INFORMATION PRIVACY: WHO’S RESPONSIBILITY? —A CASE STUDY ON THE LEGISLATIVE PROCESS OF PERSONAL DATA PROTECTION LAW IN TAIWAN

Shirley Ou Yang
NTU, shirleyouyang@ntu.edu.tw

Follow this and additional works at: http://aisel.aisnet.org/pacis2014

Recommended Citation
http://aisel.aisnet.org/pacis2014/269
INFORMATION PRIVACY: WHO’S RESPONSIBILITY?
—A CASE STUDY ON THE LEGISLATIVE PROCESS OF PERSONAL DATA PROTECTION LAW IN TAIWAN

Research-in-progress

Shirley Ou Yang, Graduate Institute of National Development, National Taiwan University, Taipei, Taiwan, R.O.C., shirleyouyang@ntu.edu.tw

Abstract

Information privacy is one of the most significant ethical issues of the information age. The advance of ICT has fostered free flow of information which has led to increasingly serious information security problem. Prior organization-level research has investigated the management of privacy concerns to avoid damage to firms and organizations. Few studies focus on the firm’s responsibility to safeguard information when facing changes in the institutional environment. Through an interpretative case study, this research analyzes the actors and issues that have appeared throughout the process of data protection legislation in Taiwan. The findings suggest that the data protection policy making in Taiwan has taken a parental pragmatic approach, leading to the ongoing hand in hand relationship between government and market. Online social norm view, technological view and information ethics view have been oversighted in the policy making process. I argue that IS researchers and IS managers need to move beyond an organizational view on information privacy, and play a more active role in participating in the public debate and discussion on privacy and data protection issues. I suggest the managerial responsibility for information liability should be taken seriously in forming a reasonable and appropriate institutional environment for a firm’s organizational privacy behaviour.

Keywords: privacy, personal data protection, data protection act, information ethics.
1 INTRODUCTION

The breach of personal data privacy has become a prominent issue in the network society. The rise of search engines, social networking sites, and blogs has made personal data more mobile, setting it free from dull databases. Rampant computer viruses, hackers, the abuse of data access by internal personnel, peer-produced privacy violations, Internet transactions disputes, and system invasions have generated wide information security concerns. These issues could easily cause colossal losses to individuals, enterprises and the government, bringing about ever increasing uncertainty and risk.

International initiatives to protect privacy and personal data have involved considerable co-operation and tension between countries. The European countries tend to view privacy as a fundamental right, deserving comprehensive legislative safeguards. The Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Individuals with regard to Automatic Processing of Personal Data and the European Union (EU) Directives on data protection are among the most influential agreements that now form the basis for privacy law in EU member countries (Rule & Greenleaf, 2008; Heisenberg, 2005).

The America and Asia Pacific region, in 2005, also reached an agreement on the Asia-Pacific Economic (APEC) ‘Privacy Framework’ to guide their respective approaches to regulation. The Framework was endorsed by most of the APEC states, including Taiwan. The priority was economic concerns rather than the protection of basic human rights. It was nonetheless a significant first step in arriving at privacy policy consensus for a region, characterized by great cultural, ethical and legal diversity (Bygrave, 2008).

In accordance with the APEC ‘Privacy Framework’ and in order to follow the globalization trend of personal data protection, the Congress of Taiwan passed its "Personal Data Protection Act (PDPA)" in May 2010. Because the enforcement rules of the PDPA are still controversial, the new law has only partially come into force, as of 2014. The most pervasive and profound influence of this new law is the breaking of the industrial-type constraints established under the old personal data protection system, but applying the new legal regulations on data collection, processing and utilization of legal persons, groups and individuals, as one whole integration is proving an imposition. This has apparently had a tremendous impact on all types of business marketing that massively collect consumers’ data as well as corporations and individuals who possess all kinds of databases.

Even though the international initiatives to protect privacy and personal data have long been developed, a recent report conducted by the British Equality and Human Rights Commission suggests that current privacy law is failing to stop breaches of personal data privacy and is not keeping pace with the rapid growth in personal data collection. The technological breakthrough and its chief by-product, the Law of Disruption, still keep taking the lead and make the old law hard to catch up with (Downes, 2009). Prior legal research has offered a number of important insights into the discussions of enforcement of personal privacy protection, ranging from technology controls (Zittrain, 2000) and commercial data collection regulations (Pasquale, 2008; Hodge, 2006) to market forces, social norm (Lessig, 1999; Rubin & Lenerd, 2002) and data “ownership” (Smarr et al. 2007; Naone, 2008). However, the policy debates in international forums over the past two decades, have largely presented a Western, liberal, democratic view, the privacy development in the Eastern, authoritarian culture has rarely been addressed (Bygrave, 2008). Privacy and personal data protection in IS literature study has nevertheless been ignored.

This study seeks to echo Bygrave’s call for more engagement with Eastern, especially Chinese, privacy issues. The purpose of this paper is to unfold the social construction of the legislative process of the PDPA in Taiwan, by investigating the conflict and struggles among actors and different stakeholders and the multiple rationalities presented during the legislative process of the PDPA (2008-2010). The following focal questions are addressed in this study: (1) which actors and stakeholders supported what competing issues and standpoints that shaped the present privacy and information security policy in Taiwan; (2) how a model regulating behaviour in cyberspace might effectively assist in a more comprehensive social construction process of privacy policy making? (3) What kind of policy decision
making model is identified in Taiwan’s PDPA legislation process? Who will inevitable be responsible for drawing a line in the dilemma economic concerns and risk concerns of privacy rights?

2 LITERATURE REVIEW

2.1 The Concept of Privacy Rights - Legal Perspective

The right to privacy is a widely discussed subject of contemporary public law theory. Originally, this concept was first brought up by Americans Warren & Brandeis (1890). They believed common law should protect "personal privacy”, that is, "the right to life is to have the right to enjoy life” – meaning “the right to be let alone”. Protection of privacy right in the U.S. Constitution mainly resorts to the Fourth and the Fifth Amendments. The Fourth Amendment protects the people for the safety of their persons, houses, papers and effects – free from unreasonable searches and arrests. It sets an important foundation for privacy protection. While the Fifth Amendment prohibits compelling anyone from disclosure of personal information of those involved in criminal cases or any other government records of proceedings, and is another type of privacy protection (Rule and Greenleaf, 2008). Traditional privacy protection concerns how to resist over-interference of state power into private sectors, as well as relevant prevention and remedy measures.

With the advent of the digital era, the information influx of the individual's family, education, community attributes, political orientation, spending habits, credit records, even medical records, comes almost 24 hours a day from electronic databases all around the public and private sectors. As a result, the risk to privacy in a network society has been stretched from the public sector intrusion on the private sectors to the private sector intrusion on individuals in seeking market interests, by massive and systematic collections, storing and using personal information, without letting the persons involved know it. For example, massive search features of Gmail use associated text advertisement mechanisms. The U.S. counter-terrorism measures use biometric identification information, and a variety of electronic surveillance (e-interpellation) as well as data mining technologies. There by the possibility of private intrusion on individuals is no longer limited to the physical space invasion, but gradually re-draws the public and private boundaries and personal self-determination space. The traditional concept of passive protection of individual privacy right of being alone has to be reshaped.

Recent studies have put forth information autonomy theory, which elaborates the privacy right and personal right. The theory argues that the disclosure and the usage of personal data should be a matter of individual decision. According to German Basic Law, the information autonomy is recognition of one’s decision on the provision and usage of his/her personal data, gifted with active participation and the possibility of forming self-determination, and is used as a passive freedom right to resist arbitrary interference from others. (Liu, 1999, 2000)

Most of the previous privacy protection discussions, from a legal perspective, normally focused on the individual personality rights and information autonomy. Namely, these studies adopt the units of analysis on individual level, but very few of them address privacy issues on a complete industrial level, nor on the dynamic law-making process.

2.2 Research on Information Security and Privacy Threats – IS Perspective

The IS research, in contrast, has largely addressed data protection issues with a corporate governance concern, regarding data as important corporate assets. Prior research found the privacy behaviors in organizations were mainly reactive and driven by external pressures, for example the international information security standards. The implementation of information security is to reduce information security risks that the organization may face, to mitigate possible losses, and therefore to ensure continuity of business operations. (Zafar & Clark, 2009; D'Arcy & Hovav; 2008; Backhouse et al. 2006; von Solms, 1994; Straub, 1990) Accordingly, information privacy issues can only become a less attended legal and ethical subject among all the many information security management subjects (such
as: risk management, awareness and education, information security policy and governance, information security investment strategy, accounting and auditing, etc.)

Such a plight can be witnessed from the quantity of information security and privacy studies published in the past top IS management journals. In the top three IS journals MIS Quarterly, Information Systems Research and JMIS, even the quantity of the less attended papers about information security was three to four times more than that of privacy rights. Papers about privacy rights, during the two to three decades of the three journals, had no more than 20 publications. The small amount of privacy papers demonstrate that the subject of personal data protection and privacy rights have long been ignored by information management studies.

Privacy in these publications can generally be divided into three main categories of organizational privacy and information protection obligations; consumer concerns about privacy; development of privacy rights measurements and privacy risk offset tools. Smith et al. (1996) collected literature of consumer concerns about privacy rights and grouped them into different types of data collections, namely, unauthorized secondary use (internal/external), improper access, data errors and reduced judgment and combining data. Culnan and Williams (2009) later classified information privacy into two major categories of information reuse (aggregation and data mining, new uses and sharing) and unauthorized access (browsing, security breaches), in which the former may cause potential harm including incorrect inferences, decision-making based on errors, exclusion and intrusions, while the latter may cause damages including breach of confidentiality, insecurity (e.g., identify theft). Agrawal and Srikant (2000), as well as Li and Sarkar (2006), then proposed the interference method to solve the conflicting dilemma between data mining and confidential data protection. In recent years, there is more related research taking consumer concerns view to address privacy issues (Anderson and Agarwal, 2011; Tsai et al, 2011; Jiang et al., 2011). All these information management literatures have acknowledged that privacy is one of the most critical corporate topics by enterprises in the information age.

These studies, however, take the organizational view to deliberate on how to manage the use of personal data without affecting the consumer’s purchase intention, in a manner of taking the privacy issue as a uncertainty factor management for alleviation of possibly business losses (Pavlou et al., 2007; Hui et al,2007; Son & Kim, 2008). Very rare, are studies with industrial views about the corporate manager’s responsibilities for the information privacy, when facing changes of their institutional environment (Culnan & Williams, 2009; Straub & Colline, 1990).

As MISQ senior editor McFarlan (1988) said, privacy rights are now a more popular social topic in this information age than in the past. Previously ignored and proposed by only a small number of social groups and sociologists in the frontline. Nevertheless, their concerns were from views different from that of information management, with less deliberate insights into the technological possibilities and limitations. He urged that information management scholars should explore studies with much broader societal issues and converse with sociologies, to collaborate in solving societal issues brought forth by technology. McFarlan believed those issues are also important to business practitioners, for their endeavor in this field can help to reduce inadvertent damages and financial losses to individuals and organizations. He also urged that the IS scholars look into corporate internal and external privacy right issues, and the new kinds of monopolies created by today’s information technology, along with the property issues of copyrights, patents, intellectual property. He suggests the businessman’s perspective should be added to the existing perspectives of the individuals, government agencies and lawyers. McFarlan emphasizes that this social and humanistic study will help the development of the IS field, cultivate young scholars and make progress of the overall IS education program.

Twenty years have passed since the appeal from McFarlan, but societal issues such as the privacy right in the information management areas still look like virgin territory. This paper is a response to such an appeal, from an institutional point of view to investigate privacy issues. Our attempt is to bring out the attentive dialogues between the law and the information management systems.
3 THE ANALYTICAL LENS

In this paper, the analytical lenses adopted are drawn from two perspectives: Lessig’s (1999) Regulation Model of Behaviour in Cyberlife, see Figure 1, and Irwin’s (1995) Model of Technology Policy Decision-Making, see Figure 2. Although these two streams of thinking take different approaches to look at technology policy making, I consider that the combination of the two can complement each other and offer more to reveal the rich insight gained during our empirical investigation.

Technology policies adhering in between scientific rationality and multiple rationalities appear ambiguous. The formulation of technology policies in the post-industrial society highly depended on experts and professionals on one hand, to expand scientific rationality and provide objective and neutral knowledge for governance; on the other hand, it had to be admitted that scientific experts are also set in the context of the operational behaviors, developed through trial and error.

Lessig (1999) suggested the regulation in the cyberspace should be considered through a holistic view. He proposed a model describing the regulation of behaviour in cyberspace dependent on four constraints—the law, social norms, the market and technological architecture which together regulate the behavior in the cyberspace. Each constraint imposes a different kind of cost for the relevant behaviour engaging in the cyberspace. Law constrains through the punishment it threatens; while markets constrain through the price that they exact. Changes in any one will affect the regulation of the whole. Norms constrain through the commonly held standards a community accepts, and architecture constrains through the physical enablings/burdens they impose. The four constraints can support or oppose the other, and each of them can be regarded as a distinct modality of regulation. Since the regulation though making law is a more expansive sense of regulation, Lessig suggests that the four modalities should be considered together as a complete view to regulate behaviour in cyberspace. This research applies this perspective.

Adapted from Lessig (1999), p. 88

Figure 1. A Model of the Regulation in Cyberspace

Unlike Lessig’s cyberspace focus, Irwin (1995) proposed three different models of technology policy decision-making, see Figure 2, an expert approach, participatory democracy approach, or a pragmatic approach, to explain the complex decision-making process and the formation of science and technology policy making, in the face of the risks and threats brought forth by technology. The so-called expert orientation is on the assumption that only the expert assessments can bring reasonable and objective decision-making. The participatory democracy approach is a technology decision-making system that allows potential victims a fair opportunity to voice concerns. The system permits a wider cross-examination of expertise and both encourage and empower citizen views and understandings. As for the pragmatic approach, it takes the applicability and manageability to reconcile the thinking of experts and democracy. It stresses the responsibility of industrial self-regulation rather than government regulation. The approach is based on the principle of practicability and manageability for consultation space and
close collaboration between the government and the industries, with flexibility, knowledge and low intensity conflict, to commit to consensuses, instead of opposite debates (Irwin, 1995).

**Figure 2. Different Models of Technology Policy Decision-Making**

For this paper, in order to investigate how the institutional environment of privacy right has been developed in Taiwan, we see that the four constraints of regulating behaviour in the cyber place are particularly relevant and useful. As different interest groups have made attempts to influence the PDPA law-making process, Lessig’s model provides broad and complete angles of the stakeholders. Adopting this analytical lens allows us to investigate the influential forces of the participants and discussed issues in the amendment process of the Taiwan’s PDPA.

This paper suggests by integrating Lessig’s model with Irwin's analysis framework, the micro and macro view acted complementarily by each. We consider the integrated analytical lenses will guide our empirical work and identify the relevant social groups and issues arising during the amendment process of Taiwan’s PDPA.

## 4 RESEARCH METHOD

The paper chooses an exploratory case study approach, as the author has assumed that access to reality is through social constructions such as language, consciousness and shared meanings (Orlikowski & Baroudi, 1991). Klein & Myers (1999) noted that understanding of individual cases requires participation of meetings, semi-structured interviews, observation records, data collection and analysis of industrial reports. Therefore, in the PDPA study, a qualitative approach was used to collect and analyze data. Specifically, a two-phase study was undertaken. In the First Phase, we collected secondary data about the legalization process of the PDPA in Taiwan. This included the governmental information policy plans, volumes of the Legislative Yuan (Congress) Gazette (Jan 1993 to April 2010) and the PDPA related meeting minutes. Besides, local news collections through the Congress database, academic articles related to this Act and the website articles of the main actors and privacy watchers, such as the Ministry of Justice, the Taiwan Association for Human Rights (TAHR), the National Union for the Protection of Personal Data (NUPPD), were also collected. In addition, the lobbyist documents from different interest groups also contributed.

In the Second Phase, we conducted seven semi-structured phone interviews, including key actors from the Legislative Yuan, bipartisan representatives from the ruling and oppositional parties; Ministry of Justice Legal Services Division; and policy makers from the Executive Yuan Science and Technology Advisory Group. The interviews were conducted from Sept 2009 through August 2010. Each interview lasted 45-90 minutes. The author also participated in meetings and seminars related to information privacy issues held by both public and private sectors. These included the Executive Yuan's "Shaping Information Security Culture, Promoting Information Security Output" Strategy Review Board (SRB) meetings, and elite public information seminars "New Information Security Concept in the Cloud Technology Age". Observation records and summaries were made.
To analyze the data, the researcher first organized the secondary data chronologically and listed major events of the PDPA legislative process in Taiwan. Triangulation was used to compare the first-hand and secondary data, and when data appeared inconsistent, the author would contact the person involved by E-mail or phone, and double checked the observation records, further document collection reinforced the data, with all the efforts, to ensure the consistency and reliability of the case studies undertaken for this paper. The research was carried out during the 7th term of the Legislative Yuan (February 2008 to April 2010).

5 PRELIMINARY RESULTS

5.1 Case Description

Taiwan’s privacy protection legislation has been established by sector. The idea of creating a special data protection law in Taiwan was born during the period of the 1990s when Taiwan was actively trying to join the WTO. It was a result of the circumstances of avoiding European Union’s accusations of this country’s lack of personal data protection. The first bill "The Computer Processed Personal Data Protection Act" was passed in 1995. This Act, however, only set the norm for the management of computer-based personal data as the protected object, excluding manual data, and only applies to 8 specific industries including hospitals, schools, mass media, telecommunication industry, credit industry, insurance industry, financial industry and securities industry. It served however as an important predecessor of the PDPA which would pass in 2010.

The second draft of the data privacy driven by citizens’ action groups, the so-called “privacy watchers”, such as TAHR, NUPPD composed of more than 50 civic organizations. As the rise of information technology added a whole new dimension to these legal perceptions, leading to the mounting of improper personal data collection and disclosure, since 2000, these so-called “privacy watchers” have continually tracked the issues of personal data privacy rights within Taiwan, and unceasingly placed more and more stress on the government to amend the law.

In response to the grassroots calls and the global trends of privacy protection, the Ministry of Justice then in 2002 formed a law amending group and undertook the "Computer Processed Personal Data Protection Act Amendment Draft." However, the draft was not successfully scheduled in the legislative agenda of the Legislative Yuan’s 5th term and was returned. In 2005 the Ministry of Justice re-submitted the amendment draft to the 6th term of the Legislative Yuan, but the draft failed to enter into the legislative review process. Not until the 7th term of the Legislative Yuan in 2008, was the draft again sent for legislative review.

5.2 Current Progress

In the first phase of the analysis, I identify three stages of the PDPA review process in the committee of Legislative Yuan: (1) The Review Stage: legal community and civic organizations were concerned about controversial issues such as public personality rights and the conflict interests with the legislative immunity rights; (2) The Negotiation Stage: industrial and civil society lobbyists were in tit for tat status; (3) The Peak Stage: the mass media involvement made both parties sit down for negotiation and swiftly pass the Third Reading. See Figure 3.

In the second phase, I then triangulated the preliminary analysis from the Legislative Yuan (Congress) Gazette and other secondary data with the first hand interview transcripts and identified controversial issues and social actors that had appeared in the different stages of the process of the PDPA revision, see Table 1. The controversial issues were: the Legislators’ speech immunity, judicial/administrative investigation power on sensitive data, data ownership, dedicated central agency, penalties, freedom of press, people online behavior.
2008 Feb → 2 Versions of PDPA (the Executive Yuan/Legislator X) submitted to the Legislative Yuan for First Reading.

2008 Mar → PDPA was sent to the Legislative Yuan Conference for article-by-article review.

2008 Sept → TAHR held seminars on PDPA.

2009 Mar → Ministry of Justice held public hearings on PDPA

2009 Aug → The Executive Yuan Science and Technology Advisory Group held SRB meetings.

2009 Oct → The civic organizations visited Ministry of Justice and legislators

2009 Nov → The ruling and opposing parties negotiated and reached consensus.

2009 Dec → Telecommunications Association lobbied penalty terms.

2010 Feb → The Internet service providers pushed the Legislative Yuan to pass PDPA

2010 Apr 20 → The amendment passed the Second Reading.

2010 Apr 21 → News media massively reported that PDPA is obstruction to freedom of the press.

2010 Apr 27 → The Legislative Yuan re-examined the new amendment version proposed by Ministry of Justice, and directly sent it to the Third Reading.

Figure 3: Journey of the Personal Data Protection Act Amendment in the seventh term of the Legislative Yuan

Drawing on Model of the Regulation in Cyberspace (Lessig, 1999), I further examined the actors and stakeholders for their standpoints on the issues, and the dynamic relationships which had driven the outcome of the new Personal Data Protection Law. The preliminary results suggest that the PDPA review process in the Legislative Yuan, technological architecture view seldom contributed to the discussion. Although the sector played an important role in the forming of the PDPA, during the negotiation stage in the review process, the law view and market view appeared to take the lead in the discussion.

In the following phase, I will further explore the meeting minutes, further secondary data and the literature from the legal and IS perspectives, made to discuss the following points: (1) The regulating concerns of the stakeholders; (2) the role of technology policy decision-making in the information age; (3) organizational privacy: the social responsibility of an information systems manager. Through a dialogue with the prior study and our empirical work, I attempt to unfold the current technology policy decision-making pattern in Taiwan in terms of Irwin’s (1995) Model in order to make suggestions to the business leaders and policy makers in further discussions.

6 EXPECTED CONTRIBUTION

This paper aims to shed light on the forming of institutional environment for organizational information privacy behaviour. By incorporating an integrated view of Lessig’s model with Irwin's analysis framework, I hope to extend an understanding that information privacy is not alone the concern of
government and market. Rather, the online social norm view, technological view and information ethics view should have taken and be encouraged to take a more active role in the policy making process. I suggest the managerial responsibility for information liability should be taken seriously in forming a reasonable and appropriate institutional environment for organizational privacy behavior.

Theoretically, this study contributes to the IS literature by incorporating Lessig’s model with Irwin's analysis framework to unfold the socio-economic and political information of privacy policy making in Taiwan. We provide a real life case in Taiwan to fill the gap of insufficient privacy rights work in the IS field, especially in the Asia Pacific countries. The evidence of this case study echoes McFarlan’s argument that more collaboration IS scholars with sociologists should interact to solve societal issues brought forth by technology. This highlights the development of IS field and IS education with more social and humanistic endeavours.

Practically, our analysis can also provide insights into managerial responsibility for information liability in forming the institutional environment. In the hopes of drawing attention to business leaders and IS managers, moving beyond an organizational view on information privacy, the study suggests IS managers, practitioners, and even hackers should take a more active role in participating in the public debate and discussion on privacy and data protection issues. Together, I hope this study will make a number of important contributions to both theory and practice in the privacy policy making process. There by encouraging a synergy and better balance of law, social norms, the market and technological architecture for a more responsible and accountable information privacy environment.
<table>
<thead>
<tr>
<th>Stages</th>
<th>Controversial Issues</th>
<th>Actors and their Standpoints</th>
<th>Contribution of cyberspace regulating modalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Review</td>
<td>Legislators’ Speech Immunity</td>
<td>3 ruling party legislators; 3 opposition party legislators</td>
<td>Ministry of Justice; L, M, N, A</td>
</tr>
<tr>
<td>I. Review</td>
<td>Judicial / Administrative Investigation Power</td>
<td>1 ruling legislator</td>
<td>Ministry of Justice; L, M, N, A</td>
</tr>
<tr>
<td>I-III</td>
<td>Data Ownership</td>
<td>Legal scholars, Civil right groups such as TAHR, NUPPD.</td>
<td>Ministry of Justice; L, N, M, A</td>
</tr>
<tr>
<td>I-III</td>
<td>Dedicated Central Agency / Safety Valve</td>
<td>TAHR; 1 ruling party legislator; Legislator X’s Version: Proposing Ministry of Justice is the executive authority</td>
<td>Ministry of Justice; L, N, M, A</td>
</tr>
<tr>
<td>II Negotiation</td>
<td>The collection of Personal sensitive Data</td>
<td>Executive Yuan version originally supports collecting sensitive data because of agreement from the person involved.</td>
<td>L, N, M, A</td>
</tr>
<tr>
<td>II Negotiation</td>
<td>Penalties</td>
<td>1 ruling party legislator; 1 opposition party legislator; Telecom Association, LegislatorX’s Edition</td>
<td>L, M, A, N</td>
</tr>
<tr>
<td>II Negotiation</td>
<td>Accelerated Review</td>
<td>1 opposition party legislator; Yahoo, PC Home and other network providers</td>
<td>L, M, A, N</td>
</tr>
<tr>
<td>III Peak</td>
<td>Dispute on Freedom of the Press</td>
<td>The Journalist Association (bipartisan negotiations to remove it in Second Reading, but was resurrected in Third Reading)</td>
<td>Ministry of Justice; L, M, N, A</td>
</tr>
<tr>
<td>III Peak</td>
<td>People online behavior</td>
<td>Mass media criticized that the amendment could set forth law breaking by just posting friends photos on Facebook. Ministry of Justice agree to revise</td>
<td>L, M, A</td>
</tr>
</tbody>
</table>

Table 1: The Major Actors and Issues in Process of PDPA revision

*L: Law; M: Market; N: Norms; A: Architecture
References


