs; (g) restrict administrative access by other means such as granting access to specified IP addresses.

FTC Settlement Order. Twitter shall comply with the MWPS Program, where violation would result in fine of $16,000. No penalty was issued.

The FTC Matter Concerning Eli Lilly and company (FTC file no. 0123214, Docket No. C-4047)\footnote{Full case materials available at https://www.ftc.gov/enforcement/cases-proceedings/012-3214/eli-lilly-company-matter}

In the FTC matter concerning Eli Lilly and Company (Lilly case), (the drug manufacturer operating through websites of Prozac.com and lilly.com), the disclosures on June 27, 2001 were due to an employee’s email message sent to individual subscribers of Medi-messenger service, an automatic email reminder service for medication refill, announcing the end of the service. The email included all 669 recipients’ email addresses within the “To:” line of message, which in turn, unintentionally disclosed each individual subscriber’s email-address to other subscribers in the mailing list.\footnote{The FTC re: Lilly, Complaint. Available at https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elililycmp.htm}

The FTC’s complaint alleged that the cause of data breach was a result of the company’s failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information. It failed to provide appropriate training for employee’s privacy and information security practice. It failed to have appropriate oversight and assistance for an employee who was new to the program used for the sending out of emails. It failed to implement appropriate checks and controls on the process, such as a review by experienced personnel and the internal pretesting of a program before sending out an email. Its failure also violated its written security procedures represented to protect consumer privacy and confidentiality of personal information collected from or about consumers.

Therefore, the FTC settlement orders prohibited further misrepresentations of Eli Lilly regarding its maintenance and protection of privacy and confidentiality of any personal information collected from or about consumers in addition to the MWPS program\footnote{The FTC re: Lilly, Decision and Order. Available at https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillydo.htm}. There was no fine.

Re: Credit Counselling Singapore; DP-1610-B0261; 29 December 2017.

Credit Counselling Singapore (CCS) is a registered charity aiding debt-distressed individual clients, such as credit counselling and facilitating the establishment of a debt-restructuring plan with creditors. The data breach was caused from the massive follow-up email sent by one of

\footnote{The FTC re: Lilly, Decision and Order. Available at https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillydo.htm}
CCS's admin staff to 96 individual clients in its debt management program (DMP), a voluntary debt repayment scheme. By inadvertently including email addresses of all individual participants in the “To” field rather than “BCC” field before being sent out, the mistake caused the 96 email addresses and associated names (for some individuals) to be visible in the “To” field to all the recipients of the follow-up email. In addition, the “Reply All” by two clients also inadvertently revealed the filled-out questionnaire including their personal data to all recipients. Thereafter, CCS received feedback from four clients who were concerned that their identities had been disclosed to the rest of the recipients.

The PDPC found the organization in breach of section 24, for it does not provide reasonable security arrangements for the personal data of clients. The CCS, Organization under the PDPA, did not have any checks or controls in place to ensure that email addresses are pasted correctly in the “bcc” field. (para. 30). As the leaked personal data at issue, including email addresses, was of a sensitive nature, therefore, a higher level of security protection is needed to be implemented. (para. 31). Regarding the nature of CCS’s work that “routinely handles large volumes of sensitive financial personal data of individuals”, the PDPC held that “it is foreseeable for CCS that there will be risks of inadvertent disclosure of sensitive personal data.”

The PDPC pointed out the availability of risk-mitigating tools, the mail-merge solution that CCS was then preparing to adopt, which could have prevented the breach incident if it had been in place sooner. (para. 33) The email addresses of clients constitute personal data because the CCS would also have the name of an individual to whom the email address belongs, and would thus be able to identify the individual from that email address. Some email addresses also revealed fully or partially the name of the individual, thus allowing an outsider to identify the individual. In addition, 16 individuals could be identified on online social media platforms based on a search of their email addresses. (para. 7-11)

The PDPC stressed that the nature and context of the follow-up email is crucial to its finding that the contact information was sensitive data in this case. It indicated that an individual on the list “is either currently facing financial debt, or was previously in debt, and that the individual is obtaining, or had previously obtained, assistance under the DMP scheme to pay off the debt.” (para. 11-12). It cited statements from the British Columbia Commissioner and Canadian Commissioner, respectively: “In my view, the fact that money was borrowed and is owed could, whether justified or not, lead to moral judgments about the individuals and their spending, financial choices, earning power or about their character generally. In particular, a lapse in, or lack of, payment to that party may be considered particularly sensitive information, given the stigma that may be attached to an individual having a delinquent debt.”; and, “the personal information involved could be used to cause harm to affected individuals in the form of financial loss, embarrassment and harassment by an unauthorized third-party debt collection agency. In my view, these are significant harms.” (para. 17-18). From this, the PDPC restated that: “Disclosure of an individual’s indebtedness to other third parties could lead to harm to the individual because it could result in social stigma, discrimination or a tarnished reputation. These are real possibilities that can affect a person’s life. Hence, the confidentiality of the individual’s financial information should not be treated lightly”. “[the] presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.” (para. 19).
The PDPC clarified the injury and actual harm of financial data and general loss of public trust in a larger credit system. In assessing the breach and determining directions, it considered para. 36 (a), that information about an individual’s adverse financial condition and/or state of indebtedness was sensitive personal data, and that the disclosure of which could cause actual or potential harm, injury or hardship to the individual, including serious reputational damage and embarrassment; and (b), given the nature of the Organization’s business of handling large volumes of sensitive personal data, the Organization ought to have put in place a system of checks for any sensitive personal data that may be disclosed, but did not do so; and (c), the data breach incident may cause members of the public to lose trust in such credit counselling organizations to safeguard their personal data, which may frustrate larger national credit management efforts.

The following mitigating factors are listed, namely: (a) the organisation had cooperated fully with the Commissioner’s investigations and had readily admitted its mistake without delay; (b) the Organisation had promptly notified all the affected recipients of the data breach incident and offered them an apology alongside a request to delete the follow-up email; (c) the Organisation had counselled the admin staff who made the mistake, and had taken further steps to prevent future data breaches such as its plan to conduct an organisation-wide refresher course on compliance with the PDPA, and the deployment of the “mail-merge” software, mentioned above, within two months; and (d) there were no other data breach incidents reported apart from this one. (para. 37)

The FTC Matter concerning Vision I Properties, LLC, et al., (File no. 042 3068)174

In the case of Vision I Properties, the company provides the online purchase checkout page and shopping cart services and licenses for thousands of small retailer merchants’ websites. The FTC alleged the company with unfair practices under section 5 when the company in 2003 started renting customer information for marketing companies. Consumer information obtained included the name, address, phone number, and purchase history of nearly one million consumers. A third party used such information for telemarketing calls and direct mailing to consumers. In this case, the FTC found that “the respondent did not adequately inform merchants in promoting its shopping cart software or at a later time that it intends to use information collected from merchant’s consumers in a manner that may be inconsistent with the merchant’s privacy policies, or that it intends to share information with third parties for marketing purposes.” Part of Vision I Properties’ statement provided that it retained full ownership of data collected from its customers. This statement was buried in the middle of an online agreement with merchants without further explanation of how its intended uses would be in conflict with the merchants’ policies. Vision I Properties ended up in a settlement agreement with the FTC. The order required the company to give up the fees of $9101 it made from renting consumer information as well as a further requirement to ensure that merchants’ customers or consumers receive a clear and conspicuous notice before their personal information is disclosed to others for marketing purposes.

The PDPC Decisions re: Social Metric Pte Ltd; Case No DP-160-A712; DP-1604-A713.175

174 Full case materials available at https://www.ftc.gov/enforcement/cases-proceedings/042-3068/vision-i-properties-llc-et-al-matter

175
In the matter concerning Social Metric, a digital marketing agency, the PDPC found it in breach of section 24 for failure to provide reasonable protection to personal data on its website. As a result, personal data of over 558 individuals contained in nine webpages were publicly accessible via an online search. This included individuals’ names, email addresses, contact numbers, employers, occupations, date and time of registration, and other information such as location to visit, activities, purpose of visit. The personal data contained on the websites were part of Social Metric’s marketing campaigns conducted for and on behalf of its clients which included creating webpages and social media.

Unreasonable Safeguard Measures. The Commissioner found that Social Metric had failed to limit access to the webpage. No security or access controls on the Website or on any of the Webpages, such as a password protection, were in place which allowed any website visitor to access such personal data. (para. 31). It also failed to take down the information after the marketing campaign ended. Social Metric argued that it was due to oversight or forgetfulness on its part that customers’ personal data was publicly accessible online, but the PDPC found these were not not valid excuses. (para. 34). Social Metric was first informed by the complainant of the unintended disclosure of personal data on the nine Webpages on 27 April 2016. Following the complaint made by the complainant to the PDPC, the PDPC had also informed Social Metric about the disclosure on the Webpages in May 2016, (para. 7), 2 months before completely taking them down. In Social Metric, the PDPC found it was liable for inadvertent unauthorized disclosure of personal data long after the campaign ended and in violation of data protection obligations under section 24 and 25 of the PDPA. It therefore imposed penalties amounting to S$18,000 on Social Metric and issued the direction to ensure that it ceased retention of personal data as a data intermediary of organization.

The FTC Matters re: Bayview Solutions LLC and re: Cornerstone and Company (FTC File No. 142 3226 and 142 32110)176

In the FTC matter against Bayview Solution and Cornerstone and Company, the defendants are debt brokers. They purchase and sell portfolios of charged-off consumer debt for eventual collection by third-party debt collectors. The debt broker companies posted consumer debt portfolios unmasked on their public accessible websites, which contained extremely sensitive information such as the amount of debt.

The website traffic revealed that more than 190 times and 340 times the public websites were accessed by visitors to Cornerstone and Bayview respectively. The FTC found these practices unfair public disclosure of consumer sensitive personal and financial information. Such disclosures posed potential harms of theft, fraud, invasion of privacy, and loss of job and unlawful debt collection. As a result, a federal court ordered the website hosting the sensitive information to take it down immediately. It also ordered the defendants to notify the affected consumers that their information had been exposed and advise them of steps they could take to protect themselves. In addition, the FTC ordered the refund of monies, and enforced the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law.

176 https://www.ftc.gov/enforcement/cases-proceedings/142-3226-x140062/bayview-solutions-llc
https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc
The PDPC Case re: Individual Data Broker; Case No DP-1701-B0485.177

This case is the first case before the PDPC relating to an individual data broker who sold personal data to third parties without authorization. The issue was brought under the breach of consent and notification obligation under Section 20 and 13 of the PDPA. The PDPC found a clear and serious breach of sections 13 and 20 for an unauthorized disclosure of personal data and unreasonable use under section 19. (para. 22-24).

The individual data broker purchased the list of personal data to boost her career in marketing. These so-called ‘leads’ generally comprised of an individual’s name, NRIC number, mobile number and annual income range. The purchase of leads was without the seller’s verification as to whether the individuals had given consent. (para. 4).

An Individual data broker had been involved in reselling data from late 2012, the period after the PDPA has been in effect, until 23 February 2017. The sale and purchase of data was on a large-scale basis, but as a side-line to her job as telemarketer. At the time of being discovered, she had in her possession approximately 30,990 leads stored in the spreadsheets and admitted to selling each for S$0.05 to S$0.20 per lead. She had advertised the sale of leads on various websites and received payment via a bank transfer by using a disguised name and another’s bank account and telephone number. The profit made from data reselling was estimated to be S$5,000.

In assessing breach and direction given, (para. 32), the PDPC found that: (a) the database of leads included personal data of a sensitive nature, i.e. NRIC numbers and salary ranges of individuals; and (b) “the guilty conscience of a premeditated and deliberate contravention of the PDPA” was indicated from her use of means to obscure her identity when she was selling the leads; and (c) the exploitation of individuals in making profit, the activities which PDPA intends to prohibit: “the profiteering from the sales of personal data by organisations at the expense of consumer or individuals is the very kind of activity which the PDPA seeks to curb, and hence, must be severely dealt with.” On balance, the PDPC’s mitigating factors, (para. 33), took into account: (a) the fact that the she had candidly admitted to the wrongdoing at the first instance; and (b) her full cooperation with investigations and helpfulness in providing evidence of the matter. In addition, the Commission considered personal financial hardship of the respondent and her family in adjusting the fine to S$6000 in reflecting the seriousness of the breach. (para. 34).

The PDPC emphasized a strong policy against unauthorized selling of personal data to others due to “the need to protect the interests of the individual and safeguard against any harm to the individual, such as identity theft or nuisance calls”. It also stressed “the need to prevent abuse by organizations in profiting from the sale of the individual’s personal data at the individual’s expense. Indeed, it is exactly these cases of potential misuse or abuse by organizations of an individual’s personal data which the PDPA seeks to safeguard against”. (para. 30).

In this case, the PDPC found the individual data broker acted as an organization under the PDPA, which is obliged to comply with its provisions. The Commission found that she did not act in a personal or domestic capacity, intending to make personal use of the leads, but to make a profit from the sale of personal data.

Chapter 4

Post-Breach Responses and Trust Relationship: Evidence from Cases and Interviews

Chapter Abstract

This chapter aims to explore what could be the drive behind these post-breach responses from organizational, with which law and enforcement can promote for better privacy. It examines the post-breach responses provided by organizations towards affected individuals found through the FTC and PDPC's data security breach cases and identifies the divergence found in these patterns in term of consistency and normative value recognized by both agencies, which implies the different emphasis given to this emerging beyond-complaint and trustful behaviors. The interview with data privacy professional in U.S. and Singapore reveals the shared organization’s perception on privacy in relation to trust, and how organization responses to data breach depend much on their relational trust with individuals. The alignment of Singapore legal ideal, enforcement to this existing function of trust relationship could explain the emergence of these desirable post-breach responses initiated voluntarily by organization respondents in cases, which enhances privacy protection. Within the limited view, the non-alignments of U.S. legal ideal, enforcement to this existing function could lead to the asymmetric result. The study puts forward the implication on the coordinating function of law. When law aligns its ideal, structure and enforcements with the non-legal factors on the ground, such as the existing individual-organization trust relationship, it could catalyze and excel these desirable post-breach practices, as seen in Singapore. The future amendment of law in Singapore also speaks to the strategic and communicative approach and norm adjudication, which catalyze these desirable post-breach responses to promote privacy.

Outline

I. Terminology and Framework.................................................................
   A. Data Security Breach Cases..............................................................
   B. Post Breach Responses of Organizations...........................................
   C. The Elements of Trust Act and Trust Relationship and What are not........
   D. The function of law: Gap, Communication, and Assurance....................
   E. Summary of Symmetry and Alignment of Post-Breach Responses............
II. Evidence on Post-Breach Responses in FTC and PDPC Cases........................
III. Evidence from Organization Interview Excerpts...................................
IV. Analysis: Trust Relationship as a non-legal factor, a meeting point between ideals with reality, and Coordination function of law..............................................................
V. Conclusion: How law enhances privacy proactive practices through trust relationships........
I. Terminology and Framework

For the purpose of this chapter, the following terms have the meanings as follows.

A. Data Security Breach Cases

"Data Security Breach Cases" means: (i) the FTC decisions including complaints, and the settlement orders categorized under "Data Security" brought under FTC Act section 5 and published on the FTC website until February 2018, comprising of 68 cases; (ii) PDPC decisions determined under protection obligation of Section 24 of the PDPA and published on the PDPC website until February 2018, comprising of 32 cases. The term, in general, refers to the cases involved organization’s inadequate security practices for preventing unauthorized disclosure of personal data, regardless of whether actual disclosure was made or not, and whether the breach caused from the insider or outsider attack. The term does not exclude cases where the breach of privacy involved.

B. Post-breach Responses: Beyond Compliant Behaviors of Organization

In this chapter, the term "post-breach responses" refers to the organizational responses after the breach occurs until the end of the investigation of the enforcement agency as found in the case materials and commissioner statements.

These organizational responses are categorized into five main types: breach notification to affected individual customers ("NC") i.e. letter and email informing breach and apology, notifying breach to the agency or authorities ("NA"), general breach remedy ("GR"), i.e. fix the vulnerabilities and prevent further breach, specific individual remedies ("SR") e.g. voucher, gift cards, cash, free services; Cooperating with the agency during investigation ("CA") i.e. being forthcoming and admitting breach.

“Beyond Compliant Behaviors” refers to acts performed by breaching organizations to affected individuals that are not mandated by the relevant law, such as HIPPA, and other U.S. state laws on data security breach notification (SBN), and the duty to report regulators such as Monetary Authority of Singapore (MAS) regulation at the material time of the breach.

In this chapter, beyond compliant behaviors are examined whether they fall into the "trust act" and "trust relationship," as defined in section I.C.

C. Trust Act and Trust Relationship: Elements and What are Not

"Trust act" or "Trustful behavior" is used interchangeably to refer to acts of parties in the "trust relationship." Trust relationship means a relationship in which a party is motivated by the trust of the other party to maintain his/her interest in the relationship.

The elements that form “trust act” are as follows: (i) self-initiation or willingness; (ii) self risk-taking or exposing to some degree of vulnerability; (iii) motivational factors of the other party’s interest in the relationship; (iv) the ongoing relationship; (v) direct performance to the other party.

What is not "trust act" or "trust relationship" are in the following circumstances when:

178 https://www.ftc.gov/taxonomy/term/249/type/case
(i) Organizations are forced choiceless to perform such acts. These acts could be cooperative acts with the other party or the enforcement agency.

(ii) There are no risk and uncertainty involved in decision-making. These could be the case when the law requires organizations to act or not to act in certain ways and completely fix organization behavior to comply with the legal requirement.

(iii) When the other motivational factors such as fears from bad reputation images, economic loss, and penalties, violation civic duty, or cooperation and civic duty are key drivers behind such acts rather than the other party's relationship interests.

The indicator that reputation, not trust, is a key driver is when there is no direct and existing relationship between parties involved in the performance of such act in question. From law and regulation literature, an organization with high visibility to public receives more reputational pressure than organizations with relatively low visibility. (Kagan et al., 2011, p 43). The visibility is measured by, for instance, characteristics of companies such as public company, size, and consumer facing.

(iv) A system that assures parties with some certainty and reduced perceived risks of a party who performs an act to the other party is not trust relationship, but assurance or system trust. As discussed further in Section I.D, law, for instance, could serve as a trust system to assure parties with perceived reduced risks to the level that is acceptable to initiate trust act to another party in a relationship.

D. The Coordinative function of laws and enforcement: Gap, Communication, Assurance, Motivation

In explaining the beyond-compliant behaviors observable from the U.S. and Singapore data security breach cases, I made an analysis from three accounts: first, relational trust between individual and organization; second, the alignment or congruence between values uphold by law and organization; third, the influence of organization over law or vice versa. I borrow the lens from law and compliance, regulation and enforcement theories to understand these behaviors. It should note that I assume the beyond-compliant behaviors in the focus of this chapter, which includes the apology, breach notification, remedies and correction actions, are broadly considered as corporate social responsibility, and voluntary decisions in regulation literature (Vogel, 2005; Kagan et. al, 2011).

E. Summary of U.S. and Singapore Legal and Organization Perception and Treatment on Post-Breach Responses to Affected Individuals

Table 4.1

<table>
<thead>
<tr>
<th>1. Organization</th>
<th>U.S</th>
<th>Singapore</th>
<th>Symmetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Ideal</td>
<td>- Relationship, Trust</td>
<td>- Relationship, Trust</td>
<td>-Yes</td>
</tr>
<tr>
<td>- Practice</td>
<td>- Yes</td>
<td>- Integrated into the</td>
<td>-Yes</td>
</tr>
</tbody>
</table>

| 2. Agency Recognition | FTC Section 5 complaints  
- Not Consistent  
- Both, a few occasions implied norm  
- Most negatively | PDPC Section 24 decisions  
- Consistent (nearly all)  
- Both, almost all clearly implied norm  
- Most positively | internal response plan, decision-making in all global firms |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Law Structure</td>
<td>Overall Fragmented, Silent under FTC Section 5, mandate under specific sectoral law, most state adopted mandate SBN with different criteria</td>
<td>Voluntary basis, the omnibus PDPC silent on SBN, but recommended in its non-legal binding guides (CARE), not required under specific laws</td>
<td></td>
</tr>
<tr>
<td>(as of February 2018)</td>
<td></td>
<td></td>
<td>-No</td>
</tr>
<tr>
<td>4. Future Law Trend</td>
<td>Mandate SBN with Stronger Requirement</td>
<td>Mandate SBN with remedial exception (Stronger presence with elevated exception status of post-breach remedy)</td>
<td>-No</td>
</tr>
<tr>
<td>5. Legal Ideals</td>
<td>Privacy rightness</td>
<td>No privacy right but privacy interests protected</td>
<td>-No</td>
</tr>
</tbody>
</table>
| Vertical Alignments of Values and Preference | Solid, fragmented, non-directional  
Strong presence of rights  
Not aligning with relational trust on the ground | Soft, directional, encouraging, carving-out rules, non-right basis  
Alignment with relational trust on the ground | |

Note: By referring to organizational and legal ideal, I mean the following:

“Organizational ideal” or organization's worldview refers to organization-individual trust relationships. I look for this evidence in the interview memo with data protection officers in Singapore and the interview excerpts from privacy on the ground in the U.S.

“Legal ideal” refers to the legal characteristics of personal data protection in U.S. and Singapore deduced from the legal constraints, predispositions and regulator's interpretation through cases, discussed in Chapter 2 and 3. It is noted that this descriptive claim entails more than what law in general purports to protect privacy, but how law, its structure, and functions purport to uphold certain normative values, actually form the shape of privacy at this moment.
**F. Comparison of Post-Breach Responses found in the FTC and PDPC**

<table>
<thead>
<tr>
<th>Dimension</th>
<th>FTC</th>
<th>PDPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Time (Promptness)</td>
<td>Broadly mentioned</td>
<td>Most notification sent 1-4 days after</td>
</tr>
<tr>
<td></td>
<td>Notify “After learning of breach”,</td>
<td>discovery, 2 weeks’ period is still</td>
</tr>
<tr>
<td></td>
<td>“shortly after learning”</td>
<td>acceptable remedies</td>
</tr>
<tr>
<td></td>
<td>Months’ time (1-8)</td>
<td></td>
</tr>
<tr>
<td>2. Amount ($)</td>
<td>Not mentioned</td>
<td>Up to SGD 100</td>
</tr>
<tr>
<td>3. Specific Kinds to Individuals</td>
<td>Reimbursement for some customers who</td>
<td>Special remedies i.e. free service and</td>
</tr>
<tr>
<td></td>
<td>requested</td>
<td>gift voucher, 24/7 call center, account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>number changes, hiring new vendor</td>
</tr>
<tr>
<td>4. Firm Characteristics</td>
<td>Most are consumer-facing firms,</td>
<td>All from organization with ongoing</td>
</tr>
<tr>
<td>(Consumer Relationship)</td>
<td>including business end-users.</td>
<td>relationship, not Data Intermediary</td>
</tr>
</tbody>
</table>

*The evidence found in the FTC cases provide limited and inconclusive view due to some post-breach responses found on the ground were omitted from mentioning in the FTC complaints, and the post-breach behaviors found may relate to the state SBN laws.

**G. Framework**

**G-1: Value driven: Organization ideal on trust relationship: drives for beyond compliance?**

Explaining from trust relationship perspectives, these beyond-complaint behaviors are trust act of organization party, which delivers directly to individuals in the ongoing relationship with breaching organizations. The motivation for the organization party is to maintain the relationship interests of the individual. In the situation of a data breach, individual interests in the relationship with organizations come from the values attached to personal or identifiable data pertaining to individuals. When data has been breached by without receiving authorized access or disclosure from the individual, those individual interests injured at the time of breach were of concerns by organization party, who drives the post-breach responses from the organization such as breach notification and remedies.

It is noted that organizations by initiating these beyond-compliant behaviors without legal mandates are prone to different kinds and varying level of risks and uncertainty involved in this regard. Legal uncertainty poses risks of unknown legal consequences from such action from the regulator viewpoint. For instance, whether the organization will receive praise for accountability and transparency from breach notification made to individuals, or those actions would only trigger investigations and lawsuits. The unsettled meaning applying to these behaviors, in the lack of agreed norm, risks being misunderstood by individuals who receive those post-breach responses, and affect how they will continue or stop their relationship with the breaching organizations. Risks also come from non-conformant practices with peers in the industry who opt
to bury the incident rather than notifying, which could turn the post-breach responses into a message of poor control of organization practices that affect the organization's competitiveness with peers. Those beyond-compliant organizational behaviors involve risks and uncertain situation fall under the elements of trust act, which organization exerts to gain trust from the individual party after the breach.

The indicator that trust relationship norm, not privacy norm, is that the practices occur before personal data protection law became in effect. Another indicator is when the practices occur despite the non-firmly established notion of privacy. The counter-arguments to trust relationship norm is also the accountability, cooperation, and reputation, discussed in Explanation G-3.

**G-2: Value Alignment: Converging points between legal and organizational minds.**

Explaining from Tyler’s value climate-building of the rule, the law infuses its value into the organizational logic and meets in minds with values upheld by employees who perform decision-making on the post-breach responses of organizations.180 It is also noted that (i) Tyler does examine the question of how to effectively induce compliant behaviors, but I apply Tyler’s model to explain beyond-compliant behaviors, (ii) I expanded the meeting points in values, suggested in Taylor's, to rational interests, which also covers moral values defined by actors involved. (iii) Tyler's concern the congruence of employee's personal values and legal values, but I apply to the broader context of organizational values and legal values in regarding data breach, security, and privacy.

For data breach responses, data privacy officers (or data protection offers, DPOs) are persons primarily responsible for handling these issues inside the organization. In large organizations, the DPO team can comprise of more than one person, including those with the title chief data privacy officer. In multinational corporations (MNCs), the person who takes responsibility for this issue could have the title of DPO leads, Regional Privacy Counsel and other privacy professional titles. More information is attached in Appendix B.

Explanation G-2 will be plausible when there is at least a contribution of two evidence from the organization's worldview and legal ideals that meets in term of trust relationship:

(i) There is supporting evidence on established organization's worldview on trust relationship in relation to their post-breach response. Specifically, the motivation of those acts is to secure the trust of the individual party and dependent on their reaction. I investigated through the interview of organizations in U.S. and Singapore.

---

180 Tom R. Tyler, The psychology of self-regulation: normative motivations for compliance, Elgar book (2011) 79-86. The Self-regulation model (or Valsaed-Based Model) is based on the premise that employees' ethical values play important role in abiding with the workplace rule of organization. Activation of employee’s internal motivation could be done when they believe that the rules of their organizations "(a) are legitimate, and hence ought to be obeyed or (b) that the values defining the organization are congruent with their own moral values, thus leading people to feel that they ought to support the organization." Tyler's 2011 put forth that the challenge is to create organizational cultures that enhance the motivational power of employees' ethical values. Legitimacy is determined from the employees' perception on their responsibility for following the organizational rules, such that the organization is entitled to have its rules and policies obeyed (also Tyler, 2006 at 85; Tyler et al., 2008 at 78)
(ii) There is supporting evidence from case documents, legislative history, and public consultation that law intends and attempts to speak in tune with these norms on trustful post-breach responses. That means the law "infuses" "new" desirable value into the climate of organization privacy practices. The infusing behavior can be observable from, i.e. training sponsored by the government, the characteristic of legal ideals in a jurisdiction that persuades post-breach behaviors. This "new" value can take the form of new language introduced by law that needs interpretation to reach an understanding, and changes to be made in organizational logics and structure. I look for the evidence of "new" in terms of confusion, attempts to convince and elaboration needs for employees to make sense of these terms in the interview memo.

(iii) The evidence of congruence as to the ideals of organization and law.

**G-3 Outside-Non-Legal Pressure: Law is less relevant, media pressure and fear of bad publicity drives organizational beyond compliant behaviors.**

Organization’s fear of reputation loss when being discovered by the public could be the explanation for breaching companies' beyond-compliant behaviors. This is, for instance, when the breaching companies believe that they have worsen image when the public learn by themselves from media about data breach incidents, and so decide to take the step to notify and remedy breach to the affected individuals to secure public trust. From this lens, the more public visibility the company has either in terms of the public company, large private company or consumer-facing entity, the more pressure it receives from the public to adopt-beyond compliant behaviors. Relatively, the counter argument would be the evidence found on the low visibility of the company with small or medium size should feel lesser urge from the public to adopt beyond-compliant behaviors to save their reputational images.

Notwithstanding, the dilemma is also present at the time of decision-making because the consequences of disclosure of breach could expose the breaching companies to further risks of the investigation by the agency, consumer lawsuits and malicious actors' further exploitation of companies' vulnerabilities derived from breach incidents. The better reputation the companies have put higher risks for them to disclose the breach to the public, as compared to small and less visible firm unless companies in the “market of virtue”, in which consumer protection, transparency, and honesty forms core basis for reputation. The latter would align the company’s interests in disclosing the breach with a good reputation, and mitigate the consequential negative impact on reputation from the post-breach behaviors. In this situation, the law, when not mandating, could become extra points to draw those companies their core values meet when adopting these desirable post breach behaviors to beyond-compliant practices.

In addition, the more intrusive breach which involved hacking activities, malicious intent of actors, and public accessibility of unauthorized disclosure of the information would appear to add more reputational pressure to notify the breach. This is because the nature of the data breach in term of the intrusiveness and exposure of breach to the public also allows the public to assess how bad the reputation the company is associated with the breach.
It is presumed that there must be a clear and agreed public measurement on the organizational performance, i.e. what is good or bad practices, applied to the organizational responses to breach in terms of notifying and remediing. Otherwise, it is not clear how reputation works in driving companies to notify breach when the public view are mixed between good reputation based on honesty and transparency and the bad reputation that comes with carelessness and poor control of individual personal data of the companies. Regarding the public measurement tools, the legal duty could infer the sense of civic duty or the right thing to do, which when such duty is not fulfilled creating the public perception of wrongdoing and bad reputation. For example, in case that the law mandates breach notification, notifying could associate with law-abiding behavior and ‘good' image, while not notifying is law-violating behaviors which relates to ‘bad' image. How the media frames the company behaviors in another way to offer the public with measure tools for the reputation from such company post-breach responses. However, the scope of this dissertation does not allow covering the full extent of media and public reaction on the post-breaches behaviors of companies, which needs a further in-depth inquiry. The basis for reputation as distinct from trust relationship is the ongoing relationship with an individual at the time such response were made, and the manner of how notification is delivered i.e. to affected individuals or the press release.

It is also noted here that the reputational-driven behaviors and the relational trust driven behaviors appear to overlap in practices and both reputation and customer trust, as I will discuss in the evidence from the interview, were raised by the interviewees when deciding to notify or not notify breach. However, reputation is often mentioned when deciding not to notify, and customer trust is mentioned when deciding to notify individuals. From a theoretical lens, these following distinctions suggest that other factors beyond reputation drive the post-breach behaviors, though not leading to a conclusive answer of trust behaviors: (i) the privileges or priority, e.g. time, direct, individual-tailored means of communication, given to the breach notifications made to affected individual party in the ongoing relationship before informing the public in general; or (ii) case when there is an imbalance proportion of low reputational pressure from the public in notifying and high legal risks from notifying of breach.

Explanation G-3 will be sound when there is at least a contribution of these supporting evidence. (i) clearly established norms in a society to label with good or bad reputation regarding the post-breaches responses, e.g., notification, admittance or breach and remedies; (ii) cases reveal the timeline of media discovery before the responses; (iii) cases reveal companies with more public visibility notify the breach than companies with less visibility.

H. Limitation of Method and Findings

The scope is limited due to the nature of case materials, legal factors, and the interviewee organizational characteristics. An asymmetry of the conclusion of facts found in the FTC’s complaints and the PDPC’s decisions provide limits in some aspects of comparison and analysis. Not all the post-breach behaviors by respondents were mentioned in the FTC decision. Therefore, such behaviors found provide limited reflection of actual corporate practices on the ground. For the PDPC decisions, the facts were mentioned consistently and the omission means none has been presented to the Commission attention until the decisions were made. Such
behaviors found the case provide some reflection on the emerging organizational practices on the ground. Furthermore, the residency of affected individuals are not mentioned in the FTC cases and therefore provide limited way to exclude the influence of required from the SBN laws of certain states on breach notification behaviors. The strategic and targeting enforcement on respondents from some industry or businesses in a certain time period, especially seen from the FTC enforcement, does not allow the finding to represent the full picture of post-breach privacy practices in the U.S. Individual complainants who are members of the public brought most cases before the PDPC. In fewer events, the PDPC decided to trigger the investigation under Section 50 of the PDPA, brought most cases.

The limits to different interviewee level in organization and by title, different time period of how the interview was conducted, questions and materials involved, prevents the complete view from comparative analysis. Small groups of interview participants do not allow generalizing the finding to represent the full pictures of organization perception and practices in U.S. and Singapore.

II. Evidence of Post-Breach Behaviors in the Cases of U.S. and Singapore

This part examines the evidence found from the FTC and PDPC cases on post-breaches responses from respondents in U.S. and Singapore. Within the limitations mentioned in part I, the comparison is made on the symmetry of both agencies’ recognition in terms of consistency and values. (See table 4.1) Consistency means how consistent such post-breach behaviors appear throughout the data security breach cases. Values mean whether (a) the factual value and normative value inferred from the contexts mentioned by the agency in the cases; (b) positively mentioned or praise versus negatively mentioned or blame by the agency. The consistency and values aspects provide implication on the agency’s perception and treatment on such behaviors, which will be assessed with the organization’s ideal and practices on the ground from the interview of organizations.

In addition, the comparative analysis is made between the patterns of positive or desirable post-breach behaviors found in the FTC and PDPC cases from the axis of time (promptness), amount (remedies), manners and kinds. This is to illustrate the magnitude of such beyond-compliant behaviors and the respondent’s characteristics. The finding provides implication for the relational trust as non-legal factors driving organizational beyond-compliance.

From the vertical view, the findings on agency’s recognition of post-breach response will be examined with evidence from the interview on the organization perception and worldview to see the alignment among values infused by the law, enforcement and the organization in practices and the coordinating function of law with the reality.

A. Post-breach Responses found in FTC Cases

“Consistency”: How consistent Post-breach Responses mentioned by the FTC in Data Security Breach
Since the first cases on data security in 2000 until February 2018, the FTC has not consistently mentioned the post-breach responses from the respondents. There are 17 out of 66 cases until February 2018 that FTC mentioned post-breach responses to individuals in the data security breach cases published on the FTC website. In these cases, the FTC mentioned one of these behaviors: breach notification to affected customers; preventing further unauthorized access, fixing the vulnerabilities.

Out of 17 cases, there are 13 cases that the respondents notified individuals of affected breach. These are the FTC matter against Guidance Software, Life is Good, DSW, Choicepoint, Premiere Capital Lending, Genica Compgeek.com, Elsavier Reed, TJX, Practice, Uber, Trendnet, Lookout, Dave&Buster, Asustek.

In those cases, they involved five small-medium private firms, one large private firm, seven public firms; eight of them were consumer-facing entity and four were non-consumer facing entity. Five of respondents are commercial retailers; the other five businesses are in the data and technology products. Breach types range from five-insider breach, caused from employees, unauthorized access through internal means, unverified subscriber, and seven respondents were hacked into its database. All involved sensitive data being accessed; six of them related to credit card fraud, two involved consumer reports, one respondent involved government-issued ID and one involved debt portfolio.

“Value”: Fact and Norm, Positive and Negative Implications

In these cases where post-breach responses were found, FTC sometimes mentioned these behaviors as a matter of fact. And, in a few occasions below, it contains normative meanings. Most contains negative notions of the delay in notification and patching of vulnerabilities after breach discovery.

Table 4.1 Types of "Post-Breach Responses" found in the FTC Cases.

<table>
<thead>
<tr>
<th>Breach Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>● sent breach notification letters to affected customers. (Guidance Software- 6 months, life is good)</td>
</tr>
<tr>
<td>● sending notification letters to customers for whom it had or obtained addresses one month after issuing the press release (DSW)</td>
</tr>
<tr>
<td>● notified approximately 35,000 California consumers and subsequently consumers in other states (Choicepoint)</td>
</tr>
<tr>
<td>● breach notification letters sent to affected drivers 5 months after discovery. The additional breach was discovered 3 months later, and additional letters were sent. (Uber)</td>
</tr>
<tr>
<td>● issued the press release in Jan 2007 in a month later after learning of the</td>
</tr>
</tbody>
</table>

181 The FTC recognized the absence of post-breaches responses in three cases (Fajilan and Associates, ACRAnets and SettlementOne and from the respondents’ post-breach remedies in the FTC matters against GMR Transcription.
breach, informing that payment info of personal information has been stolen from its computer network. (TJX)

**General Remedies**

**Positive**
- after learning, took steps to prevent further unauthorized access (Guidance Software, Life is good)
- after learning, terminated seller’s CRA logins (PCL)

**Negative**
- 4 years being aware of fraudulent accounts created but continued to furnish info to suspicious subscribers. (Choicepoint)
- still failed to detect the unauthorized access of those additional 83 reports until “more than a year” (PCL)

**Special Remedies**
- some amount of reimbursement to these customers (DSW)

**Notification Authorities**
- notified law enforcement authorities and the credit reporting agency (PCL)

---

**Table 4.2 Contexts where the FTC mentioned post-breach responses**

<table>
<thead>
<tr>
<th>Year</th>
<th>Case</th>
<th>Post-Breach Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>DSW Retail Apparel</td>
<td>In March, it issued the press release on credit card info stolen. In April 2005, respondent issued another press release listing the locations of 108 stores that were affected by the breach and stating that checking account and driver's license numbers also had been subject to the breach. Some of these checking account customers have contacted DSW requesting reimbursement for their out-of-pocket expenses, and DSW has provided some amount of reimbursement to these customers. In April 2005, respondent also began sending notification letters to customers for whom it had or obtained addresses.</td>
</tr>
<tr>
<td></td>
<td>Product</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>Choicepoint Data Platform for Business</td>
<td>4 years being aware of fraudulent accounts created but continued to furnish info to suspicious subscribers. ChoicePoint collects the information without making any contact with the consumers whose information it sells. (para 10). In February 2005, pursuant to a California state law requirement, ChoicePoint notified approximately 35,000 California consumers that it might have disclosed their personal information to persons who did not have a lawful purpose to obtain the information. Subsequently, ChoicePoint notified approximately 111,000 consumers outside of California that their information may have been compromised More recently, it notified an additional 17,000 consumers, bringing the total to 163,000 In all cases, the information disclosed by ChoicePoint included unique identifying information that facilitates</td>
</tr>
<tr>
<td>Year</td>
<td>Company/Industry</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>2007</td>
<td>Guidance IT Business Products</td>
<td>Identity theft, such as dates of birth and Social Security numbers, as well as nearly 10,000 credit reports. At least 800 cases of identity theft arose out of these incidents.</td>
</tr>
<tr>
<td>2007</td>
<td>Life is good Retail Apparel Products</td>
<td>When aware of breach 6 months after the intrusion, Respondents at which time they took steps to prevent further unauthorized access and to notify law enforcement and affected consumers.</td>
</tr>
<tr>
<td>2008</td>
<td>T.J. Maxx</td>
<td>Further, between May and December 2006, an intruder periodically intercepted payment card authorization requests in transit from in-store networks to the central corporate network, stored the information in files on the network, and transmitted the files over the internet to remote computers. After learning of the breach, the respondent took steps to prevent further unauthorized access and to notify law enforcement and affected consumers. (para. 9) Tens of millions of unique payment cards used by consumers in the United States and Canada (para. 11) and fraud charges claimed by issuing banks on these accounts. Consumer needs to wait for new cards replacement to access their card and bank account. In addition, the breach compromised the personal information of approximately 455,000 consumers who had made non-receipted merchandise returns. A month later learning of the breach, T.J. Maxx issued the press release in Jan 2007 stating that payment info of personal information has been stolen from its computer network.</td>
</tr>
<tr>
<td>2008</td>
<td>Elsaver Data Platform for Business</td>
<td>Since March 2005 (3 years after being hacked), respondent REI through LexisNexis has notified over 316,000 consumers that the attacks disclosed sensitive information about them that could be used to conduct identity theft.</td>
</tr>
<tr>
<td>2008</td>
<td>Premiere Capital Lending (Consumer Mortgage Lender)</td>
<td>PCL learned of the breach on July 25, 2006, after two consumers contacted PCL to ask why their consumer reports had been requested by PCL, a company with which the consumers had no relationship. After confirming that the requests were unauthorized, PCL terminated the seller’s CRA login and notified law enforcement authorities and the CRA, which in turn notified the three nationwide CRAs. In August 2006, PCL mailed breach notification letters to the 317 noncustomers whose reports the hacker had obtained. (para. 12)</td>
</tr>
<tr>
<td>2008</td>
<td>Genica Retail Computer Products</td>
<td>When aware of breach 6 months after the intrusion, Respondents at which time they took steps to prevent further unauthorized access and to notify law enforcement and affected consumers.</td>
</tr>
<tr>
<td>2010</td>
<td>Dave&amp;Bust</td>
<td>Between April 30, 2007, and August 28, 2007, an intruder attacked and...</td>
</tr>
<tr>
<td>Year</td>
<td>Incident</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>2011</td>
<td>Lookout</td>
<td>The 2009 Breach occurred when an employee of lookout business customer able to access the entire I-9 database containing PI of over 37,000 consumer data by making some minimal, easy-to-guess changes in URL. She entered the guessed password and ID &quot;test&quot; and able to access the entire database. It took steps to patch the vulnerabilities and disabled &quot;test account.&quot; In Jan 2010 (a month after December breach – emailed breach notification letters to (business) customers whose account the employee may have viewed.</td>
</tr>
<tr>
<td>2013</td>
<td>Trendnet</td>
<td>Respondent learned of the breach on January 13, 2012, (after the breach was posted online Jan 10), when a customer who had read about the breach contacted respondent's technical support staff to report the issue. Shortly thereafter, respondent made available new software to eliminate the vulnerability and encouraged users to install the new software by posting notices on its website and sending emails to registered users. (para. 11)</td>
</tr>
</tbody>
</table>
| 2016 | AsusTek | Notice of Design Flaws and Failure to Mitigate  
In November 2013, the security researcher again contacted respondent, warning that, based on his research, 25,000 ASUS routers now allowed for unauthenticated access to AiDisk FTP servers. The researcher suggested that respondent warn consumers about this risk during the AiDisk set up the process. However, ASUS took no action at the time.  
It was not until February 2014 – following the events described in Paragraph 32 [hacking activities] – that respondent sent an email to registered customers notifying them that firmware updates addressing these security risks and other security vulnerabilities were available. (para. 23) |
| 2017 | Uber | 5 months to discover the existence of a breach and corrected and breach notification letters sent to affected drivers 5 months after discovery. The additional breach was discovered 3 months later, and additional letters were sent. |

**Breach Notification as a Matter of Fact in The FTC Complaints**

The facts mentioned on respondent’s breach notification are found in 13 cases involved 7 online retailers\(^2\), 4 data businesses and 2 security-technology products. All of these cases have in

---

\(^2\) The FTC matters concerning Dave &Buster’s, TJX, Genica Corporation and Compgeeks.com, Life is good, DSW Footware, Uber.
common the actual disclosure of information to the unauthorized person and sensitive data leakage. For retailers, payment information including consumer's credit card numbers were stolen by the hackers. Banks reported actual loss from credit card fraud and identity theft. In cases of data businesses, the leaked personal information includes consumer reports and credit history, debt portfolios and the information found in the employees’ immigration forms. In security-technology businesses, the personal data leaked include the credit cards information from the customer's sale transaction and the live video feed from user's camera and geolocation data. The intrusiveness of breach varies: 8 cases involved hacking activities into the breaching organization’s system by outside attackers; other 5 cases involved internal means such as disguise as subscribers to receive consumer reports, or client’s employees received data information products.

The FTC noted in its decision and complaints that the organization respondents had made notification of the breach to affected customers and enforcement agency, and rendered corrective behaviors to fix the security flaws including preventive instructions for its customers. These are evident in cases involved online retailers those payment information including consumer's credit card numbers were stolen by the attackers, resulted in fraud and identity thefts (Dave & Buster's, TJX, Genica Corporation, and Compgeeks.com, Life is good, DSW Footwear). It is noticeable that the agency alleged respondents in these cases under the deception acts and/or unfair practices.

Breach Notification as a Matter of Norm

(a) Implications for Undue Delay of Breach Notification Time Period

In a few instances like the matters concerning Asustek and Uber Technologies, the FTC has claimed that the organization respondent took “five to eight months” after learning of breach to send the breach notifications to affected users. In Asustek, the FTC in mentioning about the respondent’s “failure to provide timely notice” implies that eight months’ period of time since first learned of multiple vulnerabilities from individuals who reported on hacking activities are undue delay. The agency mentioned further that the respondent failed to notify them about the vulnerabilities and advise simple steps to mitigate the issue. By contrast, the FTC in Trendnet mentioned that the IP camera vendor, systems of which were hacked resulted in users' live feed posted publicly on the internet, had made notice on its website of the breach and updated software as well as sending the email notification to its registered users two days after the news reports. The agency, however, remained silent on whether the time of notifying breach has any implications for its consideration of breach. The lack of the clear signals provided by the agency makes it unclear for the organization to get meaning of what is appropriate when it comes to post-breach responses.

(b) Implied Breach Notification as Part of Reasonable Security Practices

In Asustek, where its web application was compromised and gained unauthorized access to consumer files and router login credentials after which hackers sent the message to consumers. The agency implied that the organization's failure to alert individual consumer about the security flaws and preventive steps in a timely manner, (more than 2 months after first warned) among
other factors, provide a basis for misrepresentation of its secured products and the unfairness claims.

“Notice of Design Flaws and Failure to Mitigate

In November 2013, the security researcher again contacted respondent, warning that, based on his research, 25,000 ASUS routers now allowed for unauthenticated access to AiDisk FTP servers. The researcher suggested that respondent warn consumers about this risk during the AiDisk set up process. However, ASUS took no action at the time.

It was not until February 2014 – following the events described in Paragraph 32 [hacking activities] – that respondent sent an email to registered customers notifying them that firmware updates addressing these security risks and other security vulnerabilities were available.

Furthermore, it was not until February 21, 2014, that ASUS released a firmware update that would provide some protection to consumers who had previously set up AiDisk.” (para. 23)

“Respondent’s Failure To Reasonably Secure Its Routers And Related “Cloud” Features

Para. 30 (g.) provide adequate notice to consumers regarding (i) known vulnerabilities or security risks, (ii) steps that consumers could take to mitigate such vulnerabilities or risks, and (iii) the availability of software updates that would correct or mitigate the vulnerabilities or risks.”

This normative implication, however, does not consistently arise in other FTC cases with similar facts and therefore send an unclear message to the firms if it would apply in future cases.

(c) Other Implications for Post-Breach Responses:

- Notification Duty Related to Requirements of Other Regulations: State laws on Data Security Breach Notification and HIPPA

In the FTC matters concerning Fajilan and Associates, ACRAnets and SettlementOne Credit Corporation, these companies merged and resold consumer reports received from the three nationwide credit reporting agencies, and also were subject to requirements under the safeguard rule and FCRA requirements on information disclosures. The FTC complaints have noted in its allegation of unfair practices that these consumer report providers had not made any efforts to warn its other business end users of known threats after learning of the intrusion and unauthorized access of consumer reports, nor advice their clients to conduct a security review of their system to ensure adequate protection and verification practices. It also put forward that no efforts have been made to patch vulnerabilities nor screening procedure of upcoming users for virus-free or proper protection after failure to detect unverified users. By mentioning the absence of post-breach responses from respondents, the FTC implies its expectation to see the positive responses from the respondents in these cases.

The FTC mentioned the breach notification as required by the state laws, such as in Choicepoint and Elsavier, platforms for search engine and other verification products for business clients. It is noticeable that FTC distinguished the company notification made to the California
residency under the SBN requirement, and the other notifications later made for people residing outside California. The enactment of state laws on data security breach and the regulations highly influenced the respondents to provide post-breach practices in the U.S.\textsuperscript{183}

\textit{(d) Federal Injunction and Order to Notify Breach to affected customers}

Breach notification also mentioned by the FTC in cases involving data broker's disclosures of sensitive consumer financial data, such as debt portfolio or consumer reports. In Bayview Solution and Cornerstone LLC, the federal district court of Columbia had issue federal injunctions for respondents to take down debt portfolio that contained "extremely sensitive consumer information" on their website accessible by the public and notify affected consumers on such disclosures including steps for them to prevent identity theft. The FTC decisions and orders in re: Henry Schein Practice, ControlScan, HTC America, Compete and Oracle also included notifying breach to affected consumers.

\textbf{Unclear Normative Meanings for Desirable Post-Breach Responses, High Risk Remaining with Less Assurance}

Notwithstanding over a decade of enforcement against unreasonable data security under Section 5 of the FTC Act, the FTC in determining inadequate data security practices has not consistently recognized desirable post-breach responses through cases. From the organization's viewpoint, the messages sent from the FTC enforcement does not provide enough assurance or endorse some of these proactive behaviors by the respondents despite greater risks concerned reputation from such notification of a breach and future lawsuits. Similarly, the desirable remedying steps to be taken after the companies found data leakage has not been consistently addressed through FTC enforcement. The language and mechanism under section 5 pose limitation to information disclosure before the unauthorized disclosure take place, and tangible market-defined injury or harm to safety, fraud, and identity theft. This fails to take into account the post-breach duty like remedial action, breach notification. The protection based on fairness and reasonable consumer expectation measured at the time consumer choices has been made to engage in the relationship with business parties. Thus, less attention has been focused on the actual injured interests at the time of breach and remedies. The mandate privacy and security programs issued by the FTC settlement order with respondents also did not entail specific duty or recommend organizations to provide desirable post-breach remedies to affected consumer.

“Appropriate remedies” under the FTC Section 5 may focus on fixing existing vulnerabilities and preventing future vulnerabilities by creating a comprehensive security program rather than encouraging the respondents to provide the full refund for the misrepresentation of product security, changes or monetary compensation for the time spent by the affected consumer.\textsuperscript{184}


B. Post-breach Responses from the PDPA Cases

General Observation

After the first series of decision in April 2016 until February 2018, PDPC have made 32 decisions under Section 24 concerning the unreasonable data security arrangement, the PDPC found most organizations found lacking of adequate security measures in place to prevent unauthorized disclosure of personal data at the time of the breach. In five cases of the total cases, no breach was found in Re: BHG, and for the other four cases, only data intermediaries of organizations were found in violation of Section 24.185

In 27 cases from the total 32 cases, data leakage come from the employee's mishandling of personal data, which contains in a physical and digital format. There are only 5 cases involved outsider attacks. In 4 cases where organizations found in breach, leaked data may not actually been disclosed to the unauthorized party. For those cases with actual disclosures of leaked data, almost 90% of actual disclosure comes from the organization respondents having businesses in providing consumer products including financial products, entertainment and lifestyle services such as food and beverages; the remaining 10% of respondent businesses provide professional and education services (3 organizations). About 88.38 % of actual disclosure comes from the retail industry, 9.9% from the professional community, the remaining 1.32% from the financial industry. Most incidents were discovered by other individual customers of the organization who informed the organizations of the incident and made the complaint to the PDPC against the unreasonable data security practices of organizations. In 5 cases involving hacking activities, public members found the list of personal data posted by hackers on the third-party website publicly accessible in 4 cases, and in one case was found by the organization's IT vendor about the unauthorized access and sending of phishing emails to the organization's subscribers.

Half of the data leaked concerns personal data of sensitive nature such as NRIC (Government issued ID), passport, financial data contained in the statements for security account holder and insurance policyholder and the debt-related information of members. The other personal data includes membership information; account information, ID and Password, email address and telephone number, residential area. Two cases involve children information and date of birth.

As illustrated below, organizational respondents had endorsed behaviors beyond legal requirement towards the PDPC and consumer. The PDPC merely recognized a few of those as factual evidence without containing normative implication in the first series of case that came out in April 2016. In most cases, the PDPC clearly stated in the assessment of breach and direction issued to the respondent that post-breach behaviors were taken into account. In later decisions, some were clearly clarified which behaviors were mitigating factors and which were aggravating factors.

185 The latter includes the matter against Toh-Shi I and II, Data Post, Intermediary of Tiger Airlines and 1 case of investigation discontinued.
The following organization’s post-breach responses are found:

(a) *Notification to affected Individuals (NC)*

<table>
<thead>
<tr>
<th>Positive</th>
<th>Negative</th>
</tr>
</thead>
<tbody>
<tr>
<td>● next-day email notification of hacking activity on the website and measures taken to minimize damages (Re: Institute of Engineer Singapore),</td>
<td>● No notification sent to affected individuals (FuKwee)</td>
</tr>
<tr>
<td>● next-day warning emails sent to subscribers about the phishing emails sent by hackers (Orchard Turn Development)</td>
<td></td>
</tr>
<tr>
<td>● Apology letter shortly after the discovery of breach (Central Depository)</td>
<td></td>
</tr>
</tbody>
</table>

(b) *General Remedies (GR):* prompt corrective and remedial action

<table>
<thead>
<tr>
<th>Positive</th>
<th>Negative</th>
</tr>
</thead>
<tbody>
<tr>
<td>● disabling the access to portal member site, resetting IDs and password, removal of numbers and address on its database (Institute of Engineer Singapore)</td>
<td>● undue delay of 10 months to ensure the issues were fixed (Fei Fah)</td>
</tr>
<tr>
<td>● extra precautionary steps of terminating its vendor and hiring data protection consultant (Challenger Technology, Smiling Orchid),</td>
<td>● not taking down the websites with leaked information two months after being notified of the breach by the PDPC (Social Metric)</td>
</tr>
<tr>
<td>● recall email sent to wrong members (Metro PTE)</td>
<td></td>
</tr>
<tr>
<td>● conducting internal IT auditing and strengthen website within 1-2 months (Metro PTE)</td>
<td></td>
</tr>
<tr>
<td>● restricted view of the computer screen that has personal data (Full House Communication) ensure no lapses in guarding visitor logbook (Eagle Eyes and MCST)</td>
<td></td>
</tr>
<tr>
<td>● Reminding staff of procedure (Toh-Shi and Aviva, Hazel Gift), taking a refresher data protection compliance course</td>
<td></td>
</tr>
<tr>
<td>● Prevent recurrence of the incident, e.g. using a secured database for document sharing among employees (Propnex Realty) and deploying the mail-merge software (Credit Counselling Singapore)</td>
<td></td>
</tr>
</tbody>
</table>
(c) Special Remedies towards affected Individuals (SR)

- waiver of 1 month’s insurance payment, S$50 shopping voucher (Aviva and Toh-Shi)
- apology letter, assistance with queries and concerns, options for changing the leaked financial account number. (Central Depository)
- Apology, S$100 shopping voucher and arrangement to retrieve data from the other customer (Aviva)
- create a new account and correcting data (BHG)
- apology and option to request deletion of the leaked following up email (Credit Counselling Singapore)

(d) Cooperativeness with the agency (CA)

Positive
- Inform the PDPC of breach voluntary and being cooperative during the investigation (Singapore Computer Society, Singapore Telecommunication and Tech Mahindra)
- Admittance of breach in the first instance (Propnex Realty, Credit Counselling Singapore)
- respond in a timely manner

Negative
- Not forthcoming by providing only bare facts (K-Box)
- Delayed responses of 1 month (Fei Fah), seven months (Finantech)
- Cavalier attitudes by providing incomplete responses (Cellar door)

Consistency of Post-Breach Behavior Mentioned in the PDPC Decisions

The study found that most of these post-breach responses of the organizations were consistently recognized as relevant factors in determining the breach, direction, and penalties for the organizations under Section 24. As seen from 27 cases from the total of 31 cases, most of the post-breach practices were mentioned by the PDPC in the factual part and along with the "relevant factors" in assessing breach and/or direction given to the respondent in each case or expressly stated as "mitigating" or "aggravating" factors in the PDPC assessment.

It is noted that in 4 cases where these facts were not present, these cases involved no actual loss from the breach, no actual disclosure, or the breach caused from its intermediary, not the organizations. This could suggest that when these facts present, post-breach behaviors are not relevant in the assessment of breach.

Post-Breach Responses as a Matter of Fact
The following cases the PDPC mentioned post-breach behaviors in a neutral manner in the factual evidence of the case. The three first cases in April 2016, K-box, Challenger, FeiFah Manufacturer, the PDPC recognized that the respondent notified breach to its affected customer without mentioning that they were taken into account in their assessment. In, Aviva and Telecom provider, facts of breach notification are present, and organization found not breaching section 24. Similar fact of breach notification was found in Orchard Turn Development, without mentioning its relevancy in assessment penalties. The case involves hacking activities where phishing emails were sent out by hackers to its subscribers. In Aviva and BHG, the PDPC did not mention prompt remedies provided by organization in its assessment, as they were not found breach of Section 24.

It also is noted that when the some of the positive responses were mentioned in the factual circumstances of the cases, but not all were expressly stated by the PDPC as the mitigating or aggravating factors. In early cases, the first series of PDPC decisions, K-Box, Challenger and Fei Fah notified breach to individuals, but PDPC while mentioning as the factual evidence did not yet express as the "factors" relevant when considering breach until in the later series of cases beginning in the IES where it specifically addressed breach notification as relevant factors in assessing breach and penalties.  

Post-Breach Responses as a Matter of Norm

From the observation of the 31 cases, 27 cases demonstrate at least one type of the post-breach responses of the organization. The study found that the organizations, after learning about the breach incidents, consistently demonstrated positive "post-breach responses" towards affected individuals from breach, i.e. promptly correct and remedy the issues and promptly notify towards individuals. Such behaviors were found rendered from the organization in the very first series of the PDPC decisions rendered in 2016 until Feb 2018. General Remedies are promptly provided from organizational respondents in 20 cases. In 13 cases, organizations promptly made notification of the breach to affected customer. In 4 cases involved sensitive data leakage i.e., NRIC and financial data, Special Remedies are provided to affected customers.

Along with the positive responses, post-breach response also found mentioned negatively by the PDPC in cases where the organization did not or in a delayed manner provide post-breach responses: 5 cases involved delayed fixing issues and remedies.

Implications on promptness, manner of notification, kinds and amount of remedies

The average prompt breach notification occurs in the same day after learning breach to 4 days; the remedial action takes place from 40 minutes to 10 months.

---

186 Also, for instance, in two cases of Aviva and BHG, where organizations made the notification of breach, but the PDPC did not breach and did not consider mitigating factors in rendering penalties.

187 The study excludes one case, my Digital lock, in which the PDPC decided to discontinue the investigation.

188 Furthermore, there are 12 cases where organization cooperates with the PDPC during the investigation in providing, among others, conducting the audits and provide prompt responses to their notice. Four cases of not being forthcoming and cooperative with the agency.
Proper Time to Responses

Besides, the PDPC implied the meaning of "prompt" responses expected from the organizations regarding the following post-breach responses. For notifying affected individuals of the breach, it considers same-day to 4 days notification as "prompt" responses. For the corrective and remedial actions, the PDPC considered "undue delayed" responses and aggravating penalties applied in Social Metric, which it took 2 months for taking down personal data from the website after being notified of breach, and 10 months' time after the breach discovery to ensure that the vulnerabilities were fixed and not collecting more personal data is undue delayed (Re: Fei Fah). However, for a data intermediary of Fu Kwee, the active and acceptable step of fixing the issues in 2 weeks after learning of the breach is still considered relevant for mitigating penalties issued.

Implications for Trust Relationship and Assurance by the PDPC

Based on the evidence of the organization’s post-breach responses towards individual and the interview excerpts, I find that, among other legal factors, trust relationship could be a factor behind these organization beyond-compliant behaviors.

First, the evidence from the PDPC cases demonstrates several characteristics that fall under the trust act initiated by the organization party to the individual parties based on the ongoing relationship between them. In all of these cases, the breach notification and remedies towards the individuals are provided by the organization to the affected individuals who are their customers. These responses were not found from the business who acts as a data intermediary or the business-facing entities without a direct relationship with individuals. The organizations in these cases initiated these proactive privacy responses, which are not mandatory obligations under the Personal Data Protection and relevant laws. By initiating those acts, they take risks in the uncertainty of law that does not specify the legal consequences, and risks upsetting individuals and losing the competitive advantage with peers in the industry who may decide not to inform or remedy breach to the individuals, facing the PDPC investigations and the lawsuits by the affected individuals.

Second, the PDPC, by recognizing of these post-breach behaviors of the organization, communicates and brings the specific examples to the organizations on what practices are encouraged and discouraged to perform to the individuals and the agency after the discovery of the breach. The consistency of the agency in applying these criteria over time has assured the organization with more certainty regarding the consequences of mitigating and aggravating penalties able to be taken into account in their decision-making regarding the post-breach responses. At the same time, it provides incentives for the organization to render positive post-breach practices towards individuals for a more lenient penalty and correcting the images after the breach.

Implications for Language Cultivating Trust, Voluntary, Proactive Attitudes in Organizational Response after the Breach

The voluntary attitudes of respondents in rendering their post-breach behaviors and cooperative attitudes with the agency are considered by the PDPC when assessing the direction and penalties for breach. In the decisions Re: IES and Re: Propnex Realty, the PDPC mentioned
the act of “voluntarily” report of breach and “admittance” of breach of respondents, which imply the PDPC’s preference on the respondents’ willingness and activeness in performing their post-breach responses. In other instances, when the respondents promptly delivered notification and remedial actions to individuals as found in the PDPC decisions Re: Challenger Technologies Limited\(^{189}\), Re: Metro, Re: Singapore Computer Society\(^{190}\), they were issued with only warnings without penalties for the breach of section 24. This is notwithstanding the large number of 165,306 individuals’ membership information being disclosed to other members due to erroneous email forwarding in Re: Challenger Technologies Limited.

The language used by the PDPC also implies some non-desirable attitudes from the respondents following the breach discovery, which may result in significantly higher penalties. For example, the PDPC mentioned the respondents’ “cavalier attitude”, “ignorance” and “disregard” when it applied aggravated penalties to Cellar Door\(^{191}\), Fu Kwee\(^{192}\) and K-Box. In Re: Fu Kwee, a food caterer was imposed with the penalties amount of S$3000 for the unsecured URL order number, allowing a customer to look up other customers’ personal information such as address, contact and phone number by changing the ending numerals. This amount is relatively high in comparison with the much larger size of breach involved 190 individuals’ personal data being disclosed to the public in the decision re: GMM where the same amount of penalty was issued. The latter found desirable post-breach behaviors and cooperative attitudes. Similarly, considerably high amount of penalties found in the case of Re: Social Metric, in which the PDPC found the company delayed remedial responses and uncooperative attitudes following the breach and imposed penalties amount of S$18,000, the second largest penalties issued against organization following the highest amount of S$ 50,000 imposed for K-Box. Considering the leakage of 558 individual’s personal data unnecessarily retained on the websites operated by Social Metric with the much larger size and impact of breach found in K-box from the hackers involving the disclosure of approximately 317,000 members’ sensitive information, the amount imposed to Social Metric is considered relatively high. Also, in the decision re: Orchard Turn Development, which has been made at the same period with Social Metric and satisfactory prompt remedial action and cooperative attitudes are found, the lower amount of S$15,000 penalty was issued for the unreasonable security practices resulted in spam mail sent by hackers

\(^{189}\) The PDPC decision Re: Challenger Technologies Limited and Xirlynx, the PDPC mentioned that the respondent had taken remedial actions to inform the affected ValueClub members regarding the data breach and to rectify the mistakes caused by Xirlynx’s error. In addition, it had taken the extra precautionary step of terminating Xirlynx’s services upon discovering the cause of the data breach, and it reviewed its ValueClub communication processes to prevent a recurrence. (para. 12), cooperative to investigation (para 37c), The Commission also notes that Challenger had taken several proactive steps to remedy the breach, including engaging a new IT vendor and hiring the services of a data protection consultant. Most are business contact information not protected under the PDPA.

\(^{190}\) The leakage included 214 sensitive data of members being disclosed to other members by the email sent from the institution. The PDPC found that: Most are business contact information (generally not Personal Data under PDPA); prompt action taken by respondent to recall the emails though enabling to recall total emails sent. informed the PDPC of the data breach voluntarily and was cooperative during the investigation.

\(^{191}\) In assessing the breach and the remedial directions, the “mitigating and aggravating factors” are: Both shows the lack of awareness and knowledge of security protection i.e. being unable to identify the cause of breach, not being cooperative and forthcoming and display a cavalier attitude providing incomplete responses.

\(^{192}\) The PDPC decision Re: Fu Kwee, It found “Fu Kwee’s disregard for its obligations to appoint DPO or put in place the policy after receiving notice from PDPC” and “not forthcoming in providing information to PDPC” and “anyone who had the exact URL or who had correctly guessed the parameters could potentially access all the personal data of Fu Kwee’s customers.”
to 24,913 subscribers. How the PDPC weighs the respondent’s willingness factors along with other factors in assessing penalties needs further analysis.\textsuperscript{193}

It is noticeable that these languages containing the PDPC’s preference on the respondent’s attitudes also found in other cases involved individual consent breach such as “candidly admittance of breach in the first place” found in the matter against individual data broker, discussed in Chapter 3 and Appendix A.

**C. Comparison on the FTC and PDPC Post-Breach Responses from Cases**

There are divergent pattern of the post-breach responses from organization recognized by the FTC and the PDPC through data security breach cases. On the consistency aspect, the pattern is clearly seen in the PDPC cases from the first series of decisions up until February 2018. On the contrary, such pattern does not consistently appear in the FTC cases.

In term of normative implication regarding post-breach responses, the normative implications from the FTC are unclear as to whether the FTC mentioned as a fact or norm, and in some cases where it contains normative values, no consistency in confirming such values. From the PDPC decisions, most cases demonstrate the clear meaning of what are desirable is clearly distinguished from undesirable practices. The status given in term of mitigating and aggravating factors, though not consistently found in every case, can be inferred from the organization from what PDPC mentioned as they considered it as part of the assessment of the breach and directions given. Besides, normative meanings are clear and consistent, such as in the meaning of “promptness” in responses, and what is remedial action in “extra” or far below what is expected from the PDPC viewpoint. The PDPC by applying these criteria only to organization, not its intermediary, clearly signal “who” should deliver the breach notification and remedy to individuals.

**III. Evidence from U.S. and Singapore Organization Interviews: Worldview and Practices**

Within the limitation of the study materials and methods discussed in \textbf{H.}, the evidence from U.S. and Singapore Organization Interview demonstrate some meeting points of their privacy worldview and practices of post-breach on trust. First is a meeting in the language of consumer trust in privacy. Second is the way they similarly describe the ongoing relationship with individual that shapes their decision-making in rendering post-breach responses. The risk and uncertainty that comes with the post-breach responses from legal compliance also mentioned, though the some respondents in Singapore touched on the assurance aspects, that they would be understood from the enforcement agency when trustful post-breach responses have been delivered.

From a vertical view in connecting to legal ideals, principles and enforcement style, the interviews demonstrate the alignments towards the same direction in the Singapore to set the focal points on trust relationship as function behind better privacy practices. The U.S. brings a

\textsuperscript{193}So far, in addition to the prompt notification and remedies provided by the respondent, the PDPC considered other factors such as the nature of breach circumstances (i.e. sensitivity of data), intent involved and degree of facilitating breach, number of affected individuals and the wider impact from breach.
contrast picture of nonalignment; the disagreement between legal ideals on privacy rightness and the organization’s worldview and practices on the ground that flows into conforming and directional way to join with other jurisdictions. The implications for the function of law in harmony with its instruments on the ground will be discussed in part III.

A. Excerpt from U.S. Privacy on the Ground

The interviews conducted on the chief privacy officers of the U.S. based firms, identified by peer as leaders in privacy fields. They worked for the firms in major sectors such as health, financial service credit, and the unregulated sectors; half of those in technology sectors.

Implications for the non-legal factors that drive beyond-compliant behaviors: The excerpt of the interview with U.S. CPOs from ‘Privacy on the Ground.’

Privacy on the ground (2015) study's finding puts forward that the ambiguity of the nature of privacy and the FTC Section 5 broad terms of "unfair" and "deceptive" allows the agency's interpretation to continuously evolve through the dynamism of technology, market, consumer expectation. The interviewee described the unpredictability of the FTC, the aspect of losing trust and subject to the enforcement induces fear and risks aspect for the corporation as what keeps the firms "to be above and beyond." The state laws on security breach notification also provide an incentive for the changes the corporate behaviors, which, together with the media advocate, has promoted privacy consciousness in joining with the already existing social and technological changes.194

Through the CPOS, the study also reveals the corporation's understanding of privacy that together with the professional activism also shapes the proactive privacy practices on the ground. The interviewees mentioned managerialization of privacy by "translating of privacy into regular business language" inside the corporation through the work of privacy professionals.195

The study’s frame on privacy consumer expectations approach derives from the privacy-related values expressed by the interviewees. The language of trust has fundamentally emphasized, such as "privacy equates to trust," "correlates to trust" and is a core value associated with trust.196 Other key words found are, for instance, reputation, transparency, and honesty.

The following excerpts from the study also indicate the relationship of trust and consumer experience that influences the organization's worldview on trust and the operationalization of privacy based on individual experience.

195 Id. at 86.
196 Id. at 66.
Consumer expectations arise from the act of the firm themselves such as “ability to deliver those consistent compliant experiences, you know, that is trust.” “It is not necessarily beginning from a privacy-as-fundamental-right point of view” but rather reflects the notion of “privacy as important to what we do for a living.”

"The end objective in my mind is always what’s the right thing to do to maintain the company’s trusted relationship with our employees, with our clients, with any constituency in the society that has a relationship to us, which is probably pretty much any constituency."

"Is that consumer going to be comfortable using online banking in the future or any other new online service that the bank offers, and how many friends is he likely to tell? or, will "they start wanting to shut down the relationship, in other words, shut off the information, complaint to the FTC, send nasty letters and threatening lawsuits about email and that kind of stuff?"

The rhetoric of consumer trust becomes "something of mantra" internationally the company ...understands that trust plays a key part but isn’t able to kind of codify what...trust looks like.”

Note

It is noteworthy that I find that U.S. consumer expectation frame when speaking in the Singapore context should be viewed from individual experience, for better representing the corporation's understanding of privacy in Singapore. As explained in the next section, unlike in the U.S., data privacy in Singapore is quite a new culture, not only for employees but the individual consumer who may not at first understand what to expect from it.

Put together the view from the interview respondents and the stronger influence of SBN laws on beyond compliance corporate behaviors suggested from the literature in U.S., the FTC role works in a limited way to connect with the force on the ground. The FTC interpretation has been neither consistently recognized post-breach responses, nor clear normative implication on these post-breach behaviors. Together with the uncertain and non-directional choice of enforcement, the situation presents too much risk, less assurance, for organizations to take in the post-breach responses. Setting aside the legal influence from the SBN, these FTC cases with post-breach responses from high visibility consumer-facing entities in the retail industry could resonate to the statement from the respondents, "The biggest privacy value is part of brand." Evidence of post-breach response from a small private company in the cases of insider breach may hint some other forces on the ground beyond public reputation that directs the corporate beyond-compliant behaviors towards individuals, which requires further in-depth research.

113

---

B. Excerpts from the CLTC Memoranda on the Role of DPO in Enhancing Trust Relationship in Singapore

The DPO Interview: Evidence on Organization’s Worldview on Trust and How it Influences their Post-Breach Responses

The interview with the data privacy professionals demonstrates the organization's worldview anchored in customer trust plays a significant role in how organizations determine their post-breach responses towards an affected individual.

The interviewees from Singapore are 17 data privacy professionals in the organization operating in Singapore. Ten interviewees have the formal title of data protection officers (DPOs) of the organization; the others have the title of regional privacy officer, regional director of the public policy or privacy legal consultant, or the informal DPOs by default. Ten interviewees have other titles in the organizations such as auditor, chief information security management, CEO, COO, legal. Interviewees’ organizations provide financial products for business and consumer, consumer brand, digital and technology products and educational service. There are ten global firms, one regional firm, three cross-bordered firms and three local firms.

The organization understands privacy as individual subjective interest or preference. The interviewees, an operational DPO of a digital finance company, mentioned: “I mean we’d like to think things as privacy, right? But actually, it’s a lot more about customer experience as well.” The questionnaire answer also reveals that consumer trust and company reputation are ranked as the top-two answers the interviewee found most relevant when determining breach responses. A DPO and CISO of a luxurious consumer brand expressed: Not only company reputation has been affected, you have trust of customers in addition to company’s reputation.

The interview reveals that trust has ingrained in the logic of organization and their way of thinking about consumer preference, and what kind of actions could please and gain trust from the consumer. Specifically, what individual will react to the organization when receiving the post-breach responses are the key factors taken into account when deciding whether to notify or not notify breach. The same DPO and CISO mentioned: you have to think forward if you have to inform them, what’s gonna happen.

The organization’s fear of bad individual experience from receiving breach notification are coined in term of "information fatigue," "being desensitized," "unnecessary panic," "misunderstandings." An operational DPO in a financial product company points out the gap between the public and the professional view on breach notification: The reality is we’ll think that Company A [that notifies breach] is so transparent and it’s so good, but the public doesn’t know that they are being so transparent. The public may think that it just seems like they are careless, don’t have good policy or a good control whereas Company B that does not notify frequently will seem to have a very solid control framework. In different context, the same

198 The same DPO continued: “And whenever they look at us during a transaction or interaction, they will use that lens even if they talk to our people in an unrelated matter. They will think of us as a careless institution, which is something you definitely don’t want.” This also implies the ongoing relationship aspects concerned by the organizations from unsatisfactory individual experience.
DPO mentioned: “Data privacy law has been around for long time from the EU and US. Singapore is quite new.” While this indicates the lack of norm for breach notification practices, which call for the industry and the lawmaker to establish a more uniformed baselines, on the other hand, it also points out to the current risks borne by companies that decided to notify breach to the individuals among the unsettling individual perception of organization’s breach notification. From this view, trust relationship could be the drive behind the proactive privacy practices in notifying breach and remedies to individuals rather than fear of reputation loss.

The interview also found that trust is raised in the contexts associating with what is gain from notifying breach whereas reputation is more associated with the loss from notifying breach. From the organization's view, the individual appreciates the directness in learning of the breach from the organization itself, which relates to the value of trust and caring. A DPO and CISO of a local financial product firm asked: "how can I trust you if data leak and you don't tell me? They want to learn from us first that we care about their personal data. Definitely, about trust." This also points to the underlying relationship between organization and individual that plays a role in post-breach responses. At least, in the organization's worldview, the consumer would perceive them as a trustworthy party to a relationship.

Besides, the interview reveals that trust has ingrained in the logic of organization, their way of thinking about consumer preference, and what kind of actions could please and gain trust from the consumer. Many interviewees explained by putting themselves in the individual's shoe in predicting which behaviors will receive a desirable reaction from individuals. A DPO Team Lead of a financial product firm provided that: “We need to get the right response expected from the customer. If the company tells earlier would create trust, but also wonder why it happened so need to reassure that it will not occur again. I put myself in the individual's shoe. I wanted to know what kind of leak and what have the company done, so the customer would feel better later on. Another Privacy Consultant of E-Commerce platform agreed that it is not about notifying or not notifying but how to---the manner of notifying breach.

By conditioning their responses upon the ideal of consumer trust and maintaining individual experience, the organization has placed themselves under the influence of the relationship with the consumer, and engaged themselves in protecting the individual interest in the characteristic of "trust relationship." From there, trust relationship does not address privacy as the objective level, but at each individual interest injured at the time the breach occurs. As a Regional privacy counselor of a global financial product firm admitted: we are the culture of making complaints. The operational DPO of a global digital financial product firm added: Many times they just want to complain about what happened to them, so then it comes to the point that they just want the voucher or something. A privacy legal consultant in global e-commerce platform said: Now, it’s not just the media that do PR, but consumers themselves.”

This nature of behaviors corresponds to several PDPC cases where the complaints were made by the individuals who were disclosed to personal data of the other customer, and reported the agency to investigate the company's practices despite what appears to be a small insider breach caused by employees with very limited exposure to one person unmotivated to commit crime. This culture of complaint adds more forces for the organizations to seek resolution within
the relationship, until satisfactory individual remedy has been provided rather than the small penalties provided by the PDPC.

A Conclusion: Trust as focal points in Language and Venues for Action

With the evidence of organizational beyond-compliant behaviors from the post-breach responses found in the PDPC cases and how privacy works inside the organization through the data privacy professional lens, this momentary situation in the country of privacy non-right basis demonstrates the strong ‘culture of complaint,’ and the trust relationship works behind the beyond-compliant behaviors of the organization.

An open-unfinished gap and subtler function of law and enforcement have been sought out by regulator and lawmaker to tune in organization's interests of consumer trust and allows its managerialization of privacy to take place in the direction towards better privacy protection and secure consumer confidence in the system.

C. A Dialogue between the U.S. and Singapore Excerpts

Similar views of privacy based on trust shared by the U.S. and SG privacy professionals suggest trust relationship as a communal language of privacy for organizations in their interaction with individuals. Besides, trust relationship could be a non-legal factor that adds force to drive beyond-compliant behaviors towards better privacy protection. To clarify, here “better” means (i) broader privacy interests including subjective interests and individual experience are taken into account by organization in rendering post-breach responses, (ii) protection goes beyond individual expectation at the time of sharing data with organization to what injures at the time of the breach (iii) promptness of remedies. The PDPC decisions demonstrate evidence of organizations’ performing post-breach responses beyond legal requirements, such as prompt breach notification and remedial act to individuals, which are encouraged by the PDPC. This supports the claim that the Singapore’s privacy non-right basis, open regulatory design and the PDPC enforcement style, discussed in Chapter 2,3, which when works in tune with, and promote the trust relationship on the ground could lead to better privacy.

While such organization’s post-breach responses are neither clearly or consistently found to be encouraged by the FTC, but rather significantly influenced by several states mandatory SBN laws provides incentives for organization to enhance its privacy practices, similar view from trust relationship lens shared by the organizations in U.S. and Singapore put forward the possibility of organization’s function on trust relationship as a drive despite the asymmetry between the fragmented legal system in the U.S. and the more streamlined practices developed by organizations across different jurisdictions.

I did not object the introducing of mandatory law into the privacy legal landscape, and agree that legal mandate could be a necessity in certain situation to create some assurance and level playing among businesses in compliance. Therefrom, my view agreed with Privacy on the ground’s study for the need of a more effective and uniform breach notification requirements in U.S., which should strike a balance between ensuring a proper manner of communication as a remedy and not creating a too burdensome duty of increased operating costs for organizations.
Though, my caution is on the legal constructions, which should not interrupt the underground of the trust relationship workforce. I also encourage the consideration of leaving some gap and apply upside motivation in align with the U.S. organization’s interest to promote better privacy.

This dissertation looks into the site of Singapore for answers to the similar questions in the Bamberger & Mulligan’s study. It found the alignments in the corporations’ understanding of privacy and approaching privacy issues as strategic acts, as seen in how they decide to respond in post-breach behaviors. Data breach notification was considered as part of internal control and risk-management function. Organizations shared the understanding of privacy as individual interests.

What drives organizations in Singapore to adopt privacy-proactive or beyond compliant practices? The breach notification and post-breach remedial acts were not mandatory under the PDPA at the time of the interview and the PDPC decisions were made, allowing them to be interpreted as proactive privacy practices in Singapore. The interviews with DPOs demonstrate that the drive for adoption such privacy-pro practices comes from the ongoing relationship with individuals. The similar fear from losing trust and reputation loss raised by the interviewees in both countries relating to data breaches and responses, I find the process described from the Singapore’s excerpt does not lead to the reputation or consumer expectation as a conclusion, but individual experience. As the respondent pointed out of the un-established norm and understanding of privacy practices in Singapore in contrast to the firmly rooted and long-established notion of privacy, where good and bad reputations could be measured from privacy practices of organization. So, I find the interview reveals the underlying individual experience as organization’s stake when data is breached.

What is the role of law in shaping an organization’s privacy meaning? From this, as the interview respondents suggest the more baseline for compliance and I agree that certain baseline, regardless of forms is needed to assure industry with a defined range of mutually accepted meaning or norms on post-breach responses and communications to the wider public.

The last question is: which factors influence the corporate understanding of privacy meaning and the urge to advance it? The Singapore excerpts bring out the consumer reactions and how an individual perceives his/her data breach experience and the post-breach responses does influence the way the corporate calibrates the meaning of privacy. The interview respondents also refer to the accepted meaning in the society at the time of the breach. The un-established norm of organizational response to privacy in Singapore rather points to organizational decision-making process that is conditioned by consumer reaction, the way an individual interprets their experience on data breach at the center point of an organization’s concern, and the way they care to control it through better experience in post-breach responses towards with the individual in maintaining relationship.

From these findings, I put forward normative claims that legal design for privacy should be framed on the enhancement of these organizational interests in a trust relationship. This claim meets Waldman’s ‘Privacy as Trust’ (2018) from the other side of an organization’s stake in
maintaining consumer trust. I had clarified in the research motivation on the different view and proposition on privacy from trust relationship, not trust. My focus diverges from Waldman, among others, by viewing trust relationship from the organization’s perception not individual perception. Furthermore, I focus on that law in promoting trust norm should not limit the protection to an individual’s expectation at the time of sharing data with the organization, but to individual interests jeopardized at the time of the breach due to the relationship interest. The law should not act as a hindrance to the organization’s emerging practices driven by a trust relationship function, in which post-breach remedies reach beyond an individual’s expectation at the time of sharing data to all subjective interests at the time of breach.

In the end, I claimed that the law could utilize organizational resources, uniformed interests and practices driven from trust relationships to promote privacy, not for the society as a whole or at an objectified level, but at each relationship or intersubjective level. The latter is possible through the function of trust relationship.

III. An Analysis on the Trust Relationship, the Alignments of Ideals with Reality and the Dialogue with-in the Unfinished Gap

A. Implications on Trust Relationship as a Drive for Beyond Compliance

While the PDPC has taken into account the post-breach responses by the respondent as aggravating and mitigating factors in determining breach and penalties thereof, similar responses have not been consistently found in the FTC cases. The meanings of such behaviors to the FTC remains unclear whether the presence of such facts purports to demonstrate as part of respondent's failure in providing reasonable security practices. This correlates to the rise of beyond compliance behavior in terms of extensive remedies and notifications made to affected individuals in Singapore, and the few presences of similar behavior in the FTC decisions and orders. Explaining from the compliance theory, the PDPC by declaring their criteria of mitigating and aggravating factors has created business stakes in adopt beyond compliance behaviors despite legal requirements. Meanwhile, from trust and assurance perspectives, the PDPC has provided some assurance to the organization that their beyond-compliance behavior will be considered on balance with their lack of adequate safeguard measures that resulted in breach. Such assurance has reduced inherent risks borne by the organization when deciding to notify breach, while encouraged positive or trustful behaviors to the consumer and strengthen their trust relationship. It is the assurance provided by enforcement agency that further allows the organization to thrive in delivering behavior in favor of consumer while negating of costs arisen from doing so. It leads the organization to open for trust in consumer relationships and cooperation with the agency.

Reconnecting to the ideal of privacy and legal characteristics in both jurisdictions discussed in the earlier chapter, the PDPC emphasizes the direct relationship between the organization and consumer, and the principle of care emerged from the relationship basis besides the accountability principles. The FTC and current laws governing data security practices and the FTC have neither made any distinction about organization and data intermediary, nor delineating duty and liabilities have arisen between them on personal data treatment. These fragments existing in the design and enforcement have provided an uncertainty in organizational
compliance. While, among others, accountability has been the fundamental principle in the U.S. data security regime, the FTC practices have not yet realized or assured through the in term of remedies, reputation injury and breach notification. With the lack of emphasis on post-breach remedial and corrective behaviors toward the consumer, the trust relationship between organization and individual has not been encouraged.

With the level of assurance provided under the Singaporean personal data protection law and the agency's discretion in enforcement, business parties are more open toward taking risks in acting to regain consumer trust and then promptly remedying consumer trust by notification of the breach and offers remedies to the affected individual consumer. Such strategies would be an alternative for the U.S. to consider to fill in current fragments in the regime and provide more assurance for the business to initiate trustful acts toward the consumer.

**B. Alignments of Ideals and Reality: Law, Enforcement and Trust Relationship**

These privacy proactive practices of organizations in term of promptness in notification and extra remedies towards affected individuals after the breach have been witnessed in the PDPC cases as well as on-the-ground practices of the organizations from the interview excerpts. These post-breach responses initiated by the respondent on the basis of non-mandatory law imply the non-legal forces on the ground from individual-organization trust relationship that allows organizations to take risks and uncertainty to apologize, notify breach and remedial actions following the discovery of breach with the view to maintain affected individual interests in the ongoing relationship with the organization.

The PDPC, by recognizing these desirable trustful behaviors provided to affected individuals as mitigating factors in determining a breach and the penalties, speak to the existing organizational interests in consumer trust and the stake of losing it, thus induce the coordination from organizations. The upside and downside forces from the PDPC mitigating and aggravating factors for the desirable and undesirable post-breach responses assures the organizations with more certainty and mitigates the inherent risks in deciding to perform those behaviors towards affected individuals following the breach.

The Singapore law and legal ideal of no-privacy has set the venue on envisioning this direct ongoing individual-organization relationship, preserve and nurture it though the language of trust and the principles of reasonableness interpreted from the PDPC through cases discussed in chapter 2 and 3. In brief, those venue and interpretation of the Singapore Personal Data Protection Act and the commission has constructed the open space for subjective interests and social dimension of privacy such as trust, embarrassment, reputation, and social stigma, not limited to the market definition, to inform protected values of privacy. Intent, ongoing and direct relationships involved in breach play part in determining which capacity the actor perform in data treatment and the obligation and liabilities arisen among actors. The forms of law structure, principle and enforcement set in the alignments to reassure, direct and nurture the flow of trust relationship between organization and individuals.

My arguments for protecting privacy through promoting trust relationship align with Hartzog & Richards’ proposal. The Singaporean exemplify a case for privacy design for
promoting trust relationship, in which the ideals – hard and soft legal structure and gap, motivating forces and regulatory styles and specific case enforcements as in Chapter 2 and 3 – provide a specific way as to how the law can build upon organizational infrastructure and rationale of a trust relationship to better remedy individuals from a data breach. Humanistic dimension of privacy is also observed in interpretation of reasonable personal standard in compliance with the PDPA.

The evidence from the FTC cases does not reflect such view on the U.S. ground where there are more established sense of norm, meaning of privacy and beyond-compliant behaviors among organizational actors. In a small number of cases where those facts on post-breach responses present along with the failure to provide reasonable data security practices, depending on the contexts they found, the message sent from the FTC casts a cluster of unsettled meanings to organizations. These vary from the implications for the aggravating nature and impacts from the undue delay or not alerting individuals of the breach, just mentioning as facts, or praise from a commissioner in the statement. Such frame of privacy on-the-ground as consumer expectation approach, on the surface, appears to resonate within the FTC’s interpretation and enforcement on the reasonableness of data security practices under unfairness and deceptiveness basis of Section 5 of the FTC Act. However, the FTC measurement on consumer expectation and reliance at the time when choice has been made on consuming products and services does not align with actual consumer expectation or no-expectation but subjective interests on the ground, and relational trust that works behind current privacy proactive practices on the ground. The excerpt from the U.S. privacy professionals interview points to similar the non-legal factors hints on the relationship of trust, along with other forces, directing beyond-compliant behaviors towards individuals. With the current limits of the FTC in motivating organization to convince on the right approaches they envision, the law and regulator could consider realignment with the language and action on relational trust on the ground to add more coordinative force for compliance. This evidence of breach notification from companies with the ongoing and direct relationships with affected individuals suggest the drives from possible existing trust relationship norm on the ground.

What is at stake from the organization’s worldview operated from the trust relationship viewpoint is bad individual experience at the time of breach. The interviews of the DPOs in multi-national corporations including U.S.-based firms show that organizations conditioned their post-breach responses upon the future reaction of an individual when such a breach notification is received. From this viewpoint, the dynamics of the relationship and the organization’s worldview based on maintaining individual trust are seen to be communal, or a universal tool that governs parties’ behaviors.

C. Carving out the Gap and Let the Flow in: A Glimpse of the Future Norm-Adjudication in Singapore

These post-breach responses found in the PDPC cases are similar to examples of those recommended practices in its issued guide on managing data breach incidents, which is not legally binding. In the PDPC decision Furnituremart, the Commissioner emphasizes the
significance of an organization's management "to buy-in to adopt good data protection practices." It states:

“It is from this starting point – the management level – that the company’s policies and practices be formulated with data protection in mind. From there, such good data protection policies and practices can permeate down to and be adopted at the staff level of the company. … The Commission therefore highlights that management has an obligation to establish the standard of care that it expects staff to observe, communicate and train staff, and to put in place appropriate supervision and monitoring to ensure compliance. (para. 25).”

From this view, it can be seen that the PDPC has attempted to infuse the organization’s management to adopt its recommended practices in the guidelines and the recommendation in cases, which are specific practical steps or certain types of security products in order to meet the reasonable standard expected under Section 24.

The cultivation of norm on post-breach responses based on trust relationship can also be witnessed from the PDPC enforcement and the legal amendment process. The proposed amendment on mandatory breach notification regime and the public consultation in July until September 2017 also support this view. The proposed amendment, which has not yet finalized, specifically obliges the organizations with a duty to notify data breach as soon as practicable to affected individuals when it is likely that harm would occur to them. This duty is in addition to a separate duty to report the PDPC when criteria have been met i.e. the significant number of affected individuals involved. The data intermediary rather does not have the similar duty, but to report the organization when learning of breach.

The PDPC’s intention to cultivate norm on the post-breach remedial actions towards individual also reflects in the PDPC’s feedback to the public responses. The opinion from organization representatives and the PDPC agree on the "Post-breach remedial exceptions," under which organizations are not required to notify breach when the remedies and prevention have been sought to eliminate the potential risks to affected individuals. In the PDPC’s feedback to the public responses, it states clearly that: “The PDPC also intends to provide an exception for organisations which have taken remedial actions to reduce the potential harm or impact to the affected individuals. The organisation will need to demonstrate that, as a result of the organisation’s remedial actions, the breach is not likely to have any significant harm or impact to the affected individuals.”

This negotiation between industry and the regulator during the lawmaking process demonstrates that the gap was intentionally left to the organization party to exercise their


200 Despite the outlook of a more stringent approach towards breach notification, the participants and the Commission appeared to mutually agree on the "technology exceptions" and "post-breach remedy exceptions." "Technological protection exceptions" means organizations are not required to notify breach to affected individuals when the leaked data is intelligible for those who obtained. The proposed timeframe for notifying breach to individuals is as soon as practicable, leaving much room for the organization to exercise discretion.

201 Id. Section 10.6 and 10.7.
discretion in providing post-breach responses, in the form of remedial acts towards affected individuals party. Simply put, the law works to carve out the formalized rule, and let the flow of dynamism of trust relationship to pass through the carved out gap.

---

**A Conclusion: In the Benefits of Trust Relationship to Privacy**

Law should not hinder trust relationship functions and norm emergence from such relationship but promote it. The evidence from the interview and the cases analysis provides implication on the functions of law interacting with organizational behaviors when performing beyond-compliant behaviors to individuals. I put forward that law regarding data breach notification and remedies can achieve beyond the purpose of bad publicity to provide incentives and induce organizational trust behaviors towards individuals when it opens the gap for organizational discretion and speaks in attunement with organizational interests or values in better individual experience. That is how law utilizes the norm existing on the ground and further catalyzes it to deliver individual well-being ends.

Data breach notification is and should not be necessarily labeled with a bad reputation, but also a chance to demonstrate good values of the companies to remediate and recover individuals from the situation. Law and its normative character can take this opportunity of the unsettling public views towards organizational breach notification behaviors to clarify and differentiate what is very bad from not so bad practices. To such ends, law and regulator can take into account the post-breach responses from the companies, and more upside force to motivate beyond-compliant behaviors towards individuals. These upside forces, among others, come from when the post-breach responses speak to companies' core values centralized on *consumer trust, transparency and honesty*. It is viable that law can mitigate the perceived risks of organizations in performing these post-breach responses, not in total, but to the acceptable level that it triggers such behaviors. In this circumstance, the law, when not mandating or fixating with a negative perception, could become extra points to draw those companies their core values meet when adopting these necessarily and responsible post-breach behaviors to beyond-compliant practices.

*The Role of Law in Promoting Privacy: The Dialogue between the Alignments and the Gap*

The law can promote the norm on desirable post-breach behaviors towards individuals by introducing some baselines for post-breach behaviors in order to assure organizations with the level playing field with their peers and communicate to the public of the meaning of what are desirable post-breach behaviors. By not finishing the gap and instead persuading the organization to *fill in* through exercising their discretion in benefit of the individual trust, the law can pay less effort and achieve beyond its rigid command-and-control function through the existing individual-organization relationship.

From this function, the law is neither viewed from the outside or inside organization, nor as upward or downward force, but at the meeting point in a conversing space with the organization. Legal ideals do not posit at the higher ground, but as part of organization ideal and
logic that law could tune in. The law normative characteristics form and are part of the passage of the flow of organization experience to serve the individual well being ends.

A case of Singapore is evidence on the congruence of values between the organization’s worldview and the legal ideals of no privacy, but trust relationship. In my view, individual privacy protection also benefits from the promoting the relationship of trust between the organization and individual party, which are more established in the organization logic than the privacy culture itself. Explanation G-2 could explain the situation in Singapore from compliance perspectives.

Not forcing others to follow their ideals and legitimacy, law can speak in relevance and attunement with an organization’s interests, which perform more than a symbol of rights to a coordinating function of the law. The law in its rigidity as a symbol of rights performs as a reminder of agreed meaning, content, and upholds rightness and assurance to parties in navigating in accordance with the law. In its strategic mode, the law can negotiate with organizations and assign motivation for better privacy practices towards individuals.
Chapter 5
Lessons for Thai Personal Data Protection Law

Chapter Abstract

Chapter 5 brings the situation of data security breach in Thailand into contrast with those of the U.S. and Singapore. Thailand represents a unique case, positioned as she is, situated at the onset of a political change to a democratically-elected civilian government, the social movements towards liberation, and the economic reforms for a digital economy. The data security protection reform has both symbolic and substantive meanings to the government, business and individual parties. First, the personal data protection legislation has been the major battleground for the government and civil right activists. It symbolizes the extent of control and freedom the government has on individuals in the democratically authoritarian system. Besides, the Thai Personal Data Protection Bill (PDPB) is at the centerpiece of legal reform for driving the government’s proposed digital economy plan and the protection of consumer trust in businesses and e-commerce. Thus, the interplay of current forces and tensions demands Thai regulation to meet the dual ideals of privacy: the democratically privacy rightness and the need of promoting underlying trust among parties.

Thailand can learn from the U.S. and Singapore cases. The lesson from Singapore suggests the amendments of the Thai Bill to embed the venue for individual-organization trust relationships to arise with the enforcement agency infusing of right motivation that speaks to organization’s interests in consumer trust. The lesson from the U.S. FTC consumer protection approach to data security through section 5 enforcements also fills in the gap of the pending law, raises the privacy awareness and allows privacy remedies through the interpretation of Thai consumer protection agency. Put together, Thai data security landscape offers a hybrid view that reconciles the two approaches of increased individual self-control and promoting trust relationship.

Introduction

Despite the emergent threats from widespread data security breaches, Thailand has not yet passed the Personal Data Protection Bill to regulate business conduct and protect individual rights to privacy and personal data guaranteed by the Thai Constitution B.E. 2560 (2017). As a result, individuals receive no remedies for damages caused from a breach and start to lose trust in both the government and businesses.

This chapter borrows these lenses from the U.S. and Singapore to apply to the data breach situation in Thailand, aiming to optimize a platform for protecting individual rights and personal data, while also promoting trust relationship and cooperation among actors in Thailand. To that ends, this chapter examines to what extent would the U.S. and Singaporean approaches meet the needs of the country, situated within the current forces and tensions in political, social and economic realms. Furthermore, what kind of adjustment needs to be made to make these borrowed functions work in the specific conditions of Thailand to meet those ends?

The case studies of the U.S. and Singapore data security protection represent divergent regulatory design approaches and enforcement styles that are tailored to fit different societal ideals, individual concerns and the nature of organizational behavior in the specific contexts of
each jurisdiction. The transplantation of the lessons learned from the U.S. and Singapore to data security protection gives rise to the main considerations as to whether the transplanting of ideology, concept, values and ways of operationalization would be well-received, and would yield desirable outcomes on different soils or otherwise. Therefore, this chapter begins by exploring the similarities and differences as in the existing platform, actors’ attitudes and behaviors, flows and force within the space to ensure the viability and the smooth translation of the understandings from the U.S. and Singapore into the Thai landscape.

This chapter collected the evidence from the PDP Bills (the 2015 bill and the 2018 bill), legislative history, the public hearing and commentaries, the news reports related the issues and the excerpts from the interview of Thai startups in the digital lifestyle and consumer financing products that also operates in Singapore, and a global technology company that also operates in Thailand. First, as to the existing platform, the study found that, there are well-established platforms for consumer protection regulations and the half-finished construction of the Personal Data Protection Bill in the Thai landscape. Both have many similarities to the FTCA and the PDPA respectively, and provide good locales for the transplantation. Second, Thai consumer and local business perceptions on privacy and the awareness level are significantly different from their U.S. and Singapore counterparts. The media reports reveal relatively low consumer privacy awareness despite being relatively high internet and online social activities. Consumer are unaware of how and for what purposes the their personal data will be used by business party, the risks arising therefrom, and way to assert their rights. The privacy policy and terms of service agreements are similarly found on the company’s website, but often being disregarded by consumers who rely on businesses to not exploit their personal data.

From the view of business party, the interview excerpts suggest that the privacy culture or responsible data privacy practices has not yet been integrated into the business governance. Businesses are not aware of individual rights to personal data; they do not understand their duties and responsibilities to protect personal data of individuals and to not exploit for their own use.202

202 Thailand Internet User Profile 2017, the survey report of Thai internet users behaviors, Electronic Transactions Development Agency (Public Organization) (ETDA) published August 24, 2016. https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2017-slide.html As of 2016, Thailand has over 40 Million facebook account users. As of July 2016, from 25101 respondents, average 7 hours daily spent on the internet , 63.5% increased from last year use for entertainment and online shopping 2016, 64.1% more awareness regarding online posting, profile sharing and chatting, 59% not open email from unknown sender and suspicious links on website, 34.5 regularly password changes and enabling double authentication. Most popular online activities are social media (86.9%), search (86.5%), email (70.5%), tv program and music (60.7%), purchasing products and services (50.8% rising from 2016) Thai internet users are sharing 0.8 % of world internet users. What are the most frustrating Internet issues found by respondents in recent three months? online advertising (66.6%), slow connection (63.1%), disconnection (43.1%). Technical internet assistance (39.6%), junk email (34.2%), computer virus (21.5%) unreliable resources (11.9%), privacy intrusion or exploitation of personal data (11.0%) fraudster (6.3%). Over 40% of respondent did not shopping online did once a month. Most reasons for not shopping online are 51% fear of fraudster, not physically examining products (39.9%), no product of interest (33.9%), prefer shopping walk (31.1%), no face to face meeting with seller, 85% shopped online because of easiness, promotion, cheaper price (53.4, 51.4, 49.7%) High reputation of the seller (18.7%), safety (18.2), trustmark (16.9). Most transactions (59-77% in average) are below 1000 Bath (approximately $30) except in finance and investment (38% spent over 10,000 Bath (average $300). Payment methods are credit card (35.1%), online transfer application (31.9%), ATM (27.1), Banking website (22.6%). Types of products and services are investment and finance (4.8 times), downloading (4.9), entertainment (2.5), travel and leisure (2.5) fashion (2.4) online food order (2.4), commodity (2.3), health and beauty (2.1), IT products (1.9). Channel for report issues: 86.8% government entity, 59.8% website of product and service provider, 24.0% authority, 19.4% comment in online social community. Most does not complain because 56.7% petty amount of loss, 53.8% not worthy of time, 36.2 do not know where to report, 32.7% do not know procedure to lodge complaint. https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2016-th.html Thailand Internet User Profile, August 24, 2016.

203 The cybersecurity risk management plan has been formally recognized by the executives and implement into policy and practices. Employees in some departments (not organizational-wide) are aware and informed of the cybersecurity risks but has not
The case of recent major breach has demonstrated that the company’s website contains the user service agreements and privacy policy that includes personal data protection. However, whether such broken promise provides basis for affected individual to claim from data breach has not been widely discussed among Thai scholars, lawyers or the press.

Third, the press and public vigilance have played a limited role in forcing businesses and government to address the issues as well as in educating and raising individual awareness. Some successful attempts are seen in the recent major data breach case in April 2018, discovered by the independent cybersecurity researcher, who promptly warned the telecommunication companies on the leakage of their customer’s personal data from the unencrypted storage, but did not receive responses until he posted on his personal blog and received attention from the public and the media. The telecom provider made a public statement apologizing about the incident and blamed the ‘hacking activities’ involved with the leakage, which soon followed several technologist’s critiques on the company’s own weaknesses. The case was brought to the attention of the telecom regulator, without much news report on the investigation progress.

It remains unclear as to which enforcement agency has jurisdiction regarding data security and privacy. There are specific industry legislations that touch on privacy and confidentiality of consumer data and some overlapping jurisdictions among them. In the recent case, National Telecommunication and Broadcasting Commission (NTBC) claimed its jurisdiction over consumer protection on the incident caused by the telecom provider. The Thai consumer protection commission does not dispute this claim and remains silent. The investigation is not open to the public, and no further updates on the case have been issued from the agency at least three months since the discovery. The uncertainty and non-transparency of the procedures has presented more hurdle for individual to complaint and seek remedies through formal legal venue.

The existing platform, actors’ attitudes and behaviors, flows and force within the Thai personal data protection space presents a situation that needs immediate responses from the legal reform and solution to bring in the order and promoting trustful business behaviors towards individuals. On the ideal level, Thai privacy stands on the two flowing streams to promote democratically privacy rightness and the country’s social and economic goals to promote trust in commerce. Taken together, the right design should symbolically promote a sense of individual control on personal data, while substantively persuading business to be responsible for consumer trust and proactive in adopting safeguard measure to prevent the breach and provide remedies.

Part I provides an overview of data security in Thailand: the events related to the issues on data privacy and security breaches, the responses from Thai regulator, business and individual actors to the breach, and the relevant legal platforms to address the issues. Part II-A compares such responses to the data breach incident with their counterparts in the U.S. and Singapore to provide an estimation of capacities and limits when applying the lessons from the U.S. and Singapore to the Thai scenario. Part II-B analyzes the characteristics of potential Thai regulations
in comparison with their counterparts found in the U.S. and Singapore, to identify the gap needed to be filled in and the extended result from the transplanting of each approach into the Thai context. *Part III* proposes a hybrid view through the venues of the FTCA-Plus and the PDPA-Lite, which together would deliver both ends of personal data protection in Thailand.

---

### Part I An Overview of Data Security in Thailand

This section begins by putting into a frame a data security breach situation in Thailand and its implications for the Thai political situation and the blueprint of country’s digital economy. The situation demands the regulatory reform to introduce the symbolic meaning of individual privacy as much as the substantive privacy protection. Next, it brings into the view of the existing regulatory landscape that addresses the issues.

#### A. Data Security Breach Incidents in Thailand

1. **The Sequence of Cyberattacks on the Government Database**

   Since the military coup in 2014 until the present, the media have reported several security attacks against government websites and databases, which caused the leakage of sensitive personal information such as national IDs, passport numbers, a prisoner database and health information. These acts were claimed by the hacker groups as retaliations for the Thai government’s proposed Single Gateway project in 2015, a project aimed at monitoring information activities by cutting down the existing 12 gateways for information sharing activities to only one gateway controlled by the State, the model found in Singapore and elsewhere in Middle East Asia.\(^{204}\)

   After the Single Gateway plan was proposed, controversy erupted concerning the government’s attempt to intercept and conduct surveillance to control and suppress anti-government activities and free speech movements on the internet. The sequential cybersecurity attacks on the government database caused government websites to shut down. The groups also attacked the state-owned company, CAT Telecom Plc, which was then positioned to be the future gateway controller, and subsequently disclosed the CAT customer login IDs and passwords, national ID and numbers.\(^{205}\) The attacks together with opposition from the internet providers, the IT industry and IT specialists concerning economic loss from losing trust from foreign investment and the internet slow-down issues resulted in the government’s abandonment of the project. It followed from these incidents that the amendments to the Computer Cybercrime Act were passed to strengthen the regulation on cyber misconduct and impose harsher penalties.\(^{206}\)

---


The cyberattack on the government database was employed by several groups as retaliation to show resentment of the government’s policy. In February 2016, the foreign hacker groups invaded the website of the Ministry of Justice and disclosed a list containing prisoners’ information. The attack was intended to put pressure on the government to release a foreign prisoner who received unjust treatment by the Corrections Department. Other incidents involved the attack on the Ministry of Health Department and the Thai Navy. There are also other instances whereby the government was responsible for inadvertent data leaks. In March 2016, thousands of immigrants’ personal information, including photos and visas from passports, were disclosed by mistakes during the website testing performed by the IT company hired by the Customs Department.

Despite the government’s proposed plan to take charge of guarding the information security of the country, the attacks demonstrate the unpreparedness and weaknesses of the government in securing their own database from common threats, thus putting sensitive individual personal data at the risk of unauthorized disclosure. Several successful attacks and the existing vulnerabilities of the government database to cyberthreats have shaken the public trust in the government’s creditability and capacity to safeguard sensitive individual personal data from malicious actors.

ii. Data Security Breach in Private Industry

(a) A Major Breach of a Telecom Provider

In the private sector, the first major data leak incident was recently reported by one of the largest telecom providers in Thailand. This incident, coinciding with frequent reports received of massive personal data breach incidents around the world, has raised questions on the civil and administrative liability incurred by the breached company under the current Thai legal framework. These questions have called for a proper regulation on the practices of the industry on personal data.

Discovery of Breach

According to the news report, the data leak was discovered by an individual security researcher who claimed according to his blogpost to have warned the telecom operator in March soon after he found out that 32 gigabytes of telecom operator’s customer data were accessible by the public. These included photocopies of identification cards, passports and driving license, which contain photos, nationality, dates of birth, blood types and residential addresses of individuals. According to his blog post at the time of breach, there was no security to protect the files containing these data of customers. That means anyone with the URL could download all the customers’ scanned documents, stored on the AWS system that was shared with the public.

Company’s response

The telecom provider afterwards confirmed to the media the details of the personal data leak incident. According to the media release, it informed readers that the stored copies of national identification cards belonging to 11,400 customers who bought mobile packages through its online platform operated by its subsidiary company had been made public. On April 12, 2018, it told the public that the leak was fixed on April 11, 2018, (leaving the window gap for over a month after first discovery as claimed by the individual researcher). However, on April 17, 2018, the company further came out to acknowledge that the database had been "hacked" by an expert. At the press conference, the managing director of the telecom platform operator said that the expert did not have the right to access private information stored in its database, and that he used special tools in doing so to access such information. A business representative of the telecom provider told the press that the company had "a good security system". In response to the accusation by the telecom provider of unauthorized access to private information of users, the researcher told the press that he had warned the telecom provider “in good faith” to urge them to fix the issue before Thai nationals’ sensitive personal data fell into the hands of malicious actors.

The telecom provider’s representative told the public that it was working to prevent this kind of incident from happening in the future. In addition, the representative said that the company will notify, via SMS, its 11,400 affected customers to inform them about security measures the company had taken so far and open 24/7 free call for taking care and remedying the damages in cooperating with its subsidiary company to those affected from the incident. In its public statement in response to the breach, it stated that the company employed the best technology recognized globally by experts in the field so that users can be confident that their personal data receives the best possible protection.

Regulator’s response.

On 14 April 2018, the NBTC called the meeting with the telecom provider’s representatives to provide more information about the breach incident. The office of electronic commerce development notified the company’s customer that it now proceeded with the confirming the accuracy of information received and recommended the customers to check the information provided to the telecom provider and considered reported authority for the records in case of the consequences of identity theft.

In response to this major data leak incident, the National Broadcasting and Telecommunications Commission, the Thai regulator of the telecom industry, said that the case will undergo a thorough and full investigation as to whether the telecom company will receive any punishment under the law or not. The NBTC issued an order under the Commission’s announcement on measures of protection of user’s right to privacy.

---

211 The telecom provider declared mistakes led to the breach incident, published on April 17 2018.
212 Personal blog post.
214 The apology letter sent from the telecom provider to the affected customers for the personal data leakage, Thai Post, April 14 2018. https://www.thaipost.net/main/detail/7098 “Our team confirmed that we have always been taken the protection of our customers’ personal data as our first priority. And for the incident at issue, we are working closely with the world-class cybersecurity specialists, including proceeding legal measures to ensure that our customer personal data will received the highest technology and legal standard of protection.”
215 NBTC called urgent meeting with the telecom provider to provide information after the big leakage of phone contact, ID card and passport, April 14 2018. https://www.thaipost.net/main/detail/7096
regarding personal data, right to privacy and the freedom of communication and to order the company to discontinue the prohibited act, rectify and bring its measure in compliance with law.216

The direction issued from the NBTC requires that (i) the company shall provide safeguards and security arrangements including technical and administrative management measures that are reasonable to the company business, which should be at least reasonable standard considered the risk of technology development, including the auditing of its data security system by the information technology specialist; (ii) the company shall provide the unpaid channels for the consumer who may affect from the incident to monitor; (iii) the company shall take responsibility and remedy for any criminal or civil damages occurred to the affected customers; (iv) the company shall report measures taken by the company to the NBTC within the next seven days since the order has been received and every 15 days for progress.

The Commission is empowered under Section 66 in case of non-compliance with the order to impose the administrative fine of at least 20,000 Bath (7,000) per day for the continuing violation. 217

It called for the personal data protection measures to be clearly outlined by Thailand's five main mobile operators. The Secretary-General of the country's telecoms regulator told the reporter that the NBTC was looking to build its own data center to store customers' information run by a government agency. He further stated that, in the long-term plan, if the NBTC took the position of a responsible state agency, then the public would gain more confidence.

Public and media response

After the media release, the public and IT specialist expressed opposing opinions against the facts relating to the leakage as shared by the telecom provider. The IT specialist held the view that this incident did not require sophisticated tools to access information stored in the database, but a common and simple one. Others expressed concern regarding the inadequate safeguard to protect personal data collected by the telecom company. The case has received public attention as it was revealed soon after the Facebook breach incident that involved the misuse of 50 million U.S. citizens' personal data by the third-party vendor. After the public learned about the incidents, the shares of the telecom provider dropped 2 percent, against a 0.66 percent drop in the overall market.

(b) Other Data Breach Incidents: Financial Personal Information

Employee Leaked Personal Information

216 NBTC Announcement Article 10, protective measures of user’s right regarding the personal data, right to private life and freedom of communication. NBTC press release dated April 18, 2018. Available at https://www.nbtc.go.th/News/Press-Center/31952.aspx
217 Section 64 and 66 of the chapter IX Administrative Enforcement, Telecommunication Business Act (2001). Unofficial translation http://www.krisdika.go.th/wps/wcm/connect/46c2c6004b9e8d2a88096feca72b7e938/TELECOMMUNICATIONS+BUSINESS%ACT%2C+B.E.+2544+%282001%29.pdf?MOD=AJPERES&CACHEID=46c2c6004b9e8d2a88096feca72b7e938
In another instance, a data breach issue was raised against a bank employee that revealed an ATM fraudster scheme via her Facebook live. The disclosure involved the name and bank account information of an individual to whom the employee was instructed by the fraudster by phone to transfer an amount of money. In the live video, the bank employee intended to inform the public of the real scenario and how she had coordinated with her supervisor to play along with the plot to reveal the scheme to the public. The bank admitted that the disclosure of the client’s information infringed its privacy policy, and there would be disciplinary penalties for the employee who disclosed this information without the authorization of the client. The public, in response to this incident, condemned the lawyers that raised the issues on personal data breach, and sympathized with the bank employee whom the public believed was aiming to inform and warn them of the ATM fraud scheme in good faith.

First Massive Data Security Breach of the Third and Fourth Largest Local Banks: Corporate customer information

On 31 July 2018, the Bank of Thailand (BOT) issued the announcement re: Urging the Financial Institutions to Strengthen their Safeguard Measures on Cybersecurity. The announcement referred to the massive data leakage of the third and fourth largest Thai local banks. According to the announcement, some partial non-financial transaction data leaked to the outsiders; one incident involved the public information of corporate clients and another was mainly dealt with the loan requests of retail clients and some of corporate clients. No further damages has been reported from the customer. The banks promptly conducted the investigation on the issues and closed the window gap found in their system, check the related system and engaged specialist to conduct further assessment to ensure adequate safeguards. The BOT has urged the banks to adopt more stringent safeguards against cybersecurity attacks and inform data owner of the incidents including prepare to remedy when damages occur in the future with extra caution put into preventing similar incidents.

The news reported that the statement from the bank president disclosed that the names of 3,000 corporate customers using the bank’s website to provide letters of guarantee might have been leaked. The other bank’s statement from the bank’s president provided that the bank had detected the leakage of “general information” in the mortgages and personal loan online application from 120,000 retail clients.

B. The Existing Data Security Regulatory Landscape

The ongoing and recent massive data breaches in Thailand and other jurisdictions have put considerable pressure on the government and regulators to protect personal data and regulate the industries in a timely manner in the seemingly legal vacuum. In my view, however, the existing legal platforms and venues together with a newly constructed Personal Data

---

218 Bank of Thailand Announcement No. 51/2561, re: Urging the Financial Institutions to Strengthen their Safeguard Measures on Cybersecurity (July 31, 2018) [https://www.bot.or.th/Thai/PressandSpeeches/Press/News2561/n5161t.pdf](https://www.bot.or.th/Thai/PressandSpeeches/Press/News2561/n5161t.pdf)

Protection Bill have presented the Thai regulator with choices for proper means of regulating data processing businesses.

This section begins by introducing the Thai legal system and data security landscape consisting of general provisions and specific regulations for industries. Viewed in comparison with the U.S. and Singaporean approaches, the Thai Consumer Protection Act provides a functional equivalent to the U.S. FTCA with some extended features. I therefore refer to it as the “Thai FTCA-plus” approach. Recently added into the discussion of Thai data security landscape is the proposed Personal Data Protection Bill, which had been previously withdrawn from being promulgated into law and is now undergoing further reviews from the Thai National Legislative Assembly. This Bill resembles the Personal Data Protection Act of Singapore but lacks similar key PDPA features. To this I refer as the “Thai PDPA-lite” approach.

i. General and Specific Laws relating to Data Security Protection

Privacy is a fundamental right guaranteed under the Thai Constitution. Legal provisions relating to the right to a private life and personal data are contained in the specific legislations; for instance, the Government Information Act B.E. 2540 Article 21-25, the Financial Institution Business Act B.E. 2551 Section 154-155, the National Health Act B.E. 2550 Section 7 and the Computer Crime Act B.E. 2550 Section 11 paragraph 2 and 3, and in the provisions of the Consumer Protection Act regarding protection from unfair and false advertising, direct sales, direct marketing and consumer contract. These provisions, however, do not specify the general duty and liability for businesses that use and benefit from the personal data, or for safeguarding the protection of individuals regarding the collection, use, and disclosure of information by businesses. Moreover, they do not embrace the standard of data security practices in line with the internationally recognized standards and principles. Thus, the absence of specific laws addressing data security issues affects the transfer of information in international business transactions, especially to/from the countries where laws prohibit the transfer of information to jurisdictions in which personal data are not assured with equivalent standards under the law.


The Thai Constitution B.E. 2560 (2017), hereinafter referred to as the “Thai Constitution” guarantees the right to privacy and right to personal data under Section 32. It provides that: a person shall enjoy the rights to a private life, dignity, reputation and family. Section 32 Paragraph 2 provides that: An act abusing or affecting the rights of a person in paragraph 1, or the exploitation of personal information in any manner is prohibited unless a provision of law is enacted to allow such act where it is necessary for public interest reasons. Section 46 of the Thai Constitution provides that consumer rights shall receive protection. The limitations of such rights and liberties guaranteed under the constitution cannot be made unless they were enacted into the law with conditions specified under the constitution.

The relevant constitutional provisions on personal data and privacy rights are as follows:

Section 32 Human dignity, Right to protect one’s reputation, Right to privacy

A person shall enjoy the rights of privacy, dignity, reputation and family.
Any act violating or affecting the right of a person under paragraph one, or exploitation of personal information in any manner whatsoever shall not be permitted, except by virtue of a provision of law enacted only to the extent of necessity of public interest.

Section 33 Regulation of evidence collection, Right to privacy
A person shall enjoy the liberty of dwelling.

Entry into a dwelling without the consent of its possessor or a search of a dwelling or private place shall not be permitted, except by an order or a warrant issued by the Court or where there are other grounds as provided by law.

Note: The Thai Constitution 2017 introduced an individual right to personal data for the first time. Prior to this, the text “personal data” was not mentioned in the language of the constitution, but inferred from the provision that guarantees individual liberty in a dwelling and the right to a private life and family.

Section 26 Restriction of Rights and Liberties
The enactment of a law resulting in the restriction of rights or liberties of a person shall be in accordance with the conditions provided by the Constitution. In the case where the Constitution does not provide the conditions thereon, such law shall not be contrary to the rule of law, shall not unreasonably impose burden on or restrict the rights or liberties of a person and shall not affect the human dignity of a person, and the justification and necessity for the restriction of the rights or liberties shall also be specified.

The law under paragraph one shall be of general application, and shall not be intended to apply to any particular case or person.

Section 37: Protection from expropriation, Right to own property, Right to transfer property
A person shall enjoy the right to property and succession.

The extent and restriction of such right shall be as provided by law.

The expropriation of immovable property shall not be permitted except by virtue of the provisions of law enacted for the purpose of public utilities, national defence or acquisition of national resources, or for other public interests, and fair compensation shall be paid in due time to the owner thereof, as well as to all persons having rights thereto, who suffer loss from such expropriation by taking into consideration the public interest and impact on the person whose property has been expropriated, including any benefit which such person may obtain from such expropriation.

The expropriation of immovable property shall be made only insofar as it is necessary for the purposes provided in paragraph three, except for an expropriation to use the expropriated immovable property to compensate in order to restore fairness to the owner of property expropriated as provided by law.

An immovable property expropriation law shall specify the purpose of the expropriation and expressly prescribe a period of time for use of the immovable property. If the immovable property is not used to fulfill such purpose within such period of time or there is immovable property remaining from the use, and the
original owner or his or her heir wishes to have such immovable property returned, it shall be returned to the original owner or heir.

The time period for requesting return of expropriated immovable property which has not been used, or of the remaining immovable property, to the original owner or his or her heir, as well as the return thereof and the reclaiming of the compensation paid, shall be as provided by law.

The enactment of an immovable property expropriation law which specifically set out immovable properties or owners of immovable property subject to the expropriation as necessary, shall not be deemed contrary to section 26 paragraph two.

**ii. Consumer Protection Law Landscape: Regulations on Advertising and Consumer Contract.**

Article 46 of the Thai Constitution provides that consumer rights shall receive protection. Under the Consumer Protection Act of Thailand B.E. 2522 (1979), (TCPA) Section 4, the consumer enjoys fundamental rights as follows: (i) the right to receive correct and sufficient information and description as to the quality of goods or services; (ii) the right to enjoy freedom in the choice of goods or service; (iii) the right to expect safety in the use of goods or services; “(iii bis) the right to receive a fair contract”; and (iv) the right to have an injury considered and compensated for in accordance with the laws on such matters or within the provisions of this Act. “Consumer” mean a person who buys or obtains services from a business man or from a person who has been offered or invited by a businessman to purchase goods or obtain services, and includes a person who duly uses a good, or a person who duly obtains services from a businessman even he/she is not the person who pays the remuneration. “Business man” mean a seller, manufacturer or importer of goods for sale, or the purchaser of goods for re-sale, a person who renders services, including a person who operates an advertising business.

The TCPA provides protection regarding advertising in order to prevent the consumer from being disadvantaged by businesses. Section 22 of the TCPA prohibits the act of advertising with a statement that is unfair, false or misleading on the material aspects of the product or service. Section 22 provides that “Advertising shall not use a statement that is unfair or a statement that may cause an adverse effect on society as a whole, regardless of the fact that such a statement includes the origin, condition, quality or characteristic of the product or the service, as well as its delivery, the supply or use of the product or service. Its paragraph 2 puts forward that: “These following statements shall be deemed as the statements that are unfair or that may cause an adverse effect on society as a whole: (1) a statement that is false or exaggerated; (2) a statement that is likely to cause misunderstanding in the material aspects of the product or service, regardless of whether such a statement is created by the use of or making reference to an academic report, statistics or anything that is untrue or exaggerated....”

- Thai Consumer Protection Act (TCPA) as a FTCA-Plus

There are similarities between the established Thai Consumer Protection Act and the U.S. Section 5 of the FTC Act as to the legal objectives, prohibited acts and the power of the regulating body. The differences are that the Commission is equipped with broad powers and discretion under the TCPA, not only to prohibit the unfair and deceptive acts of businesses, but to announce the types of business contract under the regulation of the Act’s contents. The Commission has power to penalize the business and its vendors allegedly engaged in performing such conduct in the first instance, which includes jail terms. In addition, Thai laws do not present
the same issues of proof of harm and injury as in the U.S. This is because the unauthorized use of personal data is cognizable harm under the Thai Constitution. The emotional injury is also cognizable under the TCPA, which provides punitive penalties three times the damages caused by the egregious conduct of business.

In Part II of this chapter, I will discuss whether and how the FTC approach under Section 5 of the FTC Act can transplant into the Thai consumer protection law, and why adjustments are needed so as to make it functional in operation, and meet the objective of promoting individual protection in the Thai context.

iii. Personal Data Protection Bill: Data intermediary and Data Controller Liabilities

The Personal Data Protection Bill has undergone several reviews and amendment by the cabinet, the Ministry of Digital Economy and Society, Thai National Legislative Assembly and the Council of State and four public hearings. It had been first proposed in the Yingluck Shinawatra government before the Coup took place in 2014. There are several original drafts proposed by civil rights groups and the Ministry of Digital Economy and Society. On 22 May 2018, the Cabinet approved the principles of the Amended Bill of January 2018 (the 2018 Amended Bill), proposed by the Ministry of Digital Economy and Society (MDSE). The Bill is now under the review of Thai National Legislative Assembly. This recent 2018 version reconciles the propositions found in the original bill proposed by the civil rights groups and the other bill proposed by the ministry. The 2018 Amended Bill, provides significant amendments to the previous bill of the Council of State, which was to be passed into law in 2015 (the Previous Bill of 2015), but withdrawn by the cabinet to undergo further reviews.

The amendments found in the 2018 Amended Bill deviate from the previous 2015 Bill in its fundamental structures. It adds significant features which are omitted from the Previous Bill of 2015, for instance: the application of a combination approach to define personal data, the removal of spouse and heir of a deceased person from the definition of a data subject, the introduction of a definition and separate liabilities of a data processor including data security, the application of similar provisions to the commercial and non-commercial data controller, mandatory breach notification, safe harbor for reasonable data security practices, the narrowing down of an exemption from individual consent, the establishment of the sub-committee consisting of persons with expertise in technology and economics, the establishment of an office independent from the government to educate privacy awareness, the establishment of a certified accountable agent in the cross-border privacy rules framework, the exclusion of an individual employee’s civil and criminal liabilities from the damages. These amendments correspond to most of the commentary of the Previous Bill of 2015 provided by the author earlier in the research project of King Prachadiphok’s Institute, as proposed to the Thai Cabinet and the Legislative Commission for their consideration. The 2018 Amended Bill, however, still lacks emphasis on the key functions of trust and cooperation and presents additional major issues on the personal data of property-like ownership status, as will discussed further below.

The overall structure and venue of the 2018 Amended Bill and the Previous Bill remain similar to the Personal Data Protection Act of Singapore enacted in 2012. For the purpose of further comparative analysis in part II of this chapter, I provide the general provisions and highlight some distinct characteristics of the 2018 Amended Bill elaborated in the commentary notes as follows:
The Objectives

The reason for issuing this Act is to provide general protection to personal data, by providing regulations, mechanisms and measures for governing personal data. The abuse of privacy rights of personal data creates nuisance or damage to the personal data owner. This is facilitated by the advance of technology that allows such collection, use and disclosure of personal data in such exploitation. Such exploitation creates an adverse effect on the economy as a whole, with the widespread use of digital technology.

Restriction of Rights to Personal Data and Privacy

The restriction of the rights and liberties under this Act are allowed under the Constitution Section 26 and Section 32, Section 33 and Section 37. The reasons for such restrictions under this Act are to enhance the effectiveness and the remedial measures provided to an individual who has suffered from the violation.

Definition of “Personal Data”, “Data Owner”, “Rights of Data Owner”

Section 6 First and Fourth Paragraph

“Personal data” means any information pertaining to a person which can directly or indirectly identify a natural person, excluding name, position, workplace or business address and information of a deceased person.

Note: The definition of sensitive data is not provided, but a category of data which would be sensitive to the public in general is mentioned in Section 23. These are personal data concerning race, nationality, political opinion, religious belief and philosophy, sexual behavior, criminal record, health information or other information that is sensitive to the feelings of the public. In general, it requires consent from individual in the collection, use or disclosure of such information.

“Data owner” includes the legal representative of a minor (aged below 20 years old), the legal guardians of quasi-incompetent and incapacitated persons.

Section 26-28: Rights of a Data Owner

A data owner has rights to access information relating to him/her and to the disclosure of the means by which information is acquired without his/her consent unless exception provides otherwise. When the data controller does not comply with this Bill, the data owner has the right to request the deletion, disposal, de-identification of such information pertaining to him/her. The data owner has the right to the update and complete the integrity of personal data.

Note: The Bill does not include a positive definition of a data owner, i.e. the person to whom the data pertains or the person identifiable by the data. The intended use of Thai vocabulary meaning data “owner” rather than data “subject” illuminates the property status of personal data. The 2017 Constitution Section 37, concerning the State’s expropriation of movable property, serves as an enumerated power to pass the Amended 2018 Bill along with other provisions. The broader public interest exceptions compared to the Previous Bill of 2015, such as the use of personal data by the data controller to comply with the order of a government officer, hints on the possible venue for intrusion of individual rights to privacy and personal data through the government exercising control over private organizations.
Definitions of Data Controller and Data Processor

Section 6 Second and Third Paragraph

“Data Controller” means a person or juristic person with the power and duty to make decisions regarding the collection, use, or disclosure of personal data.

“Data Processor” means a person or a juristic person that collects, uses, or discloses personal data on behalf of, or in accordance with, the instructions of a data controller.

Section 29 The Duty of a Data Controller

The data controller has the following duties:

(1) to assess the privacy of personal data on a regular basis;

(2) to implement proper data security measures to prevent the unauthorized access, use, correction, change or disclosure of personal data;

(3) In the case where the personal data shall be shared with another person or legal person, the data controller shall proceed to prevent such a person from the unauthorized use or disclosure of personal data.

(4) to destroy personal data when the data retention period has expired, or when it becomes unrelated and unnecessary according to the purpose of the collection of such personal data or when consent has been withdrawn by the data subject, except for the purpose of collection for evidence or investigation.

(5) to notify the breach of personal data to the data owner without delay. If the breach of personal data exceeds the number of persons specified by the Commission, the data controller shall notify the Commission of the remedies approach without delay. Such notification shall be in accordance with the regulations and methods announced by the Commission.

Section 30: The Duty of the Data Processor

The data processor has the following duties:

(1) to process the collection, use, disclosure of personal data only by following an instruction received from the data controller, except when such an instruction violates the law or provisions under this Bill.

(2) to implement proper measures for data security to prevent the unauthorized or undue loss, access, use, correction and change or disclosure of personal data, including notifying the data controller when the breach occurs.

(3) to proceed and collect the records of processing data activity according to the regulations and methods announced by the Commission.

Note: The added definition of data processor and distinct duties on implementing proper data security measures are similar to the PDPA, but still does not include the data retention and
disposal duty found in the PDPA. The attempt to clarify the relationship between the data controller and data processor is seen in the definitions and the duties assigned to them under Sections 29 and 30 of the 2018 Amended Bill. The connection between the two actors, the data controller and data processor, and the scope of their duties lies in the “instructions” provided by the data controller to the data processor. Such a data controller-data processor relationship concept being introduced into the 2018 Amended Bill resembles the principle-agent relationship. On one hand, the individual can entrust their personal data to the data controller, who is a primary actor responsible for damage to personal data. However, there could be potential confusion and gap, when the data processor does not follow the instruction where he has liability under the Bill, or whether the data processor still has an obligation to compensate damages occurred to an individual. This is because such a duty to compensate damages is imposed on the data controller only. It is unclear if such a data processor retains the status of a data processor or tends to become the data controller himself when he does not comply with an instruction to deliver tasks within the scope of a job assigned by the data controller. Such issues in relation to trust relationship and cooperation will be further discussed in Part 2 of this chapter.

The Non-applicability and Applicability of the Bill

Section 4-5

The Amended Bill excludes the following activities from the application: domestic use of personal data; media, art and literature use according to the professional ethics and for public interest; the use according to the duties of the national legislative assembly, senior representatives and the parliaments; the court proceedings and decisions and the officers in legal procedures; processing of credit information by the credit bureau and members; and others activities for public interests according to the royal decree.

The provisions under this Bill apply to the collection, use, disclosure of personal data occurring within the Thai territory. Such activities, which partially take place within Thailand or the intended results are to take place in Thailand, shall be deemed as activities occurring within the Thai territory and falling within the scope of application.

Note: It is noticeable that this 2018 Amended Bill applies to government conduct which was previously carved out in the Previous Bill of 2015. Still, further exception could be found under the royal decree to be issued after the Bill comes into force.

General provisions on Protection of Personal Data, Consent and Exemptions

Section 17-21

A data controller cannot collect, use or disclose personal data if the data owner does not give consent before or at that time, except under the provisions which this Bill otherwise allows. The consent can be made in form of a written agreement or through electronic means except when the condition does not permit such means. The data owner can withdraw consent at any time except when contracts or the law provides restriction to the benefit of the data owner. In obtaining consent, the data owner shall be informed of the purpose of collection, use, or disclosure, and shall not be deceived or misled by such a purpose. When data falls under the exemptions, consent is also not required for its use and disclosure. (Section 24).

Consent requirement is exempt if personal data is collected: for conducting research, statistical analysis, or for the public interest, and when the data is kept confidential; for
preventing emergencies or protecting a person from danger or from publicly available information; for necessarily complying with contracts to which the data owner is a party or for processing the application of the data owner before entering into contract; for the legitimate interests of the data controller or a person or legal person other than the data controller, except when such interests are at lower priority than the fundamental rights of personal data of the data owner; for the public interest or in the exercise of a government authority by a data controller; and for other matters prescribed by a Ministry announcement.

Note: It is noticeable that the law still omits to specify the express or implied consent required from a data owner, when read together with the exception provided in Section 21 (3) under which the consent is exempt for publicly available information with direct or implied consent from the data owner. Therefore, it generally implies that “deemed consent” meets the requirement of lawful consent under the Bill. Such a restriction of withdrawal of consent due to agreements by parties allows a business to take advantage of individuals by concluding contracts before disallowing withdrawal of consent.

The too broad consent exemption also provides means for further exploitation by businesses by using the excuse of research conducted on personal data for service improvement. Some clauses infer that there could be a case where legitimate interests of the businesses override or become higher priority than protection of personal data. In addition, the overbroad use of public interest for exercising government control over a data controller to obtain personal data without consent, or without notifying the data owner, seems to threaten rather than protect personal data.

*Power of the Data Protection Commission*

The Thai Commission consists of fifteen members as follows: The Chief Commissioner appointed by the MDES, the Director of MDES as Secretary, eight committees by selection of the Director of the Prime Minister’s office, Director of the Supreme Prosecutor office, Secretary of the State Council office, Chief Consumer Protection Commissioner, Chief of the Department of Civil Rights, President of the Thai Chamber of Commerce, a Thai Industry representative and a Thai banks representative; five committees with expertise appointed by the MDES.

*Section 14*

The power includes: planning strategies and the promotion of the government’s and private campaigns; determining the measures or policy in compliance with personal data protection provided in this Bill; the issuing of regulations and announcements to comply with this Bill; announcing the guidance of personal data protection practices for the data controller and data processor; determining the administrative fine and filing the claim to the administrative court; advising the MDES on legal amendments; interpreting and determining cases under this act.

*Part II of this chapter will discuss whether and how the Singaporean PDPA approach can transplant into the Thai Personal Data Protection Bill as amended in 2018, and why adjustments are necessary so as to make it functional in operation, and meet the objective of promoting trust relationship and cooperation in the Thai context.*
Part II: A Comparison of Thai Data Security Protection with the U.S. and Singapore

This section discusses comparatively the similarities and differences as to the existing Thai regulatory landscape with the FTCA and PDPA, and how relevant actors will respond to data breach with their U.S. and Singapore counterparts. The Telecom Provider case and some interview excerpts on organization’s perception provide an estimate of responses regarding the data breach. The asymmetry found in this analysis could imply that the U.S. and Singaporean approach when applied to Thai context could provide a different outcome from the originally intended functions within their approaches. Such deviation, therefore, should be considered when designing the path for personal data protection in Thailand based on the U.S. and Singaporean approach.

A. Perspectives on Data Privacy and Security in Thailand

Based on the recent data breach incidents and the interview excerpts on organization’s perception on individual privacy in Thailand, this section provides the estimates of the way organization, individual and regulator interacts in the Thai data security landscape, which deviates from their U.S. and Singapore counterparts. These conditions, such as relatively low privacy awareness from both organization and individual sides, uncertainty about enforcement agency, pose some limits of how the U.S. and Singaporean approaches works on the Thai ground, and leads to the proposal of alterations that enable both approaches to work in a complementary way, as discussed in the final part of this chapter.

i. Different Organization’s Understanding of Individual Privacy and Their role to Protect Personal Data

Interview Excerpt: How privacy and personal data were understood by organization?

A DPO and CEO of the lifestyle digital printing services expressed different individual privacy concerns found in Thailand and Singapore. In Thailand, the right to personal data is understood from the personality rights and copyright issues whereas it is clear in Singapore that unauthorized disclosure of personal data violates individual privacy. The DPO mentioned the example of issues could be found in Singapore, “It’s about privacy. Why [did the company] post my picture taken from the event and share those pictures of myself with others? They [Individuals] may feel resentful when, for example, their boyfriend or girlfriend may find out.” In Thailand, the same DPO mentioned about the concerns on sharing the photo online without watermark, which were later used without permission by the third party. He added: mostly only celebrities care about this issue.

A DPO and CEO of the lifestyle digital printing services mentioned the difference between the level of privacy awareness in Thailand and Singapore which influences how the organization treats individual privacy differently: Overall, I feel that it is clear that Singaporean people have more privacy awareness compared to Thai people, who’d love to see themselves in the billboard or the TV ads. For Singaporean people, if we use their photo without asking their permission. They may say I’m not happy. After receiving some concerns raised by individual clients in Singapore, my role is to instruct our employees on privacy practice, and to ask for permission from individuals. In Singapore, we will provide the notice that if you take part in this event, it will deemed that your photos and video recordings may be used for company’s marketing purpose. We do not have similar practice in Thailand. My partner in SG also warned me about privacy issues, so we need to ask permission before using the personal information in our website content.
The interviewee, a South-East Asia public policy director of a global tech firm, also shared a similar privacy issue from the use of photos as part of the companies’ marketing campaign and CSR events in Thailand, which includes photos of children. However, the interviewee mentioned the firm practices were based on the legal team’s advice to ensure that the individual consents were obtained for such purposes.

A Chief Operating Officer (COO) and the DPO of a Fintech startup of consumer investment product described the Thai consumer behaviors, the sharing of data through social media platform which raised different aspects of concerns regarding personal data: The data we have so far that would be personal information is Line user ID. Thai people are familiar with using Line in their everyday communication, so we put our members together in a group for communication and providing a program tutorial after signing up for our products. We ask [for user’s] the phone number and email address, and mostly, then after payment is made and disclaimer has been read and checked by our users, we then collected the line ID from the user himself. The same DPO mentioned on risks involved in personal information collected: There is no risks as we did not collect personal financial information i.e. user’s port which will be sensitive. …The risky part is Line ID. But it’s not that bad. What could be serious is the communication in the chat group. Sometimes we mention the name of the stock, which could be captured to share with the outside, and it could upset such individual. He added that some users decided to make payment through the third-party online payment application such as Paypal, and some prefers to submit the payment transfer receipt to the admin via Facebook group chat, which restricted to only 4 employees can access such information. Still it could be risky way of practices.

In conclusion, despite the fact that most organizations promise in the service agreement entered into with individual users how their personal data receives protection and data security arrangement has been be made with the third-party vendors, organization does not share similar understanding of Thai privacy issues in similar respects with those from the Singapore and U.S. Small organizations operating in Thailand describe data privacy in relation to defamation, personality rights and copyright violation. Global organization develops more consistent understanding of privacy with the parent company in U.S. and EU. Organizations do not fully understand their responsibility for the leakage of personal data in the similar level to their U.S. and Singaporean counterparts. The news report of breach incident suggests that the organizations found having someone intruded its database could be an excuse to clear the blame away from the organization.

---

220 Line is a communication platform, which allows users to make voice calls and send instant text or messages to another user or into a chat group, in which the sender is a member.

221 Sometimes they cannot attach files, so we use shortcut like using facebook or line to send the payment slip. There could be risk at this way of practice. Especially, facebook group of the company it’s open – but only 4 people can access such information.

222 https://www.reuters.com/article/us-true-corporation-data/thai-telco-true-defends-security-measures-after-user-data-breach-idUSKBN1HO2D5 After the independent researcher discovered the breach, the business actor did not admit of the breach at the first stance, until the public followed the blog post of foreign researcher and discovered more about the leakage of personal data in the national media footage. The provider blamed the researcher and threatened with a lawsuit for the unauthorized disclosure of information and intruding into its system for the hacking activity. That was when more evidence came out to deny the telecom provider’s claim of sophisticated hacking method used to access into the system. In addition, the evidence on several attempt to communicate and warn the telecom provider through “contact” provided on the provider website shows the provider’s disregard on the significance of personal data leak which involves sensitive data. It followed the meeting with the regulator that the telecom provider said it had notified the affected user of breach and fixed the issues. It is not reported by the media or regulator whether it did as it had promised.
Despite some practices have been in place by the organizations, such as restriction of employee’s access and individual consent agreement, privacy have not been integrated into the culture of organization practices in Thailand despite implementing higher standard of practices on similar issues in their operation in Singapore.

ii. Shared Organization’s Worldview based on Individual Trust and Relationship Regarding Data Breach Notification and Remedies

Interview Excerpt: How decision on breach notification and remedies was made?

A DPO and CEO of the lifestyle digital printing services implied the responses based on the assessment of the breach impacts, which also depend on how such an individual would go at great length on the breach. According to the interviewee, If that happened in SG, we will assess what type of content and how large is the impact. For example, who is the person in the leaked photo and see if such person wants to make it a big deal. If she/he won’t make it a big deal, we will think how could we do and contact him or /her. If there is any report that individual has suffered from damages, we should contact such affected individual. He mentioned that: if there is any data breach issue, it would be my partner and I who send the apology message with deleting such violating content. Though he admitted that being open about the breach may not gain trust but also the complaint from individuals: There are two ways to look at this. My first answer is Yes. But if it will be No, that is because there will be such a complaint like how could you leak such photo!

The interviewee, a DPO and COO of Fintech, mentioned that breach notification should be made within the group of members before going public because of the fear of distorted message received by members that could affect trust. The interviewee mentioned: In financial business, trust is the most important thing. There will be more consequential problem [if we go public at first]. We didn’t tell it all straight because, in Thai culture, people like to distort the message. We think too much of many other things, so if it is not really severe, we won’t tell everything right away to the public. However, communication through social media is necessary. The interviewee admitted: if something appears in social media or know widely to public, we need to publicize via social channel. We will say that our system was hacked or will be off temporarily. This is the worst case. We will publicize via our social channel.

However, with his background in public communication, he raised that breach notification could be part of the communication strategy to be in better position if it is the case of nation-wide impact that also affect other businesses: We will jump in. It’s part of communication strategy. We’ll protect ourselves earlier. Though, the interviewee expressed that the notification of breach caused from the company itself “is like shaming ourselves that we are not ready”. However, the interviewee pointed to the advantage of promptly notifying to members in relation to increased trust: They [consumers] will trust the company more. Psychologically, if we let them know earlier, that signals that we are ready. They will think that if we are not confident, we won’t let made public. He further gave an example of how remedies could satisfy individuals and stop more complaints: once our internal system was down and we decided to announce that we extended 2 month’s membership for our members. We weighed the benefit and cost. One user wanted the refund and asked why server down so often. We did not refund, but we took advantage to let them know earlier before more complaints. It turned out positive. For business, we has no further cost. And they feel that we respond beyond user’s expectation. It increased consumer trust.

The public policy director in the global tech company also suggests that the breach notification deals with the risks of losing short-term trust from revealing organization poor practices in order to build the long-term trust through transparency. He mentioned that the local
policy followed the parent’s company practices in EU, which requires breach notification to be made to the authority and the affected consumer in case of data breach. The interviewee’s opinion however suggests the criteria for notification should be made based on the degree of breach and sensitivity of data.223

In conclusion, all interviewees raised the common theme found in the U.S. and Singapore data privacy professionals. These are, data breach in relation to trust, individual reaction, which informs organization’s post-breach responses towards individual. The interviewee discussed breach notification and remedies provided to individuals in terms of strategic action to bargain trust and risk involved in disclosing poor organization practices when choosing to be transparent and honest.

iii. No Legal Complaint Culture and Relatively Low Privacy Awareness

The relatively individual’s low privacy awareness together with high engagement in data sharing activities on social platforms and intensive data collection by organization posed high risks towards exploitation by organization or malicious actors. As of 2016, Thailand has over 40 Million facebook account users and in average 7 hours a day was spent on the Internet.

The 2017 survey report of Thai internet users behaviors, conducted by Electronic Transactions Development Agency, found that only 11% answered privacy intrusion or exploitation of personal data as most frustrating Internet issues experienced by respondents and 6.3% answered fraud, as compared to other issues like online advertising and the slow internet connection.224 However, there is a significant increase of privacy concerns from the year of 2016. 63.5% of the respondents found their behaviors changes from last year mostly regarding their increased internet use for entertainment and online shopping, followed by 64.1% found they are more concerned about online posts, profile sharing and chatting. 59% of respondents do not open email from unknown sender and suspicious links on website and 34.5% said they regularly change passwords and enabling double authentication.

The same survey also asked the respondents for their reasons when deciding not to make complaint when they found the issues online. Most said they do not complain because the petty amount of loss (56.7%), not worthy of time (55.8%). It is noteworthy that 36.2% said they do not know where to report, and 32.7% said they do not know the procedures to lodge the complaint.225 When asking about the channel for reporting issues found online, 86.8% of respondents would choose to report issues to the government entity, whereas 59.8% would report

---

223 The Policy Director of Global Tech Firm: “Notifying consumers sometimes really show how poor our system is, so it may cause us to think if we should better hide it. But, we do business on the transparent basis. If we have any problem we will notify authority, customer about the cause and the correction or remedies available for them so to build trust in long run. Even though this would affect the short-term trust, we need to evaluate what should be notified in the future. In my opinion, we need to look at the degree of breach. If we need to notify in every single case, we won’t have time to do business. It should be only case that is significant to the customer that requires notification for example those related to financial information or credit account.”

224 Thailand Internet User Profile 2017, the survey report of Thai internet users behaviors, Electronic Transactions Development Agency [Public Organization] (ETDA) published August 24, 2016. https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2017-slide.html The multiple-choice survey was conducted from 25101 respondents in July 2016. Other issues found most frustrating by the respondents are the online advertising (66.6%), slow connection (63.1%), disconnection (43.1%), junk email (34.2%), computer virus (21.5%), unreliable internet resources (11.9%).

to the website of product and service provider, 24% reports to the authority, and 19.4% provided comment in online social community.

From the interview excerpt, an organization also viewed lesser privacy concern of Thai people in comparison with Singaporean people. Following the incident, besides the general demand for stringent law on data protection, the media report did not mention that Thai consumer activist groups or the affected consumers has sought for further compensation and remedies for the leakage of data. No further updates as to whether the affected consumers have received notification of breach from the company.

The weaker consumer and low privacy awareness demonstrates the needs of law to educate and empower consumer with channel to report or inquire of breach while also needs to heavily rely on organizations’ reasonable practices in handling personal data.

**iv. The Unclear Rule, Role, and Communication with the Regulator**

The CEO of digital printing services considered legal aspects as most difficult part of handling individual privacy: *To me, it will be the legal aspect. I do not know, not really know, or not knowing completely.* The interviewee, a global tech firm’s regional public policy director revealed that difficulties are on the legal uncertainty and the low privacy and security awareness in Thailand. The interviewee raised the concern on the Thai enforcement agency: *I feel Thailand is not ready yet especially in the part of government agency who will take charge of data privacy enforcement.*

The interviewee points out the culture of business practices in Thailand that needs more transparency and trustworthiness. “All issues have not be put on the table for discussion, so we did not received cooperation and sometimes it’s about ethics and business practice in each culture.” He added, “The worst situation would be the compliance issue. Western culture gives importance on the compliance with law, rules and regulation, however in developing countries, many haven’t complied with the international law standard.” Thus, the interviewee raised the significance of adhering to the firm’s code of conducts and the global policy, which applies domestically to each jurisdiction in addition to the legal team’s advice based outside of Thailand.226

Connection with local government is the issues raised by the interviewees. The public policy director said, “We need to monitor the new law and keep our contact with local government. In the case of Thailand, we need to keep contact with ETDA and Digital Economy Ministry for updates.” Similar concern of Thai regulator is raised by the fintech DPO and COO: *Coordination with the authority and regulators is the hardest thing. As Fintech is new during this transitional period, the difficult part is how we could connect to the regulators…. In Singapore, our business consultant has informed us on data privacy policy. We were told that MAS is quite strict with the financial information practice. This is very different from practice in Thailand that we could ask almost everything. However, we have not yet requested financial information from the users, but only some basic information.*

The case of telecom provider may be clearly under the NBTC, but for other general data breach cases after the PDPA comes into force, there would be more overlaps. It is unclear how the Consumer Protection Commission viewed their roles in regulating these issues, as so far they

---

226 “If I did not stick on our code of conduct, I may get fired.” “In addition to the resources, we will rely on our policy, which is universal applied to domestic policy of each country. Our most trusted resources when it comes to privacy regulation would be our legal team privacy policy and regulation. We also consulted with our team in Europe who look at our global privacy policy by having GDPR as a key reference. We need to ensure that there is no significant conflict of our policy with the regulation.”
did not take any action in response to the data breach issues. Until this time, there are no further updates from the NBTC about the result of the investigation.

v. The media and researcher groups

The media and public vigilance in Thailand currently play a limited and less active role in discovery of the breach and the investigation and dissemination of truth, unlike their U.S. counterparts. Despite some successful attempt in the recent telecom provider cases, there is no follow up on the issues and more focus on breach occurred at the global scale rather than the local issue.

Conclusion

The abovementioned, which forms specific contexts of Thai privacy, have placed limits to the operation of the U.S. and Singapore approaches. Thai privacy regulation therefore needs the stronger assurance and cooperative functions to promote trust relationship while empowering individuals with self-control. The law should leave some gap for organizations to initiate trustful act towards individuals. However, such gap may not be widened as in the U.S. and Singapore for the much weaker norm on individual complaint, trustworthy and transparent business practices and privacy practices on the ground. Despite such lack, the relationship of trust is still considerably relevant for organizations in enhancing better practices towards individuals in term of post-breach practices. As the Thai law is pending, the interview excerpts provide beyond compliant behaviors from organizations although they also present broader issues concerning less transparent and untrustworthy behaviors of business practices in Thailand. So far, a few incidents having been investigated by the regulators of specific industries under the specific regulations are clear evidence of ineffective enforcements against unreasonable data security practices in Thailand.

In conclusion, the choice for the legal design for Thailand depends on current attitudes, roles and nature of relationship among actors in the Thai landscape of personal data protection. This is necessary for estimating whether the transplanting concept will perform the same function within the existing landscape, so as to fulfill the ends of promoting trust relationship and cooperation and individual self-control in the transplanted country. Next, section B will further discuss the existing legal structure that provides some venues for transplanting new concepts into the Thai data security protection.

B. The Thai FTCA-Plus and The PDPA-Lite Approach: The Ramp and The Highway

The analysis found that Thai Consumer Protection Act provides equivalent functions to the U.S. FTCA with some extended features. I refer to as “the Thai FTCA-plus”. In addition, many areas of the Thai Personal Data Protection Bill overlap with the PDPA, but it lacks some key trust-enhancing functions found in the PDPA. I refer to as “the Thai PDPA-lite”. Both existing venues, when applied with the lessons from the U.S. and Singapore, however, may not fully functioning as in the space of origin. This is mainly because the Thai soil lacks some key ingredients found in the spaces of origin.

As discussed in section A, the weaker role of Thai media and public vigilance as compared to U.S. could hinder the information transparency and equality between consumer and business parties, as well as less reputational pressure on business behaviors. Furthermore, the
Thai PDPA-lite is unlikely to contribute to proper environment for trust relationship and cooperation between relevant actors. This is because it lacks key PDPA functions that trigger the attitudes and motivations for trustful behaviors of the business towards consumer, and mutual interests for cooperation between business actors of different roles. The Thai soil also lacks similar fundamental trust and cooperation as in Singapore. This is more crucial when considering that the Thai PDPA-lite proposes to establish new inexperience committee as an enforcing body. Altogether, these considerations point toward a more concrete structure needed in the regulatory design, where lesser gap means lesser room for business decisions to deliberately demonstrate trustful behaviors to consumer to reinforce trust relationship between them.

This section will discuss two levels of adjustments necessary for both approaches to serve the intended goals in Thailand: first level is to add the missing key functions of original approach into the existing Thai platforms and venues; second level is an adjustment due to the differences of flow and force within the space of Thailand created by the relevant actors.

i. FTC Section 5 and Thai Consumer Protection Act: The FTCA-Plus Approach

In transplanting the FTC application of section 5 of the FTCA to data security breach issues to Thai context, it needs reexamining the functions and scope of existing Thai consumer protection laws with the FTCA section 5. As illustrated below, section 22 of Thai Consumer Protection Act prohibits against unfair and misleading advertisement and empowers the agency to order the businesses to prove the truthfulness of its advertising statements. Section 22 of TCPA therefore provide similar function to U.S. FTCA section 5. The venue of TCPA section 22 provides more protection compared to section 5 because it allows individual rights to make private claims, a self-settlement procedure between parties, penalties for violating businesses. Furthermore, TCPA section 35 also provides additional venue for consumer protection from the unfair contracts entered into with businesses. It empowers the contract committee to declare the prohibited or mandatory content to be included into consumer contracts. The contract committee can inject a model clause of data protection to be included into the regulated businesses.

a. Consumer Protection Against Unfair and Misleading Advertisement

From the analysis, there are similarities between the established Thai Consumer Protection Act and the U.S. Section 5 of the FTC Act as to the legal objectives, prohibited act, and the power of the regulating body illustrated as follows.

The TCPA objectives are similar to the FTC Act in that they both aim to protect the rights of consumer regarding their choices on product and service and the fair competition. Therefore, both prohibit the act of the business that could cause adverse impact to such objectives, that are, the unfair and deceptive acts that cause misunderstanding on the material aspects of product and service. As to the content of the act prohibited under both provisions, the FTC interpret broadly of representation to cover any act in or relating to commerce that cause consumer to understand that their personal information receives proper protection. Such act shall deem the representation, which is material in their decision-making to consume the product and service. Therefore, if the business does not actually do what they promise, such representation would be deceptive and actionable under Section 5 of the FTC Act.
Section 22 of the TCPC prohibits the similar acts, as the definition of “advertising” under the TCPC is an act, regardless of the means, expressed in the way that an ordinary person can understand the meaning and the public acknowledges such statement, with the commercial benefit purpose of the business person. Therefore, if there is any act expressed from the business person in the way that causes people to understand that their personal information receive protection regarding the privacy and security, but not true in practice which led to the unauthorized disclosure of personal data. Then, such instance could be deemed the use of advertising statement that is false or cause misunderstanding in the material aspects of the product and service, which by itself is unfair and cause adverse effect to the public. Thus, such false representation by advertising statements of the business party is actionable under Section 22 of the TCPA in the same way that the FTC triggers section 5 of the FTC Act.

The next question concerns what aspects the consumer receive protection regarding their personal data under the advertising protection of the TCPA. Section 27 of the Act empowers the Commission on Advertisement (“COA”) comparable to the FTC powers in issuing an order for business person to correct, stop using the false and misleading statements or means of advertising in violation of this Act, and the correction of the consumer’s misunderstandings which may be already caused from such acts. Besides, the COA has authority under Section 28 of the Act to order the business person to prove the truthfulness of the advertising statements reasonably believed by the COA to be prohibited under the TCPA. Such exercise of COA power will be beneficial to the consumers by informing them with truthful information necessary for evaluating the risks of data leakage involved with the product and service concerned, so that they can make informed decisions on whether to purchase from such business person. This is also preventing harm to the public.

In addition, TCPA in several aspects provide the extended venue beyond the Section 5 of the FTC, which are suitable for applying with data breach issues. For instances, the procedure allows the dispute settlement between the alleged business person and the consumer at the early stage. This opens for the opportunity to correct and remedy the injury from data leakage in a timely manner. In the case where the dispute cannot be settled between the parties and the Consumer Protection Board (CPB) convicts the business person of the offence, the prosecutor can proceed to file the case with the court. The Consumer Protection Board also have the power to settle all the offences under this act according to Section 62. The penalties include fine and jail terms. For the continuous offences, the fine is amounted to 10,000 THB per day (300 USD) or not over twice of the expenses paid for the alleged advertisement during the violation of the Act and the order of COA. The advertising business and the owner of advertising media also have liabilities under the Act. Consumer has private rights of action under the TCPA and could sue to the businessperson with the court.

Therefore, exercising COA and CPB powers under the provisions of consumer protection against the false and misleading advertising conduct of the businesses are comparable to those of the FTC actions under Section 5 of the FTC Act to the consumer data breach cases where the business person makes false or misleading representation on the security and privacy of personal data. Such consideration will help remediating the loss and preventing harm due to the unfair treatment of personal data from businesses and secure consumer trust in the market and international business transactions.
As a result, it is viable for Thai regulator to employ the FTC approach by applying the provisions of unfair and misleading advertising to business entrepreneurs which were alleged with expressed or implied representation about the security of consumer information relating to the product and service, but does not actually implement proper measures to safeguard such personal data, resulted in the data breach.

b. Consumer Protection Against Unfair Contract

Besides the advertising protection, the TCPA has the provisions regarding the protection against unfair contract with business party that put the consumer in disadvantageous position. Section 35 bis empower the Committee on Contract (COC) to announce the regulation of contracts under the conditions specified under the royal decree. The COC could regulate the content of contract entered into between the business and consumer; for instance, to clearly inform the right and duty to the consumer regarding the product and service, to prohibit the restriction or exceptions regarding the liabilities of the business person in the substantiality without adequate reasons. To this date, the businesses subject to the regulation of the COC include the lending services of financial institutions, the credit card services and the telecommunication services.

Accordingly, it is viable for the COC to exercise its authority to specify the businesses which collect, use, process or disclose sensitive personal information of consumer i.e. financial information, debts, banking account information, government issue ID card to include the clause on data security and privacy of consumer information to the consumer contracts. Such clauses shall include the duty to inform and receive consent from the consumer before the collection, use, disclosure to other party, the duty to implement adequate security measures and to enter into contractual arrangement with its vendor which processes personal data of consumer. In addition, the clause should prohibit the limitation and exclusion of the business party from the liabilities in case where the data leaks occur due to their inadequate security and privacy measures or the exploitation of such personal data by the businesses in making profit. Such protection of consumer contract will be in align with the fundamental rights of the consumer in being informed and give meaningful consent relating to the use of their personal information. This includes receiving notification when data leakage and compensation of damages that do not unfairly create too much burden to business party considered the damages occurred to them from the data breach.

c. Strengths and Weaknesses of the FTCA-Plus Approach

In my view, the Thai Consumer Protection Act venue could be an immediate venue for protecting data security of consumer while personal data protection bill has not enacted. This venue provide flexibility for the Thai Consumer Commissions to exercise power under unfair and misleading advertising and the Thai unfair contract regulations to provide necessary protection to consumer personal data. On one hand, the enforcement against unreasonable data security practices will raise privacy awareness to individuals, as well as businesses. Regulating content of consumer contract will fill in the gap under specific laws governing the industry, the boiler plate privacy policy and client/user agreements that include exemption from liabilities of the business parties. At the same time, it will caution these industries to implement reasonable
data security practices to consumer sensitive data and to develop into the norms before the Bill come into force. It is also noticeable that the Thai consumer protection imposes liabilities to an owner of advertising business operators and advertising media from the unfair and false or misleading advertisements. From this, these actors, such as e-commerce platform and social media like Facebook, Twitter, have implied duties to screen the false and misleading contents regarding the data security involved.

Even though the Thai FTCA-Plus approach would fill in the lack of specific legislation for personal data protection in Thailand, it also faces similar limitations faced by the FTC as well as the Thai Consumer Protection Commission. First limitation is on the scope that cover only commercial activities and business parties who provides service or product to the end user. This leaves out some actors such as the wholesaler and reseller who have consumer data in their possession from the application. Data business, such as the data brokerage servicer are also not properly regulated, thus demanding the specific regulations to be issued to fill in the gaps.

Second is on the data intermediary liabilities. Like the FTC case of Vision I Cart Properties, it could be foreseen the case of IT vendor employed by small businesses to handle its website be the only party who is held liable for data security breach incidents. Those small and medium businesses, who are end users of such product or service, receive protection under consumer protection provisions despite their disregard on overseeing the use of personal data by the vendor, and ensuring reasonable practices of the vendor. This will raise major problem as most IT vendors and platforms operates outside the jurisdictions, and the cooperation with foreign agencies has not yet established. As a result, consumer may end up not receiving prompt compensation and remedies from breach. The liabilities therefore should be distributed to the merchants as a primary responsible person from the breach.

The continuously weak performances of Thai media, researcher and public vigilance in discovery of breach also raise the significant issues under this approach. As an element of success under the FTCA section 5 approach also depends significantly on the investigative roles of the media and third-party researcher groups that have brought the breach scandals into public light, thus allow public forces to put pressure on big corporations’ irresponsible behaviors. These actors play active functions in proving creditability and trustworthiness of the businesses, and enhancing information transparency and equality as provided by the regulations. These active players in Thailand have been dysfunctional, compared to their counterparts in U.S., and could render the ineffectiveness of this approach.

Despite being equipped with power to reign in unreasonable data security practices of businesses, the Consumer Protection Commission has limited human and expertise resources to conduct investigations and go after the businesses, as compared to the FTC. Considering with the weaker roles of media and public vigilance, it is foreseen that Thai consumer protection enforcement agency will need to be more aggressive in exercising of power granted under the laws to order the suspicious business to prove the truthfulness of the facts of advertisement statement before the Commission. This includes considering becoming more heavy-handed in applying penalties to intentional exploitation and egregious unreasonable data security practices otherwise their advertisement representations that causes massive impact from data breach. These extended powers of the Thai Commission compensate the limitations found in the Thai ground. Otherwise, this consumer protection venue can become ineffective in protecting consumer data.
In conclusion, some adjustments are necessary for the smooth translation of the FTC approach into the Thai context due to different legal structure and actors’ behaviors. In particular, the role of enforcement agency plays important part in bringing the data breach issues into light, which will assure consumer with protection of their rights to personal data and privacy. The criteria developed on reasonableness practices of business through contracts and enforcement actions will increase certainty to businesses and still open for the PDPC mitigating and aggravating criteria to apply with. Whether and to what extent the Thai FTCA-Plus will serve the ends of promoting self-control, trust relationship and cooperation will be discussed in Part III.

ii. The PDPA and Thai Personal Data Protection Bill: The PDPC-Lite Approach

There are apparent similarities between the Thai amended Personal Data Protection Bill and the Singaporean Personal Data Protection Act in the fundamental structure that provides statutory basis for the right and duty to data security, the characterization of actors involved and relationship among them and the Commission’s power. The differences are as follows: the Thai right basis as opposed to the non-right basis to privacy protection in Singapore, the status of personal data, the lack of emphasis on trust relationship and cooperation in the law objectives and mechanism, and the lack of interpretative principle of reasonable person standard, the data protection officer, including broad exceptions provided to data processing businesses under the Bill. In addition, even though the 2018 Amended Bill provide definition and distinct liabilities for data processor, which is closely resemble to data intermediary under the PDPA, as well as the principle-agent like relationship comparable to the PDPC’s interpretation. The Thai data controller-data processor relationship faces constraints due to the vague and rigid language of “instruction”, which potentially undermine the cooperative functions between business parties while also creating the gap.

How these similarities and differences of Thai soil from the Singapore will undermine the PDPA functions reinforced by the PDPC will be discussed below as well as the consideration for adjusting fit the Thai ground.

(a) The Bill’s objectives do not speak of promoting individual trust in data processing businesses or a proper balance between individual right and economic benefits from free flow of data. Therefore, it misses an opportunity to speak to actual business stake of gaining or losing consumer trust in the long run as a result of complying and not complying with this act. In fact, such economic interests and needs for enhancing trust in data processing business and e-commerce has been clearly illustrated within the government’s digital blueprint, as agreed among relevant actors. As a result, the attitude and motivation for business compliance is not clearly communicated under the 2018 Amended Bill, and could render significantly outcome for the PDPA where such objectives create visible goals for actors in implementation of law.

(b) The Bill’s stated objectives for protecting individual personal data from business exploitation turns out to be a Pro-business regime because of many exemptions provided to business from duties to obtain consent, the compensation to individual and the safe harbor.

Regardless of the rights of data owner to personal data pertaining to him/her, the bill carves room for business to escape from the duty to obtain data owner’s consent in many occasions. This bill does not limit personal data to be collected, use, disclosure on necessary basis,
but within the scope provided under the incorporation article of the business. It is foreseeable the situation when the parties agree in advance not to withdraw consent for the benefits of consumer, which is doable under the bill. Without the substantive requirement on the meaningful consent or the explicit consent received from the individual even though the data is sensitive to data owners, these provision risks becoming a license for business to exploit personal data. Compared to the “deemed consent” concept under Singaporean regime, personal data could receive better protection thereunder according to the stricter interpretation of the PDPC.

In addition, even though data controller has a duty to compensation to individual suffered damages from the breach, certain exemption opens opportunity for data controller to use as excuses for not compensating. For instance, when the data controllers’ practice meets the requirements issued by the Thai Commission, and when the damages caused from individual’s own mistakes. Thus, rather than prompt remedies, the provision could turn out to assist business rather than consumer to get compensated from data breach. This is not mentioning the burden of proof lies on consumer on the damages, and it is not expressly stated whether non-monetary and emotional damages would be recognized under the Bill.

(c) The Bill does not incorporate the reasonable person standard as general principle in compliance, unlike the PDPA.

Without further elaboration on the substantive baseline for “proper” data security measure, it seems to be vague, and count on the Thai Commission to apply its rationale on what it deems to be proper treatment of personal data by businesses. It is foreseeable that the Thai Commission will issue the requirement and guidance for proper data security measures which rely on the industry practices. However flexible it is, this approach seems to be much obscured. In Singaporean approach, it is also arguably that the PDPC, in interpretation of reasonable person standard, relies on the Commission’s judgement of what should be rather than how the respondent would have done in such circumstance. Still, the lack of symbolic means conveying to business to understand how their exercising good judgment matters when interpreting whether they have fulfilled their obligations do speak for their attitudes and inclinations when navigating in the gaps provided under the law. The bill could be mistakenly pointing toward the opposite direction.

(d) In addition, the definition of Data Intermediary is broader than the 2018 Amended Bill to include Data Processor; the Singaporean data intermediary refers to a party who processes personal data “on behalf of” the organization (data controller) compared to “the instruction” of data controller found in the language of the Thai Bill. The data processor duties in Thai Bill are also limited than the PDPA, as Thai Bill does not provide duty on data retention and disposal to data processor. But it also includes duty to notify breach to the data controller, which is interpret by the PDPC and prepare to amend the PDPA.

(e) The Thai data controller-data processor relationship faces constraints due to the vague and rigid language of “instruction”. Such constraints potentially undermine the cooperative functions between business players parties because of the unclear boundary delineated by what is considered “instruction”. Besides, it also creates confusion as to which player will take the responsibility in the area when the data processor inadvertently does not follow instruction of data controller, but still within the scope of job assignments. In this case, the data controller could escape from liabilities if due efforts have been made on providing specific instructions thoroughly to the data processor. Thus, data controller does not have to compensate to individual. However,
data processor is still liable, but does it turn into the data controller itself in this case? The added clause defining that data processor is not the data controller raised more confusion to this point. So, if it does not, then there will be foreseeable problem when the individual will not receive any compensation from both players, as the law specifies duty to compensate for data controller only. Alternatively, if the data processor does turn into data controller itself just by advertent mistakes in not following the instructions provided by the data controller, it would present another problem: the full-loaded duty shifted to the data processor who becomes a new data controller.

Compared to Singaporean Commission interpretation, the data intermediary itself turns into organization when it intentionally deviates from the original purpose to make profit for its own. This does make sense and in align with the principal-agent relationship where the organization (like data controller) remains primary responsible actor within the purpose of work assigned. Thai Bill is in the opposite. Despite the restraint to the “instruction” makes it appear like the principal-relationship principle, the primary responsibility shift to the data processor so easily that creates the adverse effects for Thai consumer. First, it is difficult for consumer to reach the data processor that they may not have relationship with. This may prove to be more difficult considering those businesses in Thailand appears to be technology importer rather than technology exporter. Most data processor based outside the country may create more hurdle for consumer to get compensation.

This feature in Thai Bill is essentially distinct from the Singapore’s counterpart in terms of motivation to cooperate and at the same time governing each other. Such relationship is determined and governed under contractual arrangements, which are strongly recommended by the Commission to enter between them as part of reasonable data security practices. As mentioned earlier, such contracts provide the scope of duty and specific instructions for data intermediary that helps the Commission in determining whether such party acts in the capacity of data intermediary and whether they fulfil their obligations or not. In the PDPC’s decisions, the Commission also consider the de facto practices of such party. How to determine de facto instructions regarding collection, use and disclosure of personal data therefore found to be problematic issue under this Bill.

(e) The limited gap for business to exercising their judgments on personal data treatment provides less space for private participation with a strong presence of command-and-control model and centralization of the structure of this Bill. This could, in turn, hinder the self-regulation approach and the industry-developing norm on personal data practices. The bill does not encourage data controller to voluntary do exercise judgment in delivering trustful acts to individuals suffered from the breach. This is because the breach notification as well as compensation to individuals are mandatory under the Bill. Still, there remains some narrow gaps for the breaching organization to demonstrate care in consumer’s interests by performing beyond the legal required standards in remedying and correcting the breach.

This Bill, centralizing power on the Thai Commission by placing it at the top of the regime to command, enforce and sanction the parties. Unlike the Singaporean PDPC who would not apply force, but more persuade business to take their direction in performing certain action in benefiting the consumer. The cooperativeness with the agency are thus being encouraged by considering as mitigating factors from breach, whereas willful disregard and intentional neglectation are considered aggravating factors. The communication and environment established by the PDPA and implemented by the PDPC provides proper space for trust and cooperation to
emerge between business-regulator relationship. Such mitigating and aggravating factors could be considered applying by the Thai Commission in order to provide motivation for them in fulfilling obligations under this bill.

(f) This Bill added the safe harbor clause for business to be exempted from the duty to compensate damages to individual when their practices meet the Commission to be issued requirements. Such safe harbor while assuring the data controller in compliance with this bill has implied that it is unnecessary to provide compensation to individual from the breach caused by acts beyond those prescribed by the Commission. Thus, it has turned out to restrict individual from seeking private remedies from other venues i.e. based on tort and contracts. Besides, it is foreseeable that other exemption, such as blaming on individual’s fault, when often used as an excuse by business for not compensating individual from breach damages, could threaten the trust relationship between them, thus missing the whole point of personal data protection. In my view, it is good for providing assurance for businesses who had spent the due efforts in delivering reasonable practices, however, adjustments need be made so as to not pointing the loophole for business to take advantage from such.

(g) The individual complaint-based in triggering investigation is similarly to the Singaporean PDPA. However, Thai bill poses more burden on the forms and procedures of individual complaints, with which when not complying, would render the Commission rejecting the claim. Such decision to reject the complaint is also final under section 61. If the individual would like to make an appeal, it needs to follow the administrative law procedure in lodging complaint to the Thai Administrative Court. This aspect could become hurdles for individuals to receive protection in practice.

(h) The Thai Commission has power to make decisions and orders the criminal liabilities including jail term up to 6 months and/or fine amounted to 500,000 THB (17,000). These criminal liabilities for the intentional exploitation of sensitive personal data or use such personal data in the manner that causes defamation to individuals are not mentioned within the PDPA framework even though the PDPC recognizes embarrassment and reputation loss as serious breach and aggravating factors in determining penalties.

The 2018 Amended Bill, Section 65, provides that a data controller who intentionally violates the Act by use, disclosure or transfer the personal data sensitive to individuals with purpose to exploit for one’s own or other’s illegitimate benefits under the law, or in the manner that is likely to cause damages, reputation loss, being condemned or despised, or embarrassment to the other person shall be penalized as such. The director, manager or any person responsible for such business or the person with duty to instruct or omit certain actions so as to cause the juristic person commit offence under this act also have similar liabilities under such offence. Therefore, it is clear that the 2018 Amended Bill clearly recognizes the social impact on defaming individuals due to the breach of this bill and give priority to those data under section 23 which are sensitive to public feelings. That would make the basis of private claims for damages much easier?

(i) The administrative fines when there is violation of this act, which also extends to the executive director of the data controller and data processor. The maximum fine is more related to complaints to prohibit the act regarding the collection, process, and use of personal data, to destroy the personal data in the possession and delete such data. Violation of the bill will result in criminal and administrative penalties amounted to THB 500,000 (USD17, 000). The penalties
are relatively low compared to the penalties under the Singaporean agency. The authority to be established under this law has broad discretion to issue guidance and make their criteria in determining penalties to include business responses after the breach, as adopted by the Singaporean Commission.

(j) Similar broad power under the Bill.

Strength and Weaknesses of the PDPA-Lite Approach

The 2018 Amended Thai Bill fills in the gaps found in the FTCA-plus approach under the Thai consumer protection law in that it covers all data processing businesses, and provide a straightforward venue for statutory duty to data security. The said Bill, despite its recent amendments to introduce the definition of data processor and the principal-agent like relationship with the data controller, does not operate in the same way as the PDPA’s web of liabilities. This is because a more rigid scope and obligations of data intermediary that is not practical unlike that of the PDPA design reinforced by the PDPC.

The 2018 Amended Thai Bill lacks key functions for trust and cooperation found in the Singaporean design despite resemblance of the structure. The Singaporean approach provides the motivation for and attitudes of trust to actors through the legal disposition as well as assumption based on their dependent relationship nature. That is to say, relevant data processing businesses actors are interwoven within the framework and their statutory data security obligations are distributed according to the extent of control and level of involvements, and transferred to different actors as such roles cease or evolve. There are many soft criteria employed by the PDPC in determining liabilities and penalties from the breach; these are as to whether the leakage of data was intentional or inadvertent breach, the attitudes in compliance with law whether it be willful disregard or willing to cooperate with the PDPC, the remedial and corrective behaviors provided to affected individuals. These affect which provision of law applies and whether the lenient and a more heavy-handed penalties imposed on the breaching organization. These soft functions have not yet appeared in the 2018 Amended Bill framework.

Considering the relatively lower trust individual and business placed on the government agency as well as the lower trust individual have on businesses to protect their personal data, the Singaporean approach when transplanting onto Thai ground could render different outcome. That calls for certain adjustment on the balancing between the risk and gap for business decision-making to involve in compliance with the Bill. That is to say, on Thai ground, the regulation needs more control by increasing the concrete structure so as to provide directions and assurance to business in compliance, thus, narrower gap is left for business to make some counter-interest decisions to deliver trustful behaviors to individuals. Put simply, the difference due to existing attitudes and relationship among Thai actors may not at first fully open for the trust relationship approach, but could increasingly induce trust relationship into the system through cooperation between the business and the government agency.

What appears to be strengths under the 2018 Thai Amended Bill regarding individual rights to personal data and compensation, also contains several weaknesses. The criminal liabilities for intentional exploitation of the sensitive data recognizes the social dimensional value of the personal data, thus expressly recognizing harm from the unauthorized use and disclosure of sensitive personal data and the injury of individual embarrassment and reputation loss from
such activities. Despite the fact that such recognition of harms and intangible injury provide basis for damages in the private claims, individual faces other challenges due to the broad meaning of individual consent, specific procedure and forms regarding complaints, the exemptions of business liabilities due to individual’s fault. These turn out to create difficulties and rather discourage individuals suffered from the breach to seek remedies under this Bill in practice, thus weakening the protection of individual rather than promoting individuals in exercising of such rights to personal data.

C. Conclusion

In conclusion, both the existing Thai FTCA-plus and the Thai PDPA-Lite approaches provide the immediate and direct venues to the data security protection in Thailand, like the ramp and the highway. The analysis found that Thai consumer protection venue is compatible with the transplanting concepts of the U.S. with some adjustment to fit on the Thai ground. Similarly, the 2018 Amended Bill is also compatible locale for transplanting the Singaporean approach with some adjustment to fit on Thai ground. Certain amendments are needed for the transplanted will perform and render the intended outcome of needs because the differences of the existing Thai platforms as well as the flows and forces interplaying on the Thai ground from those in U.S. and Singapore.

For the Thai-FTCA plus, the Thai Consumer Protection Commission needs to be more proactive in enforcement actions in compensation for the inert role of media and public vigilance regarding breach discovery and increasing information transparency. The Thai PDPA-Lite requires more concrete structure than the original PDPA because of the existing higher individual distrust attitudes on business and regulator, thus lesser space should be opened for the business to deliberately exercise free will in handle personal data. Besides, the soft functions were missed from the original PDPA approach, which should be added into the Thai current rigid framework so as to serve the ends of promoting trust and cooperation.

Next, in Part III, I will discuss the considerations for applying both approaches to meet the country’s aims of enhancing trust and cooperation on balancing with promoting privacy self-control in Thailand.

Part III The Considerations: The Highway, The Ramp and The Hinges

In this part, I aim to discuss the considerations for applying both U.S. and Singaporean approaches to Thai Context in order to meet the country’s needs of enhancing trust relationship and cooperation while promoting individual’s self-control or privacy rights in Thailand.

(i) Introducing Soft Approach to the Hard Way: The Trust Function in Command-and-Control Approach

The existing platform provide by the 2018 Amended Bill has only hard functions, to force business to comply with regulator’s command and control over their behaviors. This way will only ensure the individual privacy rights on symbolic level and a set of procedural data security management to be followed by businesses. That means the current Bill does not further right attitudes and motivations for beyond-compliance behaviors and trust relationship to emerge in Thailand, thus not meeting the country’s economic and societal needs.
The existing Thai legal platforms situated in the current forces and flows above and under the Thai ground lacks functions of trust: the trust attitude and motivation for trustful behaviors. Lack of trust attitudes conveyed to business under the current regime means that individual actor needs to depend on the Commission protection rather than businesses themselves. Therefore, such regime does not promote the direct trust relationship between business and individual. The trust relationship thus emerges from the indirect means of regulator’s control and command of businesses to promote their trustworthiness, which is when enough could induce more trust from individual on the business character who would become more dependable to render trust behaviors.

Thus, introducing of soft elements found in the PDPA to the current Thai rigid approach are necessary for providing proper environment for individual-business trust relationship to emerge. The trust attitude and motivation for trustful behaviors can be added by the following means. First, the trust attitude can be communicated through the Bill’s objectives and principles for interpretation that speaks to the business stake of losing consumer trust from non-compliance. Second, the aggravating and mitigating factors when delivering trustful acts to individuals shall be taken into account by the Commission when considering the breach and penalties. Together, this would help assuring business of desirable behaviors and mitigate too-high risks involved in rendering such acts. Finally, the cooperative function shall include business-business relationship and business-regulator relationship. Such cooperative acts will eventually build trust relationship upon between them. These soft functions fitting into the existing Thai regulatory landscape will enhance individual-business trust relationship and cooperation in Thai regime.

The Bill’s objectives do not speak to protecting consumer trust in data processing businesses or the balance between individual right and the free flow of data. Considering together with the lack of interpretative principle such as reasonable person standard, it misses the opportunity to convey the right attitudes to business actors to deliver trustful behaviors in compliance with the Bill.

**Prompt Breach Notification and Remedies as Mitigating Criteria for Penalties**

The specific contexts of Thai privacy have placed limits to the operation of the U.S. and Singapore approaches, which calls for stronger assurance of law. The law however should leave some gap, though not widened as the U.S. and Singapore, for organizations to initiate trustful act towards individuals. The mandate data breach notification law is necessary to increase the organization privacy awareness and practices on the ground and heighten their commitment on trustworthiness and transparency. Section 29(5)\textsuperscript{227} of the 2018 Bill however does not leave a room for organization discretion to assess risks involved in breach, making it becomes another reporting duty, which may not be well-received by those more sophisticated organizations besides its burdensome costs.

These provisions have close resemblance to the new proposed amendment of Singapore in the organization’s obligation to notify affected data owner, and the duty to report to the

\textsuperscript{227} Section 29 (5) to notify the breach of personal data to the data owner without delay. If the breach of personal data exceeds the number of persons specified by the Commission, the data controller shall notify the Commission of the remedies approach without delay. Such notification shall be in accordance with the regulations and methods announced by the Commission. Section 30 (2) to implement proper measures for data security to prevent the unauthorized or undue loss, access, use, correction and change or disclosure of personal data, including notifying the data controller when the breach occurs.
Commission based on scale of affected person. However, the main distinction is that the proposed DBN in PDPA does include the remedial exception along with the technological exception to notifying breach. This ensures that notification may not create fatigue to individuals, while delegating organizations with tasks to exercise reasonable judgment and incorporate individual experience into their responses.

Despite the lack of clear evidence on organization’s willingness to notify breach and remedies unless it needs to follow the legal instruction according to the interview and the incident, it could be seen that global organizations apply higher standards in the firm policy even in the Thai privacy law vacuum and relate their decision with trust. The relationship of trust is therefore still considerably relevant, and could drive from the practices of multinational firms operating in the country to be followed by domestic firms.

The law should take the advantage of this situation to promote post-breach responses and organization trustful behaviors, the Thai commission should consider mitigating and aggravating penalties to provide incentives for the firms to be more trustful towards individuals. The Bill could add the remedial exception to prevent overload of information to consumer and desensitization.

The Thai consumer protection law can fill in the current gap and increased individual awareness through consumer contracts by mandating to include a clause requiring business in critical sectors to notify breach and remedies to affected consumer. This will increase publicity, engage media to prime privacy into the spotlight, and also enable consumer to find a proper channel to complain and be heard by the regulator.

**Transposing Blind Trust to Informed Trust: Raising Consumer Awareness and Business Trustworthiness**

The Thai consumer protection venue, the FTCA-plus, could work in complementary with the Bill in raising consumer awareness and business trustworthy character in advertising and contracts with consumers as well as information transparency that distinguishes blind trust from informed trust. This aspect of protection will further cultivate the self-control aspect of privacy and information equality in needs of discerning choice of consumption. By this venue, the media platform and advertising companies also need to improve the screening procedure of deceptive and misleading data security and privacy policies and statements because they also have liabilities under the Thai Consumer Protection Act.
Chapter 6

Moving Forward

I. Moving Thailand’s Privacy Elephant
   *A Thread, a Sugarcane Stick and a Pull*

As Thailand moves towards realizing the long-time proposed Digital Economy blueprint of Thailand 4.0, the value-based economy that seeks to blend innovation, technology and creativity within the country’s economic productivity. Strengthening trust relationship in the country is necessary to meet this tantalizing goal, similar to the reform the critical industry’s infrastructure. Much doubt has been placed on the country’s readiness to achieve this objective. The new constitution grants the right basis to data privacy, but without the venue to claim. To this date, the personal data protection bill, the heart of legal reform, with which to develop the trust ecosystem for e-commerce and trade facilitation, has not yet been enacted. Together with the blindness due to the lack of awareness or direct breach experience from both consumer and organizations parties, data privacy remains a big puzzle, neither fully understood nor integrated into the context of society.

To move this unrealized right into certain direction, the dissertation proposes to integrate trust language and motivation for an organization’s actors into the current 2018 bill and to draw the organization’s interest in adopting better privacy practices. Trust relationship should be added into the language of the bill to set the right focal points for organization actors along with the trust principles that ensures reasonable judgment of organization in handling personal data in compliance with law. In action, the new regulator should amplify language of trust by considering mitigating penalties to be applied when organization initiates prompt response and remedies to individuals and cooperating in admittance of breach. The dissertation expresses caution on the current rigidity of the proposed mandatory data breach notification requirements, which miss the opportunity to cultivate a capability to exercise good business judgment in taking individual privacy interests into their decision-making processes in response to a breach.

With the backup force from the Thai Consumer Protection Commission to trigger an investigation against the unfair and deceptive privacy and security advertisements of the products and services, and its readily-to-use power to regulate consumer contracts in the business processing consumer sensitive data, the media can become more engaged in discovery of data breach and raise public awareness. The dissertation proposes a combination of these strategies to end the Thai data privacy stagnancy, and to move closer to the dual ideals set on promoting privacy rightness and trust relationship.

II. A Forward-Looking Privacy Movement

The Crack in the Ground
   *Breach, Reinterpretation, Reinforcing Trust Relationship*

The current situation of data breach, confusion and gaps can be seen as a crack in the ground, which offers an opportunity for reinforcing trust relationship into the dialogue of privacy. Law can encourage and infuse right motivation for organization to correct and remedy actions towards consumer. The benefit is two-fold: for consumer, actual and prompt remedies are provided in term of apology, self-admittance of mistake, corrective and remedial actions; for breaching organization, the chance to demonstrate trustworthy act and regain trust in long-term
relationship from consumer in additional to correcting damaged reputation. How the existing jurisdictions—the regulatory platforms and the enforcement styles—speak to these individual trusts as a organization’s stake, then making the most from this situation to transpose the breach of trust into a trust-enhancing relationship.

**Trust Built into the Language of Privacy Law**

*Design Cultivating Trust Relationship*

What are the legal roles attributing to the environment of “willingness” and “risk-taking acts”? This part observes the design features of a regulation that could infuse trust values into a legal climate influencing organizational compliance. The design is deconstructed into four elements: the venues, the actors’ behaviors, the forces and flows, and the space.

**A. The Hard Structure: Venue for Direct Relationship**

The platform or venue provides assurance for organizations to act on trust to the individual party. Singapore law provides a venue for parties to seek self-resolution through individual compliance made to the organization’s DPO and provides mediation procedure opted by parties before the Commission’s review. The Commission applies mitigating criteria to the desirable post-breach behaviors of organization party before and during investigation such as prompt breach notification and remedies provided to affected individuals.

Rather, it is clear that the FTC decisions demonstrate a degree of reliance on an indirect approach rather than a direct relationship approach of breach discovery and remedies. This demonstrates, for instance, the FTC’s desire for a proper venue for an outside party, e.g. the media and researcher group, to become involved in a breach discovery and to report with increased transparency in order to put pressure on the business untrustworthy behaviors.

**B. The Soft Structure: Principles and Motivations Assigned to each Actor.**

These soft functions of law are the objective, interpretative principles, predisposition of characters and attitudes for business and individual to interact with each other. Trust is clearly established as the legal objective of the PDPA. Providing that reasonable person standard is an interpretative principle for compliance with the PDPA, the law embraces the human elements, duty of care and individual party’s interest in a relationship to be considered by the organization party. The premise of dependent relationships between individual and organization party is seen; the law does not attempt to empower individual with choice and decision, but ensure reasonable judgment of business party in handling data.

On the other hand, the U.S. approach is based on self-control and attitudes of distrust, motivated by the objective qualities of trustworthiness, transparency and integrity.

**C. The Silent: Reading Between the Line and Filling in the Gap.**

In the gap and ambiguity, whether it is intentionally or unintentionally provided by the law, there remains an open space that invites organization actors to read between the lines, and bear
some risk to initiate trustful decisions to individual party in notifying breach and remedies. Within the unregulated space, law need to equip organization’s actors with a compass for steering into desirable direction to prevent exploitation. The hard and soft structure of a regulation assures such a direction and reduces risks to the acceptable level to initiate trust acts.

The Singaporean approach illustrates a case that provides a proper environment for trust relationships. The law does not mandate what needs to be done after the breach, which leaves a considerable gap for a business to exert its will to perform trustful behaviors such as admittance of breach, corrective and remedial actions in favor to the consumer. The high risks inherent in such a performance on organizational reputation and the loss of consumer trust are mitigated by the Commission’s criteria that recognizes and endorses such behaviors as mitigating factors in assessing a breach. As seen from the PDPC decisions illustrated in Chapter 4, there are many instances in which the breaching organizations provided apology, notification and compensation to individuals after the breach.

The U.S. FTC approach does not recognize these trustful behaviors towards a consumer nor regards them as mitigating factors. While it does allow a business party to decide its response to an individual after the breach, exposure to too much risk and uncertainty from the lawsuits, together with a lack of clear desirable values attached to the law, could restrict organizational decision-making in a way that provides trustful act towards a consumer.

Thailand’s 2018 Amended Bill, despite mimicking the Singaporean outer structure, however, does not integrate trust relationship value within its design and implementation. It primarily relies on force and fear-driven cooperation, which lacks the integral trust relationship functions and provides no space for expression of will. The strong presence of a command-and-control approach, the criminal liabilities involved and the considerable discretion left to the Commission do not provide a proper environment for a business to initiate a trustful act to a consumer. Cooperation with the agency when successfully achieving compliance could enhance consumer trust.

From this point of view, the right regulation for promoting an individual-to-organization trust relationship should have at least the following components. First, it expresses consumer trust as the interests or motivations for a business actor to comply with, and when not complying, consumer trust becomes at stake. Second, it constructs an open space where a business party can exert free will, and initiate action to protect a consumer’s interests without a command of law. As the business actor navigates in the unregulated space, unclear of what to do, the first component gives a sense of right direction, a sense of assurance thus reducing risk and uncertainty borne by the unclear command.

**Organization Materialism and its Privacy Spiritualism on Trust Relationship**

The interview excerpts of data privacy officers in Singapore provide evidence of an organization’s worldview situated in trust relationships. Organizations understand the meaning of individual privacy based on subjective individual interest. Their decisions to render post-breach responses – i.e. communication of breach notification and remedies – are dependent on individual interpretation and reaction to them. Organization’s post-breach responses are motivated from individual experience and the maintenance of trust in their ongoing relationships
with the organization. What is at stake or of concern is trust relationship from bad individual experience at the time of breach.

In the context of the U.S. Bamberger and Mulligan’s study on privacy on the ground demonstrates similar view described by the CPOs in U.S. based firms, as the study framed from the consumer expectation approach. The convergence shed light onto the dynamics of the relationship and the organization’s worldview based on trust to as a communal, or a universal tool that governs parties’ behaviors in privacy.

In actions, the PDPC cases illustrate organizational patterns of beyond-compliant behaviors, aligning with such established worldview on trust relationship. In the context of the U.S. where privacy as a right is more established, Bamberger and Mulligan’s privacy on the ground study illustrates the behaviors in the U.S. firm which adopts the pro-privacy practices despite the existing fragmented privacy regulations. Non-legal factors such as consumer trust and reputation could be driving privacy of corporations on the ground.

**Law Flows over Organizational Logic**

The proposed mandatory DBN in the PDPA amendment, especially demonstrate the law’s strategic act to leave the remedial exception for the organizational to initiate trustful responses to individual rather than notifying breach. This intention is clearly an instance that law leaves gap. In Chapter 4, the analysis of PDPC decisions demonstrated that these post-breach behaviors such as voluntary apology, breach notification and remedial actions provided to affected individuals by breaching organizations were consistently recognized by the PDPC as mitigating factors in determining a breach and penalties. The FTC in data security breach decisions did not consistently recognize similar patterns in their decisions. An in-depth investigation is needed to determine whether similar trust relationship logic or reputational fear drives the post-breach behaviors in the U.S. requires, and whether low visibility firms in cases of insider breach perform beyond-compliant behavior in post-breach responses.

**The Open-Unfinished Gap and Fill-In**

Privacy law, when left somewhat open, can bring together the organizational ideal and logics and can utilize organizational resources to serve an individual well-beings from trust relationships.

**More than Legally Expected**

In the context of Singapore, where privacy as a right is not established, the existing function of trust relationship enhances privacy-pro practices, thus surpassing the limits posed by legal ideals and the notion of rights to cover social dimension of privacy – reputation loss, embarrassment, the intersubjective interests beyond reasonable expectation at the time of data sharing. The humanistic dimension of privacy arguments put forward by Nissembuam is also observed in PDPA operationalization in terms of the reasonable standard treatment of personal data, care, breach intent and intersubjective privacy injury recognized through regulators enforcement. The U.S. privacy rights-based ideals fail to recognize, or even reject these values. This calls for the re-examination of legal ideals to ensure that the law itself does not becomes a hindrance to the emerging norms on trust relationship, and to encourage such norms to thrive in serving individual well-being regarding data breach.
My arguments for protecting privacy through promoting trust relationship align with Hartzog & Richards’ work. Singapore contributes to a case for privacy design for promoting trust relationship, in which the ideals – hard and soft legal structure and gap, motivating forces and regulatory styles and specific case enforcements as in Chapter 2 and 3 – provide a specific way as to how the law can build upon organizational infrastructure and rationale of a trust relationship to better remedy individuals from a data breach.

The case of Singapore demonstrates that when the law is willing to lose ground and become open to a reliance upon organizational logic, it has the capability to tune in and utilize the organizational managerial logic together with the existing worldview on trust relationship and individual experience towards a better privacy outcome. The interviewee responses highlight the culture of complaint in Singapore that prompts an organization to deliver only a satisfactory experience to individuals and to opt for prompt and direct breach notification and/or more effective remedies. The case interprets the broader measurement for when individual recognizes their rights have been violated to including lodging complaint with friend in social media as threat to enable direct, prompt and effective remedy. The no ideal of privacy of Singapore law allows the on-the-ground reality and the flow of experience outside the legal procedure and logics to complete the legal vision of successful compliance.

That is, when the law in its silence finds the attunement to an organization’s interest, it performs in coordination with the organization’s operational logic of privacy in the language of trust relationship. The law in its rigidity as a symbol of rights performs as a reminder of agreed meaning, content, and upholds rightness and assurance to parties navigating in accordance with the law. In its strategic mode, the law can negotiate with organizations and assign motivation for better privacy practices towards individuals.

Steering the right attitude and motivation for businesses in complying with law is a matter of regulatory design. The hard, the soft and the silent function of law that emphasizes desirable values and communicate them in the way that aligns with the organization interest or logic when put into practice. Trust relationship itself in language and action reminds us right attitude and motivation of privacy practices. Trust relationship approach is dynamic and sustainable in that it is driven by the momentum of the past, and itself also carries the forward-looking notion as a party is motivated by future interests to maintain such relationship of trust. Its upside force can encourage a party to go beyond expectation to gain trust. Fear driven approach created by reputation could produce similar beyond compliant effects. Trust relationship has some added benefit as a party who acts on trust preserves their capacity and trust attitudes.

By accepting that an organization can be an instrument to allocate justice – which concerns timely remedies and less cost with the assistance of social media complaint – the law can in turn focus on the legal influence on meaning-making and communicative ability to reach a mutual understanding for better coordination with organizations. It does not necessarily mean that the law loses control, but utilizes both the resources to the fullest extent and an existing organization’s trust relationship worldview in society to better the society at an individual relationship level. The second level is to create points of mutual interest for organizations to cooperate with others in protecting individual personal data.
A question remains open for further discussion: “How can the law strive to be relevant in this information age, and be maintained as a primary source of assurance in competing with other assurance systems such as technology and organizations?” I reexamined the legal ideals that somehow stand apart from reality on the ground and the possibility for repositioning these legal ideals to align, decentralize and open to participation with other instruments in society in order to fulfil the legal objectives of protecting individual privacy from rightness and a pragmatic view. Openness and relevance could be a resort for law function in the information age.

There is a way between voice and presence, where information flows.
In disciplined silence it opens; with wandering talk it closes.

– Rumi
References


Decisions of Singapore’s Personal Data Protection Commission

Re K Box Entertainment Group Pte Ltd and another [2016] SGPDPC 1
Re The Institution of Engineers Singapore [2016] SGPDPC 2
Re Fei Fah Medical Manufacturing Pte Ltd [2016] SGPDPC 3
Re Universal Travel Corporation Pte Ltd [2016] SGPDPC 4
Re Yes Tuition Agency [2016] SGPDPC 5
Re Challenger Technologies Limited and another [2016] SGPDPC 6
Re Metro Pte Ltd [2016] SGPDPC 7
Re Full House Communications Pte Ltd [2016] SGPDPC 8
Re Singapore Computer Society [2016] SGPDPC 9
Re Central Depository (Pte) Limited and another [2016] SGPDPC 11
Re Spear Security Force Pte Ltd [2016] SGPDPC 12
Re Fu Kwee Kitchen Catering Services and another [2016] SGPDPC 14
Re Aviva Ltd and another [2016] SGPDPC 15
Re ABR Holdings Limited [2016] SGPDPC 16
Re GMM Technoworld Pte Ltd [2016] SGPDPC 18
Re Smiling Orchid (S) Pte Ltd and others [2016] SGPDPC 19
Re My Digital Lock Pte Ltd [2016] SGPDPC 20
Re The Cellar Door Pte Ltd and another [2016] SGPDPC 22
Re Propnex Realty Pte Ltd [2017] SGPDPC 1
Re JP Pepperdine Group Pte Ltd [2017] SGPDPC 2
Re Tech Mahindra [2017] SGPDPC 3
Re National University of Singapore [2017] SGPDPC 5
Re Tiger Airways Singapore Pte Ltd and others [2017] SGPDPC 6
Re Furnituremart.sg [2017] SGPDPC 7
Re Exceltec Property Management and two others [2017] SGPDPC 8
Re Hazel Florist & Gifts Pte Ltd [2017] SGPDPC 9
Re Data Post Pte Ltd [2017] SGPDPC 10
Re Orchard Turn Developments Pte. Ltd [2017] SGPDPC12
Re Aviva Ltd [2017] SGPDPC 14
Re BHG (Singapore) Pte. Ltd [2017] SGPDPC 16
Re Social Metric Pte Ltd [2017] SGPDPC 17
Re ComGateway (S) Pte. Ltd [2017] SGPDPC 19
Re Credit Counselling Singapore [2017] SGPDPC 18
Re Individual Data Broker [2018] SGPDPC 1
Re Aviva Ltd [2018] SGPDPC 4

Federal Trade Commission Cases

In the Matter of CardSystems Solutions, Inc., et al. FTC File No. 052 3148
In the Matter of ChoicePoint Inc. FTC File No. 052 3069
In the Matter of DSW Inc., FTC File No. 052 3096
In the Matter of Superior Mortgage Corp., FTC File No. 052 3136
In the Matter of BJ’s Wholesale Club, Inc., FTC File No. 042 3160
In the Matter of Vision I Properties, LLC, et al., FTC File No. 042 3068
In the Matter of Sunbelt Lending Services, Inc., FTC File No. 042 3153
In the Matter of Nationwide Mortgage Group, Inc. et al., FTC File No. 042 3104
In the Matter of Petco Animal Supplies, Inc., FTC File No. 032 3221
In the Matter of MTS, Inc., et al., FTC File No. 032-3209
In the Matter of Guess?, Inc., FTC File No. 022 3260
In the Matter of Microsoft Corporation, FTC File No. 012 3240
In the Matter of Eli Lilly And Company, FTC File No. 012 3214
In the Matter of Rennert, Sandra L., et al., FTC File No. 992 3245
In the Matter of VTech Electronics Limited, FTC File No. 162 3032
In the Matter of Lenovo, Inc., FTC File No. 152 3134
In the Matter of TaxSlayer, FTC File No. 162 3063
In the Matter of Uber Technologies, Inc., FTC File No. 152 3054
In the Matter of D-Link, FTC File No. 132 3157
In the Matter of Ashley Madison, FTC File No. 152 3284
In the Matter of ASUSTeK Computer Inc., FTC File No. 142 3156
In the Matter of Henry Schein Practice Solutions, Inc., FTC File No. 142 3161
In the Matter of Oracle Corporation, FTC File No. 132 3115
In the Matter of Bayview Solutions, LLC, FTC File No. 142 3226
In the Matter of Cornerstone and Company, LLC, FTC File No. 142 3211
In the Matter of Snapchat, Inc., FTC File No. 132 3078
In the Matter of Credit Karma, Inc., FTC File No. 132 3091
In the Matter of Fandango, LLC, FTC File No. 132 3089
In the Matter of GMR Transcription Services, Inc., FTC File No. 122 3095
In the Matter of foru™ International Corporation, FTC File No. 112 3095
In the Matter of Genelink, Inc. FTC File No. 112 3095
In the Matter of Accretive Health, Inc. FTC File No. 122 3077
In the Matter of TRENDnet, Inc., FTC File No. 122 3090
In the Matter of CVS Caremark Corporation, FTC File No. 072 3119
In the Matter of ControlScan, Inc., FTC File No. 072 3165
In the Matter of HTC America Inc., FTC File No. 122 3049
In the Matter of CBR Systems, Inc., FTC File No. 112 3120
In the Matter of PLS Financial Services, Inc., et al., FTC File No. 1023172
In the Matter of Compete, Inc., FTC File No. 102 3155
In the Matter of Wyndham Worldwide Corporation, FTC File No. 102 3142
In the Matter of EPN, Inc., also d/b/a Checknet, Inc., FTC File No. 112 3143
In the Matter of Franklin's Budget Car Sales, Inc., FTC File No. 102 3094
In the Matter of RockYou, Inc., FTC File No. 102 3120
In the Matter of Upromise, Inc., FTC File No. 102 3116
In the Matter of Lookout Services, Inc., FTC File No. 102 3076
In the Matter of Ceridian Corporation, FTC File No. 102 3160
In the Matter of Fajilan and Associates, Inc, FTC File No. 092 3089
In the Matter of ACRAnet, Inc., FTC File No. 092 3088
In the Matter of Settlement One Credit Corporation, FTC File No. 082 3208
In the Matter of Rite Aid Corporation, FTC File No. 072 3121
In the Matter of Twitter, Inc., FTC File No. 092 3093
In the Matter of Dave & Buster's, Inc., FTC File No. 082 3153
In the Matter of LifeLock, Inc., FTC File No. 072 3069
In the Matter of James B. Nutter & Company, FTC File No. 072 3108
In the Matter of Rental Research Services, Inc., FTC File No. 072 3228
In the Matter of Genicia Corporation and Compgeneks.com, FTC File No. 082 3113
In the Matter of Navone, Gregory, FTC File No. 072 3067
In the Matter of Premier Capital Lending, Inc., et al., FTC File No. 723 004
In the Matter of Reed Elsevier Inc. and Seisint, Inc., FTC File No. 052 3094
In the Matter of TJX Companies, FTC File No. 072 3055
In the Matter of ValueClick, Inc., FTC File No. 072 3111
In the Matter of Goal Financial, LLC, FTC File No. 072 3013
In the Matter of Life is good, Inc. et al., FTC File No. 072 3046
In the Matter of American United Mortgage Company, FTC File No. 062 3103
In the Matter of Guidance Software, Inc., FTC File No. 062 3057
Appendix A
<table>
<thead>
<tr>
<th><strong>PDPC Cases</strong></th>
<th><strong>Post-Breach Response</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. K-Box and Finantech (Entertainment Chain)</strong>&lt;br&gt;Breach involved public disclosure of 317,000 members personal information on third party website (pastebin.com) as notified by the Real Singapore Website, unknown call, social media and employees. (para 13). The leaked data includes name, NRIC and passport number, mailing address in Singapore, contact number, email address, gender, nationality, profession and date of birth (para 3). On the same date of 16 September 2014, it posted a letter on its website notifying of breach. (para 13) The cause was likely from hacker’s use of admin user account with weak admin password, and planted a malware control and command centre to retrieve and export the members’ data. The Commission issued the largest amount of penalties $50,000 (the maximum is 1M) to K-Box and $10,000 for Finantex to be paid in addition to the DPO to be appointed in the timeframe of 30 days.</td>
<td>• Notify Affected Customers on the same day of discovery¹&lt;br&gt;• <em>(MT)</em> Deleted and disabled unauthorized admin account with weak password the next day after being notified of breach by its vendor and most remedial actions were taken within a month after breach discovery.&lt;br&gt;• <em>(AG)</em> Not forthcoming in providing information during the investigation. They had only provided bare facts. Its vendor also failed to be forthcoming with the 7 months’ response to PDPC.</td>
</tr>
<tr>
<td><strong>2. Challenger Technologies Limited and Xirlynx Innovations (Retailer of IT products)</strong>&lt;br&gt;Insider leak of 165,306 ValueClub membership information including names, membership programs and points and expiry dates forwarded in the email to other members. The errors in sending process causing data of a member being exposed to others. The Commission considered limit of leak to insiders and non-sensitive and non-harmful nature of information and other remedies provided to issue warnings to Challenger Technologies and its data intermediary for failing to make reasonable security arrangements to prevent unauthorized disclosure.</td>
<td>• <em>(MT)</em> It had taken remedial actions to inform the affected ValueClub members regarding the data breach and to rectify the mistakes caused by Xirlynx’s error. In addition, it had taken the extra precautionary step of terminating Xirlynx’s services upon discovering the cause of the data breach, and it reviewed its ValueClub communication processes to prevent a reoccurrence. (para. 12) &lt;br&gt;• <em>(MT)</em> cooperative to investigation (para 37c) &lt;br&gt;• <em>(MT)</em> The Commission also notes that Challenger had taken several proactive steps to remedy the breach,</td>
</tr>
</tbody>
</table>
3. FEI FAH MEDICAL MANUFACTURING (Medical Manufacturing, Healthcare)

The company’s website was hacked by the unknown resulted in 900 user IDs and passwords and email address and personal phone number being disclosed on publicly accessible third party website (pastebin.com). The PDPC investigated and alerted the FEI FAH on the incident. FEI FAH took steps to instruct its Hong Kong-based data intermediary IT Factory to implement remedial actions, but not able to ensure remedies. The Commission found that FEI FAH failed to implement proper and adequate protective measures to secure its website and server, issued the corrective order including direction to implement new websites, conduct vulnerability scan, and regular report the implementation to the PDPC in addition to penalties of $5,000.

- It had no knowledge of data leakage prior to receiving the Commission’s Notice. However, after being alerted to the Data Leak, it sent email notifications to all affected individuals, informing them that there had been hacking activity on the Site and that their personal data may have been compromised. (para. 11)
- (AG*R) not being cooperative or forthcoming in the Commission’s investigation for taking almost a month to response.
- (AG*R) Even though it instructed its HK website vendor to fix the issue, its website still collected more information and the remedies had not been ensured until 10 months after first breach discovery, which is deemed undue delay.

4. Metro PTE LTD (Department Store)

Membership information of 445 individuals were disclosed on the third party website by hackers in March 2015. The leaked data include names, personal email addresses, NRIC numbers, personal mobile phone numbers, and dates of birth and Facebook user IDs. Individual complainant discovered in March 2015 personal data of herself and family members by conducting Google search after received unknown call. The Commission found the leak caused from only hacking activities in February 2014 before the effective date of the PDPA, but it still failed to provide adequate

- The Respondent instructed its IT vendor to remove any user information from the server of the hacked corporate website and engaged an expert to carry out an assessment and audit of the security of its internal as well as external i.e. internet systems, and reported the Commission in July 2015.
- (MI*R) The Commission
security arrangement thereafter. It rendered only a warning for the breached organization.

considered that the corrective action, i.e. strengthening website security and internal IT auditing and assessment was made *shortly after the breach* (1-2 months). However, it still failed to patch at least one significant issue after the following breach.

- *(Mi*R)* No further evidence of leak after PDPA in effect

<table>
<thead>
<tr>
<th>5. SINGAPORE COMPUTER SOCIETY</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Professional social group event)</em></td>
</tr>
<tr>
<td>The insider leak involved the registration information of 214 individuals being forwarded by an employee to other members on the list. Leaked information included full names, NRIC numbers, contact numbers, email addresses, organization and designation information. After receiving notice from some registrants of concerns about the unauthorized disclosure of their personal data, the respondent recalled email 40 minutes after mailing out and notified the Commission that it inadvertently disclosed certain personal data of individuals attending an event organized by the Respondent. The Respondent’s DPO subsequently sent an official email apology to 11 registrants who had raised concerns to the Respondent over the incident. All accepted the apology and did not pursue the matter further. The Commission found the respondent failed to provide reasonable data security practices due to poor handling of personal data and issued warning.</td>
</tr>
<tr>
<td><em>(Mi</em>R)* Most are business contact information (generally not Personal Data under PDPA);</td>
</tr>
<tr>
<td><em>(Mi</em>R)* prompt action taken by respondent to recall the emails though enabling to recall total emails sent.</td>
</tr>
<tr>
<td><em>(Mi</em>R)* informed the PDPC of the data breach voluntarily and was cooperative during the investigation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. FULL HOUSE COMMUNICATIONS PTE LTD</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Advertising event organizer)</em></td>
</tr>
<tr>
<td>The auto-filled drop down menu on the respondent’s computer program allowed other individual participants to access information of other individual customers who participate in the lucky draw events. Information requested by the form included the name, identity card number, occupation, contact number, email address and residential address. An individual with his mother who purchased participated in the event made complaint to the PDPC. The PDPC found the</td>
</tr>
<tr>
<td><em>(Mi</em>R)* Respondent took action shortly after the complaint was made to stop the use of the drop-down boxes and to arrange for its staff to fill in the forms.</td>
</tr>
</tbody>
</table>
respondent, by enabling the auto-filled text function, failed to provide reasonable security protection and issued warning. In issuing direction, it considered the impact is limited due to narrow gap for observing and collecting information, and the prompt correction made by the respondents.

7. THE INSTITUTION OF ENGINEERS SINGAPORE
(Professional Community)
The leak of 60,000 Institution of Engineers Singapore member's log-in passwords and IDs of members being disclosed on third party website accessible by the public. An individual wrote to IES on 1 October 2014 about the data leakage. IES self-reported the Commission and provided vulnerability scan report in November 2014. The cause was likely from the cross-site scripting, found among 48 high severity security flaws on its website according to the first vulnerability scan report. The Commission viewed that anyone with a valid user ID and password, though posted randomly by hackers, would effectively be able to access the entire profile of an IES member and identify him or her. It found the IES had made insufficient effort to ensure the security of personal data stored on the Site (e.g. not encrypting the data storage, not preventing common threats such as SQL and CSS, not making arrangement with its vendor on security measures). As a result, numerous security vulnerabilities existed in the site at the time of the Data Leak, which could have been reasonably detected and patched by available means. The Commission issued financial penalty of S$10,000.00 and the direction for IES to conduct further vulnerability scan on its website, patch all weaknesses, report the results and measures taken by IES to the PDPC within 60 days.

* • (Mi*R) forthcoming and cooperative with PDPC in investigation
• (Mi*R) Prompt measures taken after breach discovery i.e. disabling members' portal on its site, password reset for all members' accounts, and its admin accounts.
• (Mi*R) Next-day email notification to all IES members, informing them of the hacking activity on the site, as well as the measures taken to minimize damage
• (Mi*R) removal of the telephone numbers and addresses of IES members previously stored on the database of the Site.
• (Mi*R) conducting additional security scan and patch all identified vulnerabilities.

8. CENTRAL DEPOSITORY (PTE) LIMITED and Toh-Shi Printing (Toh-shi I)
CDP provides clearing, settlement and depository facilities in the Singapore securities market. Toh-shi is the external vendor engaging by CDP to process the printing of CDP’s accountholder statements, and thus a data intermediary.

Toh-Shi’s employee caused the errors during the

CDP (Principal organization)
On 11 June 2015, CDP reported the PDPC after received reports from 6 accountholders of receiving wrong statements of May containing information of other account holders and, on the same day, issued press release to inform and apologize for the breach incident.
The sorting process of the monthly statements. As a result, the mails sent out to accountholders contain information of other accountholders on the second page. The leak affected 195 accountholders and 92 of them received the sensitive financial data i.e. name, address and account number, securities holdings, transaction summary, payment summary belonging to other holders.

The Commission satisfied with CDP’s measures and found it had adequate security policies and procedures in place i.e. the security arrangement and transfer protocol entered into with Toh-Shi.

The Commission imposed a financial penalty of $5,000 on Toh-Shi for failing to implement proper and adequate verification while processing personal data as a data intermediary. The human error due to the manual process in this case, the sorting conducted manually by only one person, could have been minimized by the processes or technology solutions.

On 15 June 2015, CDP reissued the corrected statements with an apology letter to the 195 affected account holders. On 17 June 2015, its parent company started to contact the affected account holders to assist with any queries or concerns, and to give them an option to change their CDP account numbers.

From what the Commission noted that no accountholders requested changes.

Toh-Shi had review its staff training, add more layer of check, and employed the technology-solution to check misaligning page, barcode and seek its customer approval layers before disclosure.

(AG*R) A considerable number of affected individuals (195 in total)
(AG*R) Sensitive data involved.
(AG*R) breach could have been avoidable.

(PDPC (same day) and being cooperative during investigation.
(AG*R) prompt remedial and preventive actions following the data breach incident.

9. SPEAR SECURITY FORCE PTE.LTD
Condominium Security Service

The security guards under respondent’s supervision had left the visitor’s book open and unattended at the Condominium’s entrance during the lapses allowing unauthorized access of personal data. The complainant, a resident, raised concerns to both the management and the respondent, but did not an adequate response. The personal data in the book included the visitor’s name, mobile phone number, time of entry, the unit number visited and the purpose of the visit. The Commission considered that the respondent failed to provide reasonable security arrangement. Warning was issued due to

- securing the log book only after it received complaint and feedback e.g. instructing guards on duty to hand over the book and not to disclose to any third party, keeping the book within the sight of security camera, and issuing warning and penalties for employee violating the policy.
10. Fu Kwee Kitchen Catering Services and Pixart (Catering Services and its online order maintenance servicer)

A customer reported the PDPC that she could retrieve another customer’s order details and personal data i.e. name, postal address and contact number by changing the numerals at the end of the online order url. A customer’s order did not expire. Anyone who had the exact URL or who had correctly guessed the parameters could potentially access all the personal data of Fu Kwee’s customers.

The Commission found both respondents failed to implement proper and adequate measures to prevent unauthorized access of personal data. A financial penalty of $3,000 and $1,000 were imposed on Fu Kwee Kitchen Catering Services and its data intermediary, Pixart, respectively, including directions for Fu Kwee to send employees for training, appoint a DPO and conduct a security audit of its website.

Fu Kwee was unaware receipt of the Commission’s notice. Two weeks later, it instructed its data intermediary to address the issue. No notifications were sent by either Fu Kwee or Pixart to the customers affected by the data breach.

Fu Kwee (AG*R- Breach) Fu Kwee’s disregard for its obligations to appoint DPO or put in place the policy after receiving notice from PDPC.

Pixart (AG*R) not forthcoming in providing information on anyone who had the exact URL or who had correctly guessed the parameters could potentially access all the personal data of Fu Kwee’s customers.

Pixart (AG*R) not forthcoming in providing information on (Mi*R) Active and acceptable steps taken to fix the issue within about two weeks after learnt from PDPC of data breach.

11. Aviva Ltd and Toh-Shi Printing (Toh-Shi II) Insurance group and mail out service provider (MAS)

Erroneous annual premium statement were mailed out to 7,794 insurance policy holders disclosing personal information of the other policy holder including name of dependent, the sum assured, the premium amount, the type of coverage belonging to 8022 individuals of the other group. The error caused by Toh-Shi’s employee failing to spot the mismatched data during the sorting process.

The Commission did not find breach for Aviva for “it has undertaken an appropriate level of due diligence to assure itself that its data intermediary, Toh-Shi, is capable of complying

On 8 March, the same day with the mailing out, Aviva informed Toh-Shi that 3 policyholders received statements of others.

On 9 March, the PDPC and the Monetary Authority of Singapore was also notified of this incident by Aviva on 10 March 2016

On 10 March, Aviva called for a recovery meeting.

On 11 March, Toh-Shi reprinted and sent out the 7,794 corrected statements together with an apology letter prepared by Aviva and a S$50
with the PDPA and Aviva had no direct part to play in the actual breach itself. The data breach was mainly caused by Toh-Shi’s staff failing to comply with its own security measures and procedures by conducting further sorting after the final approval by Aviva and resulted in penalties of $25000.

| 12. ABR HOLDINGS LIMITED  
*Restaurant Chain*  
The respondent’s Swensen’s Kids Club website allowed access to a member’s name and DOB by entering either a membership number or valid ID number (such as NRIC or birth certificates). Complaints made by individuals before the PDPC came into effect and again in a few weeks after with more complaints. A Warning was issued by the PDPC for the failure to provide reasonable security measures considering available tools for retrieving personal data by simulating the number in sequence. |

| shopping voucher to affected policyholders and a waiver of 1 month’s insurance premium as a token for the inconvenience. |

| Toh-Shi  
*(AG*R Breach)* Large number involved, sensitive nature of data, not merely from a financial perspective but can also be socially embarrassing, second breach within a year.  
*(Mi*R Breach)* Prompt notice given to the PDPC and remedial action (e.g. reminding staffs to adhere to the procedure), being cooperative during investigation. |

| On the same day, the respondents remove the display of member’s name and DOB when the account is accessed, left only the redemption status, stamp points and expiry date.  
*(Mi*R) Prompt Remedial Action  
(Same-day with the second notice from the PDPC)  
*(Mi*R) Occurrence in the first week after PDPA came into force.  
*(Mi*R) Data limited to DOB and Name (of kids) |

| 13. GMM Technoworld Pte.  
*SME Gadget retail Products*  
The new plug-in on platform used by the respondent collected and publicly disclosed 190 individuals’ customer information provided in the warranty registration form, including the customers’ names, email addresses, mobile phone numbers and residential addresses without company’s awareness. The Plug-in was rather designed display information, and the respondent’s lack of awareness, wrong use without proper configuration resulted in breach of section 24 and $3000 penalties. |

| *(Mi*R) cooperative and provided its responses on a timely basis;  
*(Mi*R) immediate steps taken to stop the further unauthorized disclosure, and implemented corrective measures to protect its customers’ personal data. |

| *(Mi*R) Limited time exposure of half an hour and one individual affected, a non-systematic error of |

| 14. My Digital Lock  
*Lock and safety products*  
A warning issued for the facebook post made by a |
company’s personnel about the conversation on group chat including customer mobile and residential address just to save on the computer desktop.

15. Smiling Orchid

*SMEs food caterer*

Orders placed for Smiling Orchid’s bakery and catering services through its website including his full name, residential address, mobile number, workplace address and workplace email address. The Complainant did a random search of his full name on www.yahoo.com.sg. Among the search results was a URL link to a website containing details of the Complainant’s Order. In addition, by changing the numerals at the end of the URL, the order details of other customers could be accessed. The Complainant reported the Data Breach Incident to Smiling Orchid but did not receive any response. It showed the overall lack of security awareness of Smiling Orchid and failure to make reasonable security arrangements. It further clarified the duty of organization or data controllers to follow through with the procedures to check that the outsourced provider is indeed delivering the services (para 51-52.)

Not forthcoming or cooperative, and the same breach incident occurred after being informed by PDPC and failure to fix at the cause of problem, the way it put all data base at risk. The Commission emphasized that it was no excuse under Section 24 that Smiling Orchid being SME with no technical expertise. Though, the Commission took into account the steps taken by Smiling Orchid to remedy the breach, including engaging a new IT vendor to revamp web.

$3000

16. Cellar door and GIW

*food and wine products and website operator*

The leak of personal data found on Pastebin, a third-party public accessible website, included partial Cellar door’s customer database comprising of full names, mobile and residential telephone numbers, residential addresses, email addresses and passwords. The respondents learned of breach from the Commission. The Commission found both respondents’ measures failed below the standard reasonably expected e.g. inadequate security policies and processes to protect the personal data, including the lack of security testing, ongoing maintenance, policy or process in place and the lack of threat prevention i.e. no server firewall installed, unencrypted login credentials. Penalties of $5000 and $3000 were issued to Cellar door and GIW respectively.

In assessing the breach and the remedial directions, the “mitigating and aggravating factors” set out below.

- (AG*Breach) Both shows the lack of awareness and knowledge of security protection i.e. being unable to identify the cause of breach
- (AG* Breach) Not being forthcoming or cooperative and display a cavalier attitude providing incomplete responses

17. JP Pepperdine Group and GIW

*Restaurant brand*

(MI and AG*Breach and directions)
The membership information of 30,000 members collected for the restaurant operator’s internal use was publicly accessible through a random search in its website, which link was also published on the restaurant brochure, and by entering simulated membership numbers. Personal data includes names, gender, marital status, nationality, race, NRIC/Passport number, date of birth, mobile and home phone number, email addresses, residential addresses, and other membership details. The Commission found that JP Pepperdine and its IT outsourcer failed to provide adequate security to protect personal data including no security protection from threats, poor password policy, and itself facilitating unauthorized access by distributing the brochure with link to access its database. Penalties of $10,000 issued to the respondent.

<table>
<thead>
<tr>
<th>18. Propnex Realty Pte Ltd</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Real estate agency</strong></td>
</tr>
<tr>
<td>After receiving contact from a telemarketer, the complainant found her name and telephone number available on the Internet search result, along with other 1,765 individuals in the respondent’s link. It contained the respondent's Do-Not-Call files with full name, mobile number and landline, residential address, email address accessible by the public. The list was placed on the virtual online sharing system of the respondent, without any password protection or authentication, or internal policy prohibiting the sharing of sensitive documents on the system. Therefore, it was indexed by google and searchable on the Internet. PropNex was unaware until being informed of complaints by the Commission on 31 December 2015. Organization could have and should have been aware of these weaknesses and limitations when they made use of this security measure from, among others, Google support article, The Commission issued penalties of $10,000 and direction for the respondent to patch the vulnerabilities and fix the design flaw on its document sharing system.</td>
</tr>
<tr>
<td>• Took prompt action to remedy the breach when notified by the Commission</td>
</tr>
<tr>
<td>On 29 October 2015, after receiving the Commission’s notification, the Organisation introduced password protection feature and subsequently removed URL from Brochure.</td>
</tr>
<tr>
<td>• (AG*B) substantial amount of 30,000 members at risk increased by the dissemination of brochure, sensitive info, preventability and being able to mitigating impact by review and removal of webpage after the end of event.</td>
</tr>
<tr>
<td>4 days after noticing of breach, the respondent deleted the list from its system and informed Google to exclude the link from its search results and took steps to prevent similar incident occurring by sharing documents through a secured database required authentication.</td>
</tr>
</tbody>
</table>

(Mi*R Breach)

| • Admittance in the first instance of breach |
| • 96% is non-personal data (either phone number, residential address or email address without other PI) |
| • Breach caused by the respondent’s system flaw |
| • prompt remedial actions taken to rectify and prevent the recurrence of the data breach; |
| • being cooperative and forthcoming during the investigations |
| • have in place a data protection policy which |
### 19. Singapore Telecommunications and Tech Mahindra

*Telecommunication company and IT vendor*

The erroneous coding issue made by the IT vendor’s employee caused a disclosure of an individual’s sensitive personal data including his NRIC, billing address and Singtel account number to other 2.78 Million users of its feature, but actually viewed by 2,518 users using its onepass feature. On 29 February 2016, Singtel learned of the incident from its users’ report of their information accounts being replaced with the data of affected individual.

The Commission did not find Singtel breach of section 24 because it provides reasonable security arrangements by entering into contract, follow through the procedure, conduct the on-site visits and specific instructions to ensure the security practices of its vendor. $10,000 penalty was imposed on Tech Mahindra.

<table>
<thead>
<tr>
<th>Singtel</th>
<th>Shortly after receiving reports of the incident, SingTel shut down the application and disabled access to the profile webpages on the portals. SingTel also notified the affected customer of the incident.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mahindra</td>
<td>In assessing breach and remedial actions, mitigating and aggravating factors are set out below. (para. 26)</td>
</tr>
<tr>
<td></td>
<td>(AG) NRIC number is of a sensitive nature;</td>
</tr>
<tr>
<td></td>
<td>(AG) unauthorised modification of the personal data of 2.78 million users in addition to unauthorized disclosure of one individual information.</td>
</tr>
<tr>
<td></td>
<td>(AG) the breach could have been avoided if SOP was followed.</td>
</tr>
<tr>
<td></td>
<td>(MI) only 2,518 users had viewed</td>
</tr>
<tr>
<td></td>
<td>(MI) Tech Mahindra and Singtel had jointly notified the Commission of the data breach and was cooperative in the course of the investigation</td>
</tr>
<tr>
<td></td>
<td>(MI) Singtel and Tech Mahindra took prompt remedial and preventative actions.</td>
</tr>
</tbody>
</table>

### 20. National University of Singapore

A student of the respondent complained that the URL link circulated for the respondent’s orientation camp disclosed the personal data of about 143 student volunteers without receiving authorization. Unknown party changed the setting for the document to be visible to anyone outside the group who has the link. Personal data in the spreadsheet contained the full names, mobile numbers, student ID number, shirt sizes, dietary preferences, and dates of birth, dormitory room numbers, and email addresses of affected students. The Commission found that the safeguards were inadequate in the circumstances because “no

| (R* Breach) | a significant number of affected individuals (approximately 143 students); |
| (R* Breach) | (b) the potential adverse consequences from a misuse of the student matriculation number, i.e. identity theft, pranks or nuisances in the student’s name. |
| (Mi*R Breach) | being cooperative with the Commission and forthcoming |

| (Mi*R Breach) | being cooperative with the Commission and forthcoming |

---

182
formalized data protection training in place to train and equip its students with the mind-set, knowledge, skills and tools to protect personal data.” Organisation’s failure to provide adequate training for the student leaders, a type of security arrangement, before they handled personal data, this increased the risk of a data breach occurrence. A direction for mandatory training was issued.

### 21. Furnituremart.sg
**Furniture Retailer**
The reused invoice paper issued by the respondent to the new customers (complainant) had disclosed the printed personal data of its other customer on the back. Personal data involved the other customer’s surname, home address, e-mail address, and telephone number, which could possibly identify that individual. Despite the respondent’s policy restricting the reuse of invoice, no data protection training was conducted to its employees, showing lack of reasonable security arrangement of the respondent. The commission emphasized the organization’s management to “buy-in” good data practice and to establish the obligations for the standard of care to the staff level. (para. 24-25). It found inadequate security arrangements of respondents and issues directions to the respondent to review its policy, adopt effective procedure to data protection and conduct training for staff awareness in handling personal data.

### 22. Tiger Airways Singapore, SATS, APS
**Airlines, ground service provider and its subsidiary** assigned the duty involved boarding process.

Improper disposal of the partially printed passenger list involved unverified number of individuals by the APS employee, made the list accessible by anyone in the area of the trash bin near the gate, including passengers and airport staff. Personal data included passenger’s name, booking reference number, fare class, check-in number, booking date, seat number, destination and flight number, which could used for retrieving other information through the manage my bookings page, such as, full name, passport number, home address, phone number, email address and last four digits of the credit card used for payment, car rental and hotel booking until the last traveling date. The Commission did not find Tiger Air breach because adequate security

---

<table>
<thead>
<tr>
<th>(para. 29) “Mitigating factors”</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Mi*) disclosed to only one single individuals</td>
</tr>
<tr>
<td>(Mi*) not sensitive data</td>
</tr>
<tr>
<td>(Mi*) no actual loss</td>
</tr>
</tbody>
</table>

**Mitigating Factors**

*Breach and direction (para. 39)*

(Mi*B) the limited access and time of exposure of the list containing personal data of passengers, (Mi*B) no complaints of any actual unauthorized access from any passenger.
Arrangements had been made with its data intermediary to reasonably expected APS and SAT to comply with the PDPA. The Commission found that APS failed to ensure by having its own separate policy and conduct staff training contextualized and customized to each operational setting. Direction was given to the APS to review its disposal policy and operation.

### 23. DataPost

<table>
<thead>
<tr>
<th>Printing companies for banks</th>
<th>The Bank alerted the Commission to the incident, and informed the Commission that the recipient had received the additional SRS statement on or about 17 June 2016.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial statements of two customers of a bank were inadvertently disclosed to the other bank customer due to the respondent’s employee’s error during the printing operation. A customer who received additional banking statements of retirement plan of two others reported the bank to make complaint to the Commission. The Commission found DPL did not meet the reasonable standards expected of it, and could have been avoided if DPL had taken some simple additional precautions, for example, additional level checkers to ensure the accuracy. A financial penalty of $3,000 was imposed on DataPost with a direction to review its working procedures relating to printing operations, to improve its staff training of its staff, and review its personal data protection policy.</td>
<td></td>
</tr>
</tbody>
</table>

### 24. HAZEL FLORIST & GIFTS PTE LTD

<table>
<thead>
<tr>
<th>Gift shop</th>
<th>N/A notifying affected individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>The respondent’s employee inadvertently disclosed personal data of at least 24 individuals including one NRIC to the other customer by reusing the customer’s order forms to fill in the gift package. The gift receiver made complaint to the Commission. Personal data contained in order forms included names, delivery addresses, telephone numbers of the recipients and the reasons the gift. The Commission found that the respondent breached of section 24 for failure to ensure adequate security arrangements to protect the personal data, i.e., not ensuring that its employees went through data protection training, no proper supervision at work or policy to provide specific guidance. A warning was issued to the respondent.</td>
<td></td>
</tr>
</tbody>
</table>

Post-breach remedial action:
Reminder Post, Team Meeting on the reminder of PI, Limit access of the disposal box of Order form, revising order form by showing only address, data, time and item code no.; Determining direction; (para. 23):

- **(Mi*R)** limited disclosure to only 1 person, limited sensitivity except the NRIC of an individual being disclosed
- **(Mi*R)** remedial actions taken to prevent the disclosure in the future
- **(Mi*R)** being fully
| 25. **Eagle Eye and MCST 3696**  
(Condominium Security management service, Organization) | **Remedial Action**  
Following the data breach incident, the MCST 3696 and Eagle eye had removed the table at the Condominium gantry so that all visitor registrations would only be done at the guardhouse. This was to ensure that the logbook was kept in the guardhouse at all times (para. 9); NC  
(MI*R) However, in view that Eagle Eye and MCST 3696 have taken reasonably adequate steps to remedy the lapses during the course of the investigations, the Commission has decided not to impose any directions against them. Instead, it has decided to issue a Warning (para.30) |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The security operator failed to safeguard the guestbook keeping record of visitors of the condominium by leaving it unattended and unprotected from the prying eyes. The complainant took a picture of the book left open and untended, and reported the Commission. The book therefore contained the dates and times of entry and the NRIC numbers of the swimming coaches. The Commission found the MCST 3696 had the primary and shared responsibility with Eagle Eye but failed to ensure system in place for the safekeeping of the logbook at all times, and ensure its data intermediary reasonable practices by putting in place actual processes in protecting the logbook. Warning was issued to both respondents.</td>
<td></td>
</tr>
</tbody>
</table>
| 26. **Orchard Turn Developments Pte. Ltd. And Super-E Management**  
Property manager of a retail mall and its IT service provider | **OTD**  
On 27 and 29 December 2015, emails were sent to the affected subscribers informing them of the Phishing Emails that had been sent. (para.8)  
Engaged KPMG Services to investigate the incident and found the weak credentials leading to unauthorized access in addition to other 24 vulnerabilities to attacks.  
Removed all the personal data on the attacked server limited retention period to 14 days. (para. 40)  
Super-E subsequently discovered the intrusion of the server and the emails sent out to subscribers, then disabled the server at issue to prevent further dispatches of Phishing Emails |
| An intruder compromised the respondent’s server to access personal data of 24,913 individual subscribers, including email address, birthdate, and membership registration date, and sent the phishing emails to them on 26 December 2015. The email included links directing to advertising page, which requested subscribers of their personal data. The perpetrator gained unauthorized access to the respondent’s EDM Application using valid admin account credentials to access the subscriber list. The organization’s design of keeping a duplicate personal data on servers for a period longer than necessary increased risks and not prudent. In addition the commission found the absence of proper policy and practices prohibiting the sharing of passwords among admins and requiring of periodical password changes failed to put in place reasonable security arrangement. The Commission issued a financial penalty of $15,000 and the direction to fix all vulnerabilities detectable and conducting security test and implement |  |
password policy and staff training.

The commission cited numbers of foreign decisions on the importance of good password policy: Ashley Madison, Twitter, Reed Elsevier re: sharing passwords among users allowing attacker to obtain and conduct database search).

| R*Breach and direction | (AG*R) a large number of individuals of 24,913 subscribers out of a potential 47,635 subscribers, further risks from phishing email, not making reasonable efforts to put in place proper password management policies, and to ensure the security of the personal data set by reasonably anticipating, identifying and rectifying the technical security vulnerabilities at an earlier stage (regular patching and conduct assessment of vulnerabilities) |
| Mi*R | (d) being cooperative and forthcoming in providing timely responses to the Commission |
| (e) the Organisation took prompt remedial action after being alerted to the data breach incident, as well as other corrective measures to improve its IT security. |

| 27. Former Financial Consultant | Respondent confirmed that he had disposed of the folders at the location. |
| The individual complainant found the insurance policy-related documents including 13 certificates of life assurance at a trash bin of a residential estate. Personal data including name of policyholder, NRIC number, benefits, assured amount, insured period, premium, address and policy number. The Commission found an independent contractor, a former employee of an insurance company failed to provide reasonable security measures in disposal of the folders containing personal data, which opens up to potential data breaches from a recovery of documents through ‘dumpster diving’. The documents were simply put inside the trash bin in a tied plastic bag without shredding, and thus being retrievable by anyone who searches for recyclable or paper waste. (para.19) The respondent could have used the locked console boxes provided by its previous employer according to its disposal standard, but failed to do so. A penalty of $1,000 was issued. |
| AG*R | Sensitive data |
| Mi*R | Not disposing in the high traffic area |
The insurance company had reasonable policies in place, which required financial advisors to return client data to dispose properly and securely, and communicated these policies through appropriate channels to the employees and further instructing by letter upon the respondent’s resignation.

The Commission referred to the PDPC’s guide to disposal.

28. Aviva Ltd
(Multinational insurance company)

The respondent had mistakenly mailed to one of its policyholders insurance documents containing sensitive personal data of the other policyholder. The leaked personal data included full name, ID type, FIN, nationality, date of birth, gender, marital status, relationship of up to three individuals. The family member of the recipient of wrong documents alerted Aviva on 1 November 2016 and made complaint to the Commission on 8 November 2016. Organization investigated into the incident and its employee's error. (para. 4)

The Commission found that the respondent did not provide reasonable security arrangement to prevent unauthorized disclosure, among others, by not having oversight of the enveloping process nor any supervision the processing staff and relying on only person to check the contents before mailing out to the policyholders. It found these practices were amounted to extremely weak internal controls and significantly failed the standard of protection given such sensitive personal data involved that should be “processed and sent with particular care” and a best practice of additional checks, according to the Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data.

NC, NA, CR
(Unknown time period,) Organisation also sent an apology letter to recipient and retrieved the wrongly delivered documents. Organisation sent an apology letter along with shopping vouchers worth S$100. (para. 43)

Following its internal investigation, the Organisation revised its procedures for the enveloping process to include random checks. After the data breach incident, the Organisation counselled the staff in question, carried out an audit on the staff’s enveloping output for one week, and revised its SOPs to add an additional layer of checks by the Team Leader of the enveloping process.

AG-MI* Breach (para. 45)
(AG) sensitive data;
(AG) the Organisation is in the business of handling large volumes of personal data, the disclosure of which may cause exceptional damage, injury or hardship to the affected individuals;
(MI) being cooperative fully with investigations and was forthcoming in admitting its mistake;
(MI) the Organisation had notified the affected victim, i.e. the Second Policyholder, of the data breach incident, and offered an apology and shopping vouchers, and had
also made arrangements to retrieve the wrongly delivered documents from the First Policyholder; (MI) the unauthorised disclosure of Personal Data was limited to possibly three individuals; and (MI) no evidence of actual loss or damage

29. BHG (Singapore) Pte. Ltd.
Department store with outlets

An unauthorized access of a customer’s account information disclosed personal data including the name, gender, date of birth, race, marital status, range of income group and residential address of the affected customer. The victim keyed in his details on the registration form left with the complainant’s email address and telephone number, and submitted to the staff. As a result, the complainant after resetting her password found that she logged into the account of another customer, alerted the respondent and the Commission. The Commission found that the respondent did not breach because the unauthorized access was caused by "a confluence of events and circumstances" that would have been difficult to foresee" (para. 22). The respondent had in place reasonable security arrangements including a mandatory training program for employees, 10 months on the job training for staffs on the registration process and how to refresh the form when having technical issues before the incident occurred. No further direction was issued because the remedial actions satisfactorily addresses the residual harm.  

YZK noted that the protection is not absolute in nature; in that the obligation is not automatically breached upon the occurrence of a data leak. This case provides a classic example of the application of “this principle. (para. 1)

“Remedial Action By Organization”  
Once learnt about breach from the complainant, the organization conducted the internal investigation and the following remedial actions: (para. 29)  
MI*(a) Responding to the affected individual by creating new account and correcting data;  
MI*(b) Remedial action concerning staff training by scheduling refresher data protection training;  
MI* (c) Remedial action concerning technical safeguards correcting the wifi issue by purchase and updated app;  
(d) Further remedial action on operational processes (to review the membership registration process and stronger authentication checks for password reset.

30. Social Metric Pte Ltd
Social Media Marketing Agency

The respondent failed to remove those webpages created for its clients after the marketing campaigns were over. The webpages contained the personal data of over 558 individuals who were its clients' customers. The personal data in these nine Webpages included names; email addresses, contact numbers, employers; occupations, date and time of registration, including recent place visiting, activity

R*Breach (para. 37)  
AG*R (a) children data involved  
AG*R (b) Social Metric did not take prompt remedial actions after being informed of the data breach by the Commissioner;  
AG*R (c) Social Metric had, on more than on occasion, informed the Commissioner that the
and purpose of visits. Two out of the nine Webpages also contained the personal data i.e. name and age of about 155 children. The organization collected these information via private message on FB directly by individuals.

The Commissioner found that Social Metric failed to comply with its Protection Obligation by not limit access and left the personal data exposed online for public access without any password protection.

Social Metric’s prolonged failure to put in place the necessary security measures was inexplicable and a flagrant breach of its Protection Obligation under the PDPA. Forgetfulness on its part are not valid excuses.

<table>
<thead>
<tr>
<th>Social Metric was first informed by the complainant of the unintended disclosure of personal data on the nine Webpages on 27 April 2016, following by the PDPC notice in May 2016. Six out of the nine Webpages were still available online until 11 July 2016 that all had been taken down. The personal data was left for a period of at least 2 months since being aware.</th>
</tr>
</thead>
</table>

**31 ComGateway Pte. Ltd**

online portal service for shopping and shipping

The respondent provided an electronic platform to process, track and manage shipping and transaction orders from its customers. About 108,085 customers had made shipments via the Organisation

The URL of the shipping order was made possible for anyone to gain access to a customer’s information by systematically changing the last character of the URL until it found valid link, and therefore was susceptible to manipulation with the available decoding tools. The leaked personal data included individual customer’s contact, name, and email address. The penalty of $10,000 was issued to ComGateway for its failure to implementing a logging function that creates a log entry whenever a session variable mismatch occurred, which would provide the Organisation with diagnostic data.

The Commissioner claimed its position similar to personal data in question had been deleted when this was not the case;

AG*R(d) generally uncooperative throughout the investigation process. Social Metric demonstrated its uncooperative attitude by making unsubstantiated claims of an external hack, and that it had engaged freelance developers, causing multiple delays in the investigation process.

Social Metric’s prolonged failure to put in place the necessary security measures was inexplicable and a flagrant breach of its Protection Obligation under the PDPA. Forgetfulness on its part are not valid excuses.

Organisation after learned of breach has since taken the following remediation steps:

(a) Removing all personal data from the Shipping Webpage, noting that the Commissioner does not advocate the removal of personal data purely as a risk avoidance measure if the removal detracts from the usability of the Organisation’s Website. Such steps would in the Commissioner’s view be excessive and unnecessary, especially if there are other reasonable technical or operational means to achieve the objective of protecting personal data. (para. 24)

**R breach and direction**

• substantial volume of shipping transactions for individual customers
authorities in other jurisdictions.

- cooperated fully
- took prompt action to remedy the breach when notified by the Commissioner; and
- conduct regular penetration tests, vulnerability tests and code reviews

<table>
<thead>
<tr>
<th>32 Credit Counselling Singapore</th>
<th><strong>Clarify injury and actual harm of financial data and general losing of public trust of larger credit system.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered charity for individual debt counseling and facilitation</td>
<td>In assessing the breach and determining the directions; para. 36 (a) information about an individual's adverse financial condition and/or state of indebtedness was sensitive personal data, and the disclosure of which could cause actual or potential harm, injury or hardship to the individual, including serious reputational damage and embarrassment; (b) given the business nature handling large volumes of sensitive personal data (does not mention about non-profit nature); and (c) the data breach incident may cause members of the public to lose trust in such credit counseling organizations to safeguard their personal data, which may frustrate the larger national credit management efforts.</td>
</tr>
</tbody>
</table>

mitigating factors: (para. 37): (a) cooperated fully with the Commissioner’s investigations and **had readily admitted its mistake without delay**; (b) promptly notified all the affected recipients of the data breach incident and offered them an apology alongside a
(request to delete the Follow-up Email (c) advised the admin staff who made the mistake, and steps taken to prevent future data breaches i.e. taking a refresher course on compliance with the PDPA, and using the “mail-merge” software within two months; no other data breach incidents reported apart from this one.

TKH*: Disclosure of an individual's indebtedness to other third parties could lead to harm to the individual because it could result in social stigma, discrimination or tarnish his reputation. These are real possibilities that can affect a person's life. Hence, the confidentiality of the individual's financial information should not be treated lightly. (para. 19)

agreeing with Canada, UK HK
<table>
<thead>
<tr>
<th>Name / Other Reg</th>
<th>Industry</th>
<th>In/Out</th>
<th>Indiv/Bus</th>
<th>Type of Data Breach Size</th>
<th>Notification/Remedy</th>
<th>Decision &amp; Order Remarks</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Rennert, Sandra H D</td>
<td>Phar Retail Co</td>
<td>Int misuse</td>
<td>Indiv</td>
<td>H/F/G</td>
<td>11000 -</td>
<td>-</td>
<td>PrivReq</td>
</tr>
<tr>
<td>2 Elly &amp; Co Inc</td>
<td>Phar Retail Co</td>
<td>Inadq discs</td>
<td>Indiv</td>
<td>G</td>
<td>666</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>3 Microsoft Corp</td>
<td>COPPA UD</td>
<td>Tech Retail Co</td>
<td>Inadq sec/ Ext</td>
<td>C</td>
<td>NonExp</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>4 Guess?</td>
<td>Ultra Retail Eco</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>C</td>
<td>&gt;1</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>5 MTS, Inc., et al</td>
<td>Ultra Retail Eco</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>PurH</td>
<td>5,225</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>6 Petco Animal Sg</td>
<td>Retail Ecom</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>C</td>
<td>&gt;1</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>7 NATIONALWIDE M GLBA UD</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F</td>
<td>SSN ACC</td>
<td>NonExp</td>
<td>-</td>
</tr>
<tr>
<td>8 Sunbelt Lending</td>
<td>GLBA UD</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F</td>
<td>SSN ACC</td>
<td>NonExp</td>
</tr>
<tr>
<td>10 B&amp;J's Wholesale CU</td>
<td>Warehouse Retail Eco</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F</td>
<td>&gt;1</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>11 Superior Mortgage GLBA UD</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F CrdHist</td>
<td>Unknown</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>12 DSW Inc.</td>
<td>Ultra Retail Eco</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F ACCN</td>
<td>140000 card</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>13 ChoicPoint Inc.</td>
<td>FCRA UD Cal S</td>
<td>Data Broker for B</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>F CrdHist</td>
<td>163,000 Y</td>
<td>-</td>
</tr>
<tr>
<td>14 CardSystems So U</td>
<td>B2C Products</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>F Crd</td>
<td>1000000 card</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>15 Nations Title Age GLBA UD</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Bus-Indiv</td>
<td>F CrdHist</td>
<td>Unknown</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>17 American United FCRA</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F CrdHist</td>
<td>36 indiv</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>18 Life is good</td>
<td>Apparel Retail Eco</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>&gt;1000 cards</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>19 Goal Financial</td>
<td>GLBA D</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F CrdHist</td>
<td>7000 fees+34000 -</td>
<td>-</td>
</tr>
<tr>
<td>20 ValueClick</td>
<td>D CAN-SPAM Ac</td>
<td>Promo Ecom</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>unknown</td>
<td>-</td>
</tr>
<tr>
<td>21 TJX Companies U</td>
<td>Apparel Retail Eco</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>1000000 card</td>
<td>4 Y</td>
<td>Y</td>
</tr>
<tr>
<td>22 Reed Elsevier Le</td>
<td>Data Broker for B</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>SSN DRLVC</td>
<td>100000 Y</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>23 Premier Capital L GLBA UD</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>F CrdHist</td>
<td>&gt;400 report</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>24 Gregory Navone FCRA U</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>F CrdHist</td>
<td>&gt;230 report</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>25 Genica Corp</td>
<td>Elc Retail Eco</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>&gt;100</td>
<td>Y</td>
<td>SeReq</td>
</tr>
<tr>
<td>26 Rental FCRA</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>F CrdHist</td>
<td>&gt;318 report</td>
<td>FCRA</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>27 James B. Nutter GLBA</td>
<td>Financial Con Ph</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F CrdHist</td>
<td>Millions spam mail</td>
<td>STGR PrivRule</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>28 Lifedock</td>
<td>Security Con Ph</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>Disgorgement</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>29 Dave &amp; Buster's U</td>
<td>Entertainment Retail</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F CrdHist</td>
<td>130000 Y</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>30 Twitter</td>
<td>Social Networking</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>IP, Contact, 1st at least 8+1 PA reset</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>31 Rite Aid Corporate</td>
<td>Pharmacy Retail Co</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>H N/A</td>
<td>SeReq</td>
<td>MspRes Secur</td>
<td></td>
</tr>
<tr>
<td>32 Settlement One GLBA FCRA U</td>
<td>Credit Report Sel</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>F CrdHist</td>
<td>784 reports N N</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>33 Aracnet Inc. GLBA FCRA U</td>
<td>Credit Report Sel</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>F CrdHist</td>
<td>694 reports N N</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>34 Fajilan and assoc GLBA FCRA U</td>
<td>Credit Report Sel</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>F CrdHist</td>
<td>323 reports N N</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>35 Certigan Corp U</td>
<td>Payroll process</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>SSN</td>
<td>27,673</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>36 Lookout Service U</td>
<td>Immigration data</td>
<td>Inadq sec</td>
<td>Bus-Indiv</td>
<td>SSN</td>
<td>37000 Y</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>37 UPMrise U</td>
<td>Software too</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>SSN CrdF</td>
<td>At least 150000 comp</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>38 RockYou COPPA UD</td>
<td>Online site service</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>Childr email passw</td>
<td>179000</td>
<td>SeReq</td>
<td>$250,000 civil pen</td>
</tr>
<tr>
<td>39 Franklin's Budget GLBA UD</td>
<td>Online automobile</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>SSN DRLVC</td>
<td>95,000</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>40 EPN</td>
<td>collecting debts</td>
<td>Inadq sec</td>
<td>Bus-Indiv</td>
<td>SSN debt H</td>
<td>3800</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>41 FTCv Wynyard Worldwide Corp</td>
<td>Hotel Franchise</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>10,000</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>42 Compete D</td>
<td>market research</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>SSN</td>
<td>4000000</td>
<td>SeReq</td>
</tr>
<tr>
<td>43 PLS Financial Sc GLBA FCRA U</td>
<td>Consumer Loan</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>SSN</td>
<td>29</td>
<td>SeReq</td>
</tr>
<tr>
<td>44 CBR SYSTEMS D</td>
<td>Cord blood Bank</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>DRLVC</td>
<td>298,000</td>
<td>-</td>
</tr>
<tr>
<td>45 HTC America U</td>
<td>Mobile Device M</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>Location</td>
<td>Bef</td>
<td>18,300,000</td>
<td>-</td>
</tr>
<tr>
<td>46 ControlScan Inc</td>
<td>web Certification</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>SSN</td>
<td>SeReq</td>
<td>$75000, notify</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>47 CVS Caremark U</td>
<td>Prescription</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>F Crd</td>
<td>DRF at least 1</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>48 LabMD U</td>
<td>Medical Lab serv</td>
<td>Inadq sec</td>
<td>Bus-Indiv</td>
<td>H</td>
<td>9,300</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>49 Trendnet Inc U</td>
<td>IP Camera retail</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>IP, location, I</td>
<td>700 Y Y</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>50 Accretive Health, U</td>
<td>hospital operator</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>H SSN</td>
<td>23,000</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>51 Genelink U</td>
<td>health products</td>
<td>Inadq sec</td>
<td>Bus-Indiv</td>
<td>Acct Crd E</td>
<td>30,000</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>52 Secu™ International</td>
<td>health products w</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>Acct Crd E</td>
<td>30,000</td>
<td>-</td>
<td>SeReq</td>
</tr>
<tr>
<td>53 GMR Transcript Inc</td>
<td>Audio transcriptic</td>
<td>Inadq sec</td>
<td>Bus</td>
<td>SSN DRLVC NA</td>
<td>Y</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>54 Fandango U</td>
<td>Movie ticket retail</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>SSN CrdF</td>
<td>18.5 M download</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>55 Credit Direct D</td>
<td>Credit Monitoring</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>SSN CrdHist N/A</td>
<td>-</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>56 Snapchat U</td>
<td>Social Networking</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>Photo Msg Location</td>
<td>-</td>
<td>SeReq</td>
<td>MspRes Secur</td>
</tr>
<tr>
<td>57 FTCv Cornerstone U</td>
<td>Selling debt portfo</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>Name, ACC</td>
<td>40,600</td>
<td>-</td>
<td>SeReq, prelim injunction t</td>
</tr>
<tr>
<td>58 FTCv Bayview Si U</td>
<td>Selling debt portfo</td>
<td>Inadq sec</td>
<td>Indiv</td>
<td>Name, ACC</td>
<td>28,000</td>
<td>-</td>
<td>SeReq, prelim injunction t</td>
</tr>
<tr>
<td>59 LabMDvFTC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Order Name**
- None

**Other Reg**
- None

**Industry**
- None

**In/Out**
- None

**Indiv/Bus**
- None

**Type of Data Breach Size**
- None

**Notification/Remedy**
- None

**Decision & Order Remarks**
- None

**Cause**
- None
<table>
<thead>
<tr>
<th>Order</th>
<th>Name</th>
<th>Info</th>
<th>Notifying</th>
<th>General remedies</th>
<th>Coope- rate</th>
<th>size</th>
<th>con-face</th>
<th>Ins/Out</th>
<th>Sensitivity</th>
<th>Penalties</th>
<th>Actual Breach Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>K-Box Entertainment</td>
<td>1</td>
<td>1</td>
<td>0* L</td>
<td>1 Out</td>
<td>Gov ID</td>
<td>50,000</td>
<td>317000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Challenger Consumer prod</td>
<td>1</td>
<td>1*</td>
<td>1* L</td>
<td>1 Ins</td>
<td>Membership warning</td>
<td>165306</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Fei Fah Consumer prod</td>
<td>1</td>
<td>0*</td>
<td>0* L</td>
<td>1 Out</td>
<td>Membership</td>
<td>5,000</td>
<td>900</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Metro Entertainment</td>
<td>1*</td>
<td>L</td>
<td>1 Out</td>
<td>Gov ID</td>
<td>warning</td>
<td>445</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Singapore Comp Professional</td>
<td>1</td>
<td>1*</td>
<td>L</td>
<td>1 Ins</td>
<td>Gov ID</td>
<td>warning</td>
<td>214</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Full House Marketing</td>
<td>1*</td>
<td>1</td>
<td>L</td>
<td>1 Ins</td>
<td>Gov ID</td>
<td>warning</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Institute of Engin Professional</td>
<td>1</td>
<td>1*</td>
<td>1* L</td>
<td>1 Out</td>
<td>Account ID Pass</td>
<td>10,000</td>
<td>60000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Central Clearing Consumer prod</td>
<td>1*</td>
<td>1*</td>
<td>L</td>
<td>0 Ins</td>
<td>Financial Data</td>
<td>0</td>
<td>195</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Spear Security Security Service</td>
<td>1</td>
<td>1*</td>
<td>M</td>
<td>1B Out</td>
<td>General warning</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Fukwee Catering Entertainment</td>
<td>0*</td>
<td>0*</td>
<td>M</td>
<td>1 Ins</td>
<td>General</td>
<td>3000</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Aviva Consumer prod</td>
<td>1</td>
<td>1</td>
<td>L</td>
<td>1 Ins</td>
<td>Financial Data</td>
<td>0</td>
<td>7794</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>ABR holding Entertainment</td>
<td>1*</td>
<td>1</td>
<td>L</td>
<td>1 Ins</td>
<td>Gov ID* Children warning</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>GMM Consumer products</td>
<td>1*</td>
<td>1*</td>
<td>S</td>
<td>1 Ins</td>
<td>General</td>
<td>3000</td>
<td>190</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Lifelock</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Smiling Orchid Entertainment</td>
<td>1*</td>
<td>0*</td>
<td>S</td>
<td>1 Ins</td>
<td>General</td>
<td>3000</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Cellar Door Entertainment</td>
<td>0*</td>
<td>0*</td>
<td>S</td>
<td>1 Out</td>
<td>General</td>
<td>5000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>JP Pepperdine Entertainment</td>
<td>1</td>
<td>L</td>
<td>1 Ins</td>
<td>Gov ID</td>
<td>10000</td>
<td>30000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Propnex Realty Marketing</td>
<td>1*</td>
<td>1*</td>
<td>L</td>
<td>0 Ins</td>
<td>General</td>
<td>10000</td>
<td>1765</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Telecom Consumer Prod</td>
<td>1</td>
<td>1*</td>
<td>L</td>
<td>1 Ins</td>
<td>NRIC</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>NUS Professional</td>
<td>1*</td>
<td>L</td>
<td>1 Ins</td>
<td>Student ID</td>
<td>Direction</td>
<td>143</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Furniture Mart Consumer Product</td>
<td>1*</td>
<td>1</td>
<td>M</td>
<td>1 Ins</td>
<td>General</td>
<td>Direction</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Tiger Air Security Service</td>
<td></td>
<td>L</td>
<td>1 Ins</td>
<td>Gov ID</td>
<td>0</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Data Post Printing Service</td>
<td>1*</td>
<td>S</td>
<td>1B Ins</td>
<td>NRIC warning</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Hazel Consumer Product</td>
<td>1*</td>
<td>1*</td>
<td>S</td>
<td>1 Ins</td>
<td>Gov ID</td>
<td>warning</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Eagle Eye and M Security Service</td>
<td>1*</td>
<td>1*</td>
<td>1B Ins</td>
<td>NRIC warning</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Orchard Turn De Entertainment</td>
<td>1</td>
<td>1*</td>
<td>L</td>
<td>1 Out</td>
<td>General</td>
<td>15000</td>
<td>24913</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Former Financial Consumer Product</td>
<td>1*</td>
<td>1</td>
<td>S</td>
<td>0 Ins</td>
<td>Financial Data</td>
<td>1000</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Aviva Consumer Prod</td>
<td>1*</td>
<td>1*</td>
<td>L</td>
<td>1 Ins</td>
<td>Financial Data</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>BHG Entertainment</td>
<td>1</td>
<td>L</td>
<td>1 Ins</td>
<td>general income r</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Social metric Marketing</td>
<td>0*</td>
<td>0*</td>
<td>M</td>
<td>1B Ins</td>
<td>Children</td>
<td>18,000</td>
<td>558</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Comgateway Consumer Product</td>
<td>0*</td>
<td>1</td>
<td>L</td>
<td>1 Ins</td>
<td>general</td>
<td>10,000</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Credit Counsellor Consumer Prod</td>
<td>1*</td>
<td>1</td>
<td>L</td>
<td>1 Ins</td>
<td>Financial Data</td>
<td>10000</td>
<td>96</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1= positive 0 negative
1*=positive and mitigating factor
0*=negative and aggravating factor
N/A = not mentioned
Note: * = recognized by the agency
Note: 1B= company with business clients but also facing consumer

193
Appendix B

Excerpts from the CLTC Project Memo
The Role of DPOs in Enhancing Trust Relationship: Data Breach Notification in Singapore
**Note:**
The interview was conducted in July 2017 as part of the CLTC Project, *The Role of DPOs in Enhancing Trust Relationship: Data Breach Notification in Singapore*. The interviewees are 17 data privacy professionals of the organizations operating in Singapore.

<table>
<thead>
<tr>
<th>No.</th>
<th>Job Title</th>
<th>Organization Description</th>
<th>Other Position(s) in the Firm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Protection Officer</td>
<td>Leading digital financial products for consumer and business</td>
<td>Compliance Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global (U.S. base)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Data Protection Officer</td>
<td>Leading financial products for business</td>
<td>Deputy CEO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global (Asian base)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Regional privacy counsellor lead</td>
<td>Leading financial products for business</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global (U.S. base)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Privacy Consultant</td>
<td>Leading e-commerce platform</td>
<td>Legal</td>
</tr>
<tr>
<td></td>
<td>Legal</td>
<td>Global (Asian base)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Data Protection Officer</td>
<td>Leading brand consumer product</td>
<td>Information Security Regional Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global (European base)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Data Protection Officer</td>
<td>Leading Financial product for business</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global (U.S. base)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Data Protection Officer</td>
<td>Financial services for business and consumer</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cross-bordered (Asian base)</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Regional Data Privacy Officer</td>
<td>Leading telecommunication products</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global (European base)</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Chief of Legal and Compliance on</td>
<td>Leading technology consumer products</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity and Privacy</td>
<td>Global (Asian base)</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Data Protection Officer Lead</td>
<td>Financial Consumer Products</td>
<td>Auditor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regional (Asian Base)</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Data Protection Officer</td>
<td>Financial Consumer Products</td>
<td>Chief Information Security Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local (Asian Base)</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Data Protection Officer</td>
<td>Financial Consumer Products</td>
<td>VP Information</td>
</tr>
</tbody>
</table>
1. DPO Tiptoeing in Consumers’ Shoes: Discussion on Consumer Experience

When asked what urges them not to notify consumers of a breach, interviewees used these words to describe “consumer experience” regarding breach notifications: “information fatigue”, “being desensitized”, “unnecessary panic”, “misunderstandings” and “big mistakes”.

“unnecessary panic” : the DPO, operational and compliance MNC , “If it comes to not notifying, we take that decision and scrutinize a little more. But if it comes to notifying, in general, our concern is that we cause panic that is unnecessary. That’s the main contribution we have.”

This DPO further gave an example of two companies, company A that took a very opened approach to notify consumers even when small things happen, and company B that chose to notify only when there is a very significant, serious breach (in contrast to a small to moderate one or significant but not serious one.)

According to this DPO, “So, then, the reality is we’ll think that Company A is so transparent and it’s so good, but the public doesn’t know that they are being so transparent. The public may think that it just seems like they are careless , don’t have good policy or a good control whereas Company B that does not notify frequently will seem to have a very solid control framework. That’s why smart and intelligence may not happen, and they [Company B] may rationalize that the reason they report only the serious ones is because the confidentiality is strong and few situations that happen are very serious as there so few and fine in between. Simpler never happen there because of their strong control framework. The consumer does not know the difference. He thinks that Company A is careless. The reality is that to some extent all decision making that you have taken is a lot more. I mean we’d like to think things as privacy, right? But actually, it’s a lot more about customer experience as well. If you notify them regularly about small incidents that happen, it’s very likely that they will be not very happy with you because they think their data is less secure, and therefore their money is less secure as a result.
They may also think that, as a [institution], any time that they have interaction with you. It'll mean at the back of their minds they will that that the company is frequently [making] mistakes by losing data and very careless overall. And whenever they look at us during a transaction or interaction, they will use that lens even if they talk to our people in an unrelated matter. They will think of us as a careless institution, which is something you definitely don’t want.

This DPO clarified the differences between the notion of “consumer panic” and “information fatigue”: It’s not exactly the same. I guess there are two things. One is that, so let’s say tomorrow in Singapore we have mandatory breach notification regime. If they have very draconian law, which means any small thing you need to notify, then the first few times you get the panic. They will be like OMG what happened…So initially, it must create the panic, but overtime the problem is that if people will become desensitized to it, it will be basically like, when I won’t be here. It’s okay. They don’t happen every month. Because the PDP applies to all organizations. As a consumer, I could one day get a notification from the food courts that I went to and signed up for their membership, and the second day I will get a message from the bank. To me, both will look the same of data breaches. So as a customer, as an individual, I will not be able to distinguish which is the sensitivity, and the criticality of them. Over time I will get so many of these that I will eventually become information overloaded or something like this. So, there will be definitely a concern. When the PDPC asks the industry for advice, our feedback will always be that it’s okay if you want to make it mandatory, but there should still be a qualitative review at the hand of the institution. So, if the institution is able to justify right why they didn’t notify the individual in the situation with a good rationale, you should accept. Do not be that just because of this I have to be obligated.

Another interviewee, DPO and legals MNC, explained how “unnecessary panic” challenges the approach taken by the organization regarding consumer notification: “Unnecessary panic. Maybe the situation is not as bad as it seems. It’s under control but if we don’t handle it properly, then the PR will be a mess, right? And another thing is if you are not sure about the situation. Just setting aside the attracts that you would receive whether to pick public notices or to contact them [consumers] individually. I think if you handle the breach notification badly, it can be worse. PR -- if we don’t handle it well, it will take a negative turn. It’s a PR thing, PR is not just the media, but the way people take it or react to it. Now, it’s not just the media that do PR, but consumers themselves.”

Another interviewee, DPO and CISO, mentioned the concerns of “Information fatigue and a possible false alarm calls for fast investigation to the cause before notification is made.” This interviewee further mentioned that “It [notifying breach] may cause some consumers to fatigue. Senior people to get alarmed. Because in the first place, they do a physical transaction, not an online transaction. So, they may not have an interest in whether it [their secure data] is lost or not. They gonna take you along the way exactly when and why it is lost and how you are going to recover, protect, or how you’re going to cover me with something. To prevent that, you have to work very fast to investigate, and make sure that it’s all irretrievable data that is lost and
that it is irrelevant. That’s the first thing about personal data. Apart from the PDPA, even sensitive data to the company, you definitely need to inform the CEO because you don’t want a competitor to pick it up.

The DPOs also mentioned the difference between communicating to business and individual customers.

An interviewee, a full-time, chief regional privacy of MNC, referred to the differing reactions of businesses and individual consumers when informed of a breach: Absolutely, I agree, and think it’s different between telling a business entity and telling an individual, because individuals don’t know how to react. It’s all about their personal interest. There will be more rational thinking involved should we do something about this, Would it affect the business? With Individuals, we are the culture of making complaint. They may send it viral, call the newspaper or post on Facebook, then it gets shared many times. Sounds like I’m a very big corporation. I didn’t talk on behalf of a big organization, but also as an individual. Do people really have any need to know? Is it gonna affect them? How are they gonna react to it and how can they make decisions and act smart when given that info about them? All these things. “Honestly, [notifying breach] it’s really simple mistakes” if there are not major stuffs and It’s definitely zero impacts for individuals.”

2. An Interview Excerpt on “Calming an Unhappy Consumer in the Culture of Compliant”

Calming the unhappy customer is a step organizations take to prevent the escalation of individuals’ claims and the level of subsequent public exposure. Organizations prefer to close the case with the unhappy consumer before the issues reaches the public and the authorities.

According to the interviewee, DPO and legal of MNC , “PR is not just the media, but the way people take it or react to it. Now, it’s not just the media that do PR, but consumers themselves.”

An interviewee, Operational DPO and compliance of the MNC , explained “the culture of complaint” that pervades in Singapore in relation to negative customer experience and misunderstandings.

“Many times, there is misunderstanding. If I’m not happy, as a consumer, there is the consumer protection agency, but more like a government agency, if they [consumers] see anything that could be interpreted as a data breach, they will go to the PDPC instead. This is the culture. It’s a first world problem. Even if it’s trivial, they will go at great lengths. They escalate to the PDPC and MAS or a member of parliament. That’s a culture thing. First one and a half year since the the PDP, we put effort for customer service to handle the cases. It comes down significantly now. And the public is more educated now.”

This interviewee described the process of resolving consumer complaints:“We are able to close the case with customers [before getting elevated]. Some people just want to get the voucher from the [institution], They know that sometimes they can get small amounts like SGD 100-200. Some people know this or maybe they experienced it before in another company. They went to the airline they got delayed and got the voucher. In their minds, I think they think the big
company have a service left I will get money from them. So, even though it's something small, they will keep coming to us, keep complaining. So, very often times we tell them, 'We told you the cases. We apologize. We can't turn back time and send the letter to the right address. Something that is no risk of harm to individuals. So, what do you want? Often times, you find that, do they want the [institution] to close down because of one individual’s resentment? So, what do you want as a consumer? Many times they just want to complain about what happened to them, so then it comes to the point that they just want the voucher or something. So, in the initial setup of the complaint, we have some cases that it is a general issue because we still see the frequency of this process where we would give something [to the consumer]. But over time, we stopped doing it like this. Because we don’t want to encourage something like that.

This interviewee also added that difficult consumers will be handled by the second line of response: that are the legal and compliance departments.

3. DPO Excerpt on “Breach Notification as Constraining the Fire from Getting Out-of-Control”

Interviewees explained that they felt compelled to notify consumers of a breach when the impact of the breach is high, i.e. involving sensitive data or a large volume of data leakage. In other instances, the interviewees indicated that they consider the seriousness of the threat to consumers by third party acquisition of leaked data, and the level of exposure to the public of such an occurrence that could suggest weak internal control. There are two phrases often mentioned by the interviewees in their answer on why they make certain decisions on breach notification: First is “Nothing to Hide”; Second is “Better Tell It Now or Never”. Both associates with the fear of consumer receiving the news from third party instead of direct notification from the organization itself. Mentioned along this theme are trust, transparency, honesty and control.

A Nothing to Hide Approach: The interviewees believe that hiding something from consumers that will ultimately be revealed definitely affects baseline trust and future interactions. According to the interviewee, DPO and CISO, “I lost something and I’d better let you know. It’s better than if they find out in the newspaper and wonder what you’re doing. Do you know who got my data leaked? it’s best that we notify them. If they start receiving strange calls, strange mail not sent from an employee, someone from lease, and later they come back to you and find out then, this is not good.”

This interviewee also believes that authorities will look favorably upon organizations that are proactive about consumer protection. He explained, “The law tries not to force you to do things that are not necessary. Like when the PDPA says “reasonable,” [we interpret it as] and whatever you do that is not detrimental to the customer or something that you take into positive consideration. If there’s any investigation or something happens, I guess that I believe that even the authorities would take into consideration that you’re proactive in handling such things and not trying to hide and hoping that nobody knows. If you’re positive about the loss, and if you
have sufficient facts, you should inform consumers as soon as possible. It’s not very nice for consumers or anybody to find out from third parties. [If this happens,] they may immediately think you know what’s happening but don’t tell them [customers] and wonder how they can trust you with their money. Definitely, about trust.”

Another interviewee, a DPO and CISO of MNC, shared the same view on transparency and trust in relation to notifying directly to consumer:

“So, of course, if we have means to contact them [affected consumers], why not? Yes, they could go public after learning this, so it has to be a management decision. Because you have to think forward if you have to inform them, what’s gonna happen. You have to be ready for the press. Go public. If you want to gain customer trust, you have to be transparent. To me, it’s individual transparency. You don’t hide. …It depends if it’s just the name that is breached—to me it is just personal data. To me, I feel that it’s not a big deal. Unless this person got the name credit card number, and more info that can do alot of things. Then we need to straightaway inform the customers. Definitely. Rather than the consumer finding out the news from the media, that is not so good. I agree that if there is not any law, most people will just keep quiet. Until somebody posts the [leaked customer] information on the internet. …Case like that could happen everywhere, so it’s gonna be a major thing. Not only company reputation has been affected, you have trust of customers in addition to company’s reputation. And you also get the PDPC come after you.

Another Interviewee, DPO and CISO of MNC, related the “nothing to hide” with honesty and internal sense of duty and responsibility to the public behind the Decision-making.

“Of course, Simple. Honest. We don’t want to hide information that consumers or individuals have a legally protected right to know. So, that’s being honest and being in compliance with the law. Of course, personal data law has specific obligations and requirements. It only affects a few individuals. I would send them notices or compensation according to the law so we could close the case. Again, [if] it affects a certain number of individuals, then we should do more, like notifying the regulators and [making a] public announcement to apologize. If the law does not require us to do so,like in SG [Singapore], as a DPO, I am looking for the seriousness. How serious the breach is, or if it is something minor. We make a determination somewhere between the line. Serious is when it affects thousands, a sizable number of customers or data subjects. Then, I will highly recommend to management that someone notify it. It’s part of the public responsibility or social responsibility.

Better Tell It Now or Never:
The interviewee, chief regional privacy of MNC, mentioned: “that would be the law or possible serious misuse of data like fraud or it gonna be out on the papers, hackers can access the data or threatening them. The cost of notifying breach is massive, benefit is if it is a big incident to begin with. In Australia, they put up their hands in the air, we gonna manage it. If we know that it gonna come out in the end, that’s the only situation I can see might benefit be telling consumers. Other than that, it depends on the incidents, if they are really affected. Our law is not protecting privacy but it’s about data protection. From organizational perspectives, in fact, we don’t want to do that unless we really had to and that’s the thing.