Hexa–Dimension Code of Practice for Data Privacy Protection

Wanbil William Lee
Wanbil & Associates, Hong Kong

INTRODUCTION

Contemporary cyberspace inhabitants live and work in a *technology-driven information-intensive* era, a *phenomenon* born out of a *vicious circle*. The consequence is a mixture of blessing and nightmare. Data protection emerges as a critical concern and data privacy protection an urgent and vital problem for information security management. Given the situation, the front-line information security personnel is among the first to bear the brunt and in dire need of a pragmatic guidance.

A recently developed set of International Data Privacy Principles was proposed as a reference considered to be useful for tackling the *first need* (Zankl, 2016). Hong Kong's Personal Data (Personal) Privacy Ordinance (PDPO), a data protection principle-based law like many others legislated by western jurisdictions, which has been in force for a number of years (Chang, 2016), can make a contribution the *second need*. To address the *third need*, a framework that comprises a 6-d code based on the 6-d metric and an operationalization scheme is recommended.

A first-cut version of the framework was recently presented to an audience of Information Security Management specialists (Lee, 2015a). The rationale of the metric, the definition of the code and its worthiness for recommendation, and an indicative guideline to operationalize the code, are described in this article.

BACKGROUND

Technology-Driven Information-Intensive Phenomenon and the Vicious Circle

Netizens are provided with such technologies as *Customer Relationship Management*, *Web-lining* and *Call Centre*, and so on; they can by means of these facilities conduct their daily activities more efficiently and effectively, and optimize the outcome of these activities, because they are better-informed and able to innovate marketing, to accelerate business promotion, to enlarge data storage capacity and communication coverage, to increase retrieval facilities, and to improve transaction speed in a more transparent and open environment. But then they will need to rely increasingly heavily on the technologies. While transparency and communication keep on improving, more and more data are consumed and correspondingly generated. Briefly, "the happier the consumers of information, the higher the demand for more information and the more the technology is used, the more the data and the speedier the processing, the more transparent the cyberspace, and the happier the consumers" – a *vicious circle* is formed; the *technology-driven information-intensive phenomenon* created. (See Figure 1).

The consequence is good and bad. The good is the accelerated arrival of such technologies as Big Data, Cloud Computing, Internet of Things

Figure 1. A conceptual graph of the circle and the phenomenon
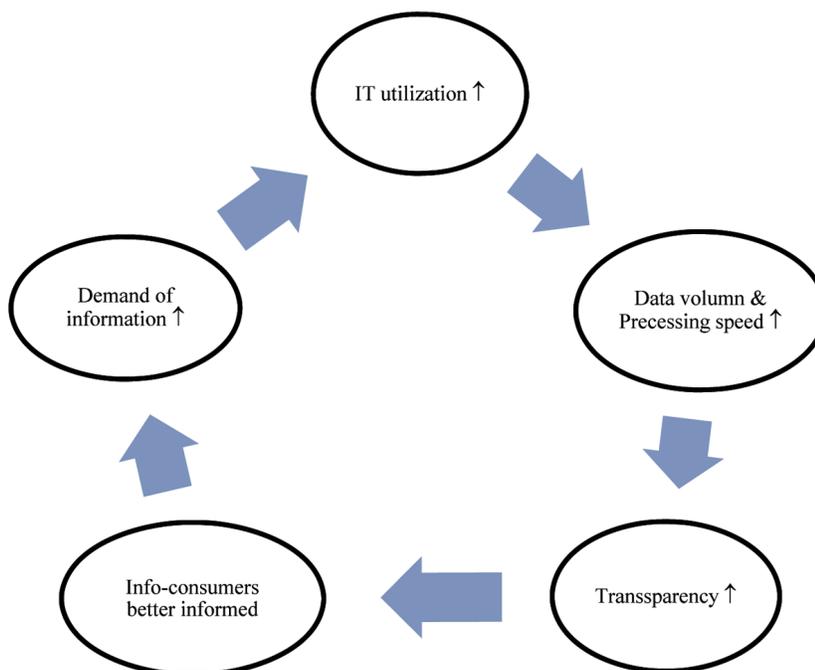
and a plethora of social engineering tools. These technologies enable integration of massive, scattered datasets, efficient interpretation of the integrated data, and speedier communication of the information. An obvious benefit is that with a huge amount of information being made available, the cyber-world becomes more transparent and netizens are better informed. And the bad is that there emerges a plethora of additional security threats bred in the loopholes in the new technologies, in the use of them or in the facilities enabled by the massive volume of data they generate, which the cyber-miscreants are ever lurking around to exploit when detected. However, that numerous clandestine activities are brought to light, for example, the Snowden episode (*South China Morning Post*, 2013) and the Panama Papers leak (Wilson, 2016), can be beneficial to some people/ organizations and adversary to others.

Data Privacy Protection Problem

The problem is rooted in the *way* the data are collected about and are used adversely against data subjects, and the *right* of the data subjects to that data, and has to deal the *techno-ethical-risk* which is originated in the way the technology is applied and the human users of the technology and the data, though the technology per se is neutral, yet the use of the technology is not (Parker, 1986; Neumann, 1995; and Williams, 1997). The protection of data privacy means to ensure that data privacy is not breached, that is, the data content is securely stored and accessed only with proper authority, and that the right of the data subjects not abused. Solving the problem means developing, reviewing, and implementing information protection and data privacy policies, standards, guidelines and processes (the policies), and mitigation measures; and to identify new technology risks; and to ensure that the policies are appropriately enhanced, communicated and complied with, and that mitigation measures are properly implemented.

The issue of data privacy invasion and the harmful impacts thereof have extended beyond the individuals and corporations to the regional/ national governments, instanced by the UK House

Related Content

Hybrid Data Mining Approach for Image Segmentation Based Classification
Mrutyunjaya Panda, Aboul Ella Hassanien and Ajith Abraham (2016). *International Journal of Rough Sets and Data Analysis (pp. 65-81).*
www.irma-international.org/article/hybrid-data-mining-approach-for-image-segmentation-based-classification/150465

Modeling Rumors in Twitter: An Overview
Rhythm Walia and M.P.S. Bhatia (2016). *International Journal of Rough Sets and Data Analysis (pp. 46-67).*
www.irma-international.org/article/modeling-rumors-in-twitter/163103

8-Bit Quantizer for Chaotic Generator With Reduced Hardware Complexity
Zamarrud and Muhammed Izharuddin (2018). *International Journal of Rough Sets and Data Analysis (pp. 55-70).*
www.irma-international.org/article/8-bit-quantizer-for-chaotic-generator-with-reduced-hardware-complexity/206877

Serious Games Advancing the Technology of Engaging Information
Peter A. Smith and Clint Bowers (2018). *Encyclopedia of Information Science and Technology, Fourth Edition (pp. 3327-3336).*
www.irma-international.org/chapter/serious-games-advancing-the-technology-of-engaging-information/184044

Human Ear Recognition System
Durgesh Singh and Sanjay Kumar Singh (2015). *Encyclopedia of Information Science and Technology, Third Edition (pp. 5475-5481).*
www.irma-international.org/chapter/human-ear-recognition-system/112999