Hexa-Dimension Metric, Ethical Matrix, and Cybersecurity

4

Wanbil William Lee
The Computer Ethics Society, Hong Kong & Wanbil and Asssociates, Hong Kong

INTRODUCTION

Enormous spending on protecting data continues, hacking continues, yet data protection must helplessly go on. This is attributable to a *vicious circle* born out of a technology-driven information-intensive *modus operati*, culminating in a *chronic problem* which is complicated by a *tripartite relationship* and exacerbated by a muddled view of the key concepts which hinders a wholesome appreciation of the problem. The consequence amounts to business opportunities for the data protection enterprises and employment opportunities for the information security practitioners but a nightmare that haunts corporate and information security managers and the netizens at large. Given the status quo, an ethics-based framework was perceived and developed with the aim to mitigate rather than eradicate, to lessen the incidence of hacking or make hacking exasperate. Grounded in Ethical Computing (Lee, 2015b), this ethical approach aims to identify the concerns of the stakeholders against the ethical values, and to evaluate and balance the issues thus identified and discovered which invariably involve conflicting interests. This Ethical Matrix and Hexa-dimension Metric (Lee, 2019) poise to lend a hand. This article is an exposition of the problem that leads to the new methodology and will end with an illustration of the newly adapted/developed tools.

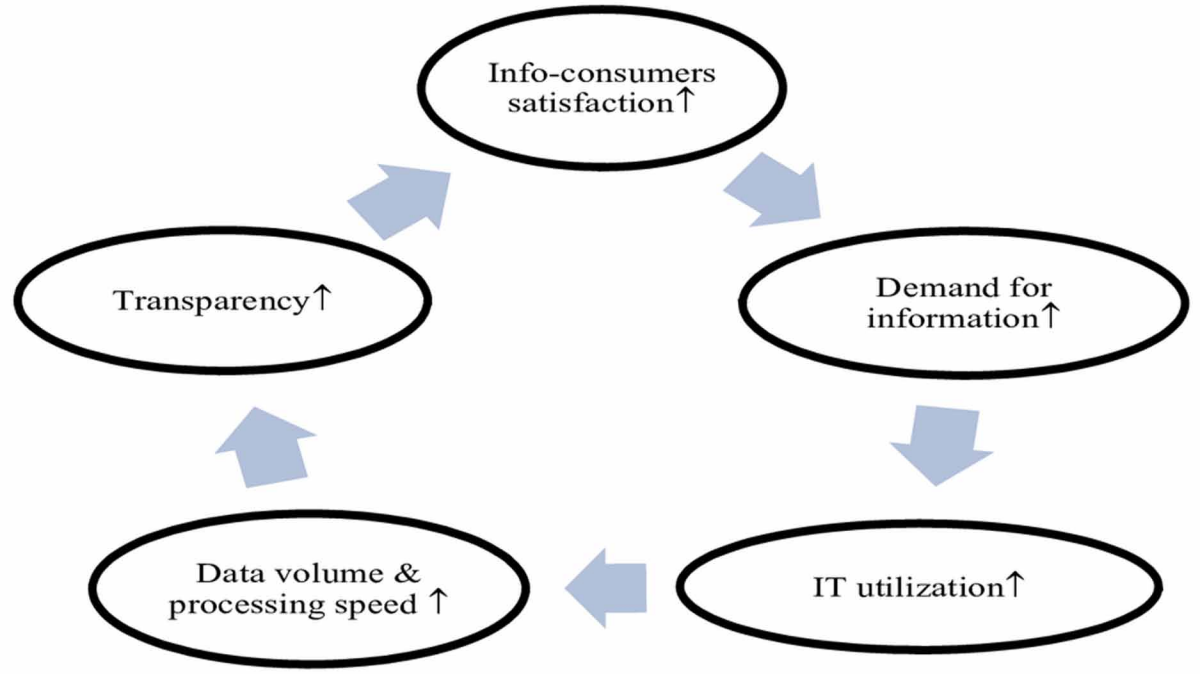
BACKGROUND

Data Generation/Consumption/Protection – A Vicious Circle

Netizens can by means of the facilities provided by advanced interruptive technologies such as Big Data, Cloud Computing, IoT, AI and ML and so on conduct their daily activities more efficiently and effectively. These technologies enable integration of massive, scattered datasets, efficient interpretation of the integrated data, and speedier communication of the information. These facilities bring along obvious benefits and security threats on account of a huge amount of information being made available. As the cyber-world becomes a more transparent and open environment, netizens 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. At the same time, through that transparency loopholes in these new technologies where threats are bred provide opportunities for the cyber-miscreants to exploit and attack. However, as the clandestine activities that are brought to light, for example, the Snowden episode (*South China Morning Post*, 2013) and the Panama Papers leak (Wilson, 2016), the consequences can be beneficial to some people/organizations and adversary to others.

DOI: 10.4018/978-1-7998-3479-3.ch030

Figure 1. A conceptual graph of the circle and the phenomenon



The better-informed are the consumers, the more information is demanded and supplied. Supplying more information improves profit and uses more technologies. Using more technologies makes more information available. Consumers are happier and demand more information. More information is supplied and mote technologies are used. The volume of information increases as more information is collected and generated. This culminates in a *vicious circle*.

Data Protection: A Chronic Problem

We spend more (the big spending on cybersecurity), we lose more (still get hacked and the enormous aftermath of the cyberwars) but data protection has to go on. The symptom is big spending and cyberwar and the cause is that we do not take ethics seriously.

The Big Spending: This the following exemplify: US$1.5 billion by American financial institutions alone (US Homeland Security Research, 2016). £6.2m in 2016 compared to £3m in 2015 by UK organizations (CyLon, 2017). Gartner predicted in 2017 that worldwide spending to grow to $93 billion in 2018 from $86.4 billion in 2017 (Bradley, 2017), and forecasted in 2018 that Hong Kong's budget for data security (the fastest growing product category) would reach HK$85 million in 2019, mainland China to reach almost 23.9 billion yuan (HK$27.2 billion) and 27.3 billion yuan, respectively 2018 and 2019, and globally, expected spending on information security products and services to reach more than US$114 billion in 2018 and to US$124 billion in 2019 (Bushell-Embling, 2018).

Cyberwar symbolizes nation-to-nation conflicts such as the US-China trade-based and military-oriented cyberespionage (Onag, 2018), the alleged Russian interference of the US general election in 2016 (The New York Times, 2018a), and the UK allegation of Russia's tampering of Brexit voting (The New York Times, 2018b), also denotes conflicts at lower scales such as the fight between advertisers and users of ad blockers (Wicker and Karlsson, 2017) and the dispute between consumers of the digital technologies and