A STUDY OF POTENTIAL PITFALLS IN THE DEVELOPMENT OF SMART CITIES AND MITIGATION MEASURES

RUIQU MA

PhD

The Hong Kong Polytechnic University

2019

The Hong Kong Polytechnic University

Department of Building and Real Estate

A Study of Potential Pitfalls in the Development of Smart Cities and Mitigation Measures

Ruiqu MA

A thesis submitted in partial fulfillment of the requirements

for the degree of Doctor of Philosophy

November 2018

CERTIFICATE OF ORIGINALITY

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces neither material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgement has been made in the text.

Signature:________________

Ruiqu MA

ABSTRACT

Growing urbanization brings about problems, such as traffic congestion, energy shortages, high crime rates, and environmental pollution. Therefore, the concept of a "smart city" (SC) was introduced as an innovative approach to solving these problems and improving the quality of life using advanced information and communication technologies (ICT). However, *"Smart cities are not a panacea for all ills, and they bring their own problems"*. Based on an extensive literature review, the research firstly identifies four potential pitfalls in the development of SCs. They include system information insecurity, privacy leakage, information islands and digital divide. However, there is a lack of systematic and empirical research on the potential pitfalls of SC development concerning both technological and non-technological aspects. Existing assessment schemes of SC development mostly focus on the positive and functional aspects of SCs, but sparingly evaluate the possible downsides. A SC cannot claim to be successful by solely measuring how much it has done or what it aims to achieve without designing against possible pitfalls. Hence, this research aims at bridging these knowledge gaps.

This research has three objectives, namely, (1) the identification of pitfalls in the development of SCs; (2) the analysis of possible causes and adverse effects; and (3) the development of recommendations for a better SC development. Questionnaire Survey # 1 was conducted on SC experts for them to rate the relative importance of possible causes, adverse effects of each pitfall in terms of its likelihood, severity, and the effectiveness of mitigation measures. Initial findings on the key issues to tackle these pitfalls, and the effectiveness of possible measures to mitigate them were obtained at this stage.

Three case studies were then conducted to investigate the four common pitfalls in the context of several SC projects in Hong Kong to empirically fulfill the second and third objectives. Empirical data needed for the first case study were collected through Questionnaire Survey # 2 to investigate how users perceived these pitfalls in the context of mobile apps that provide real-time parking information. It was found that the concept of SC was not yet popular among Hong Kong citizens. System insecurity and privacy leakage were found to cause concern among the app users, but their awareness regarding protecting personal data left much room for improvement. Digital divide existed widely among disadvantaged groups. Following the questionnaire survey, several interviews were conducted in Hong Kong with the following: (1) stakeholders participating in the smart parking app projects that were initiated by the public and private sector, and (2) disadvantaged people and organizations helping the disabled. Interviews informed that insufficient collaboration among private carpark operators resulted in islands of real-time parking information. Digital divide cannot be entirely narrowed down by the mere provision of ICT facilities but also hands-on training and special care for these groups. The second case study investigated the pitfall of system information insecurity by analyzing the intrinsic reliability of smart parking information systems. It was found that a failure in a central system server may be caused by malicious attacks, human errors, and hardware and software failures. Through the use of Fuzzy Fault Tree Analysis (FFTA), the possible mechanisms of service non-availability and relative importance of events causing service non-availability were investigated. An integrated approach is needed to mitigate against system unreliability. The third case study was on open data development. Social Network Analysis (SNA) was used to investigate the interrelationships of barriers faced by different stakeholders involved, and highlights that open data is the key to bridge over information islands in emerging SCs. It was found that the lack of open data policy should be tackled as a matter of priority to provide technical guidance for the public sector, to ensure data quality and achieve the expected outcomes. It is also necessary to improve the IT literacy/mindset of the public sector, encourage engagement from private entities and provide a feedback loop for users. To conclude, findings obtained from the above surveys and case studies were used to derive general mitigation/preventative measures against each pitfall within “emerging SCs”. This study contributes to the knowledge body by revealing challenges faced by city managers and enabling proactive solutions to alleviate possible downsides of SCs.

ACKNOWLEDGEMENT

First and foremost, I would like to express my profound gratitude to my chief supervisor, Prof. Patrick Lam, for his immense knowledge, patience, and inspiration for my PhD study. Without his precious support, conducting and finishing this research would be impossible. I will bear in mind his belief in pursuing lifelong learning and exploring new domains in my future career.

I also would like to sincerely appreciate my co-supervisor, Dr. C.K. Leung, for his consistent support and encouragement throughout the research work. He contributed his time whenever I needed advice or suggestions about his specializations on electronic and information engineering.

I would like to thank all the interviewees and questionnaire respondents for their valuable time and efforts in providing empirical data for this research.

This thesis is heartily dedicated to my parents. They have been encouraging and supporting me at every stage of my personal and academic life. I would not have made it this far without them. I am also lucky to have good friends, especially Ms. Bingyi Li, Mr. Bai Hua, Ms. Ji Ma, and Dr. Hu Xiao. They brought me much happiness and positive attitude before and during my PhD study.

I am thankful to meet new friends during my PhD study. I would particularly like to thank Ms. Xiaosen Huo, Ms. Yijie Zhao, Ms. Xiaoyin Li, Mr. Khwaja Mateen Mazher, and Mr. Emmanuel Kingsford Owusu. My time in Hong Kong was made wonderful largely because of them. Last but not least, my sincere thanks go to the staff of the Department of BRE. My journey of studying at the Department of BRE leaves me with treasured memories of their kindness.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

APIs	Application Programming Interfaces
B/Ds	Bureaus/departments
CI	Critical Importance
COPO	Chief Open Platform Officer
EAL	Evaluation Assurance Level
FFTA	Fuzzy Fault Tree Analysis
GDPR	General Data Protection Regulation (European Union)
ICT	Information Communication Technology
IoT	Internet of Things
IT	Information Technology
ISO	International Organization for Standardization
NGOs	Non-governmental Organizations
ODbL	Open Database License
OGCIO	Office of the Government Chief Information Officer (Hong Kong)
OL	Occurrence Likelihood
PbD	Privacy by Design
PDPO	Personal Data (Privacy) Ordinance (Hong Kong)
PI	Probability Importance
PSI	Public Sector Information
RI	Risk Impact
SC	Smart Cities
SE	Severity (if it occurs)
SI	Structure importance
SNA	Social Network Analysis
SPIS	Smart Parking Information System
TE	Top Event (of the fault tree)

PRELUDE

A fairly common story unfolds like this.

A man is sitting in a street-walk *café* drinking coffee, planning to drive to his next destination. He connects his smartphone to the surrounding free Wi-Fi network quickly without using a password. He then switches among different mobile applications to check real-time parking vacancy information near his destination because there is no integrated platform of city-wide parking information, which gives the exact location he wants to go to. Suddenly, he receives a series of messages and email push notifications of product promotion, and he starts to doubt the security of the free Wi-Fi network, worrying about the confidentiality of the online bank transactions he carried out 10 minutes ago. As he sits there frowning, an old couple aged about 60 years old, sitting next to him, asks:

- *"Good morning, young man! May we ask if there is any cinema nearby?"*

- *"Of course, there is. Let me check my phone. Yes, it takes only 15 minutes walking to the Grand Cinema."*

- *"Thanks a lot! Can you give us some directions?"*

- *"Turn right when you leave the café, go straight to the first junction, cross it, and turn left. When you see the huge Supermall, go across the footbridge in front of it and…"*

- *"Oh, it's so hard to remember! Thank you so much anyway! We shall ask for further help from pedestrians along the way."*

- *"My pleasure! By the way, which movie do you want to watch? I think you need to book the tickets in advance as it is Sunday today; people usually crowd the cinema."*

- *“What is the most popular movie currently? We do not know how to buy tickets in advance.”*

Then, the kindhearted man opens an online booking system of the cinema with his smartphone to search for movie information and book tickets for them. However, the service turns out to be unavailable, and a prompt message appears, saying that the booking system is down. They smile bitterly at each other.

Consider the above day-to-day scenario in an emerging SC where most services are digitalized and online. Several problems are brought forth, including privacy leakage, information disintegration, digital divide, and system insecurity.

CHAPTER 1 INTRODUCTION

1.1 Research background

1.1.1 Definitions of Smart City (SC)

The World Health Organization (WHO, 2016) forecast that the world's urban population will rise from 54% in 2015 to 66% by 2050. Growing urbanization brings about problems, such as traffic congestion, energy shortages, high crime rates, and environmental pollution. Therefore, the concept of a "smart city" was introduced as an innovative approach to solving these problems and improving life quality; SC uses advanced information and communication technologies (ICT) (Alawadhi *et al.*, 2012; Albino *et al.*, 2015). Cases can be found in different places worldwide. For instance, smart waste management in Barcelona is enabled by Internet-connected sensors and wireless links that are equipped within trash bins to monitor how full they are. Instead of following fixed collection schedules, the cleaners come up with dynamic routes and determine collection frequencies according to real-time information of bin capacity, saving 20%–30% in energy while keeping the streets clean. Transport for London uses advanced video camera technology to make road crossing easy and safe by detecting the number of pedestrians waiting at crossings to adjust the pedestrian crossings' signal change periods accordingly. This practice aims to reduce casualties in London's streets by 40% by 2020 (Cooley, 2014). The smart grid emerged to improve energy efficiency and reliability via automatic electricity dispatch control and other technological advances. The US government has claimed the largest investment for modernizing power grids in US history, that is, USD3.4 billion in grant awards, supporting a wide range of smart grid technologies (Gungor *et al.*, 2011). A new paradigm in SCs is Mobility as a Service (MaaS), which provides customers a platform that integrates all existing transportation options (Expósito-Izquierdo *et al.*, 2017). A known case of MaaS is Uber, which allows users to order a private car through a tracking system to travel. Another is RideScout, a mobile application that aggregates information from public, private, and social transportation services into a single interface. It also includes a social function that allows planning trips in groups by creating user groups and integrating other platforms, such as Google, Twitter, and Facebook.

Since its introduction in the 1990s, the concept of SC is still evolving (Hollands, 2008). No single definition of SC is agreed upon due to numerous purposes (Cocchia, 2014) and various needs and conditions in different cities (Hollands, 2008; Nam & Pardo, 2011; Neirotti *et al.*, 2014). Table 1-1 shows a list of SC's definitions. The list shows that SCs are distinguished by a pervasive use of ICT (Neirotti *et al.*, 2014). This finding is due to the fact that the initial drive of SC implementation is technological innovation rather than policy (Cocchia, 2014). As claimed by Greenfield (2010), SC is about the increasing extent to which cities are composed of ubiquitous information technologies and digital devices.

Table 1-1. A plethora of definitions of SC

Emphasis	Definition of SC	Source
Technology application	*"A smart city is one that has digital technology embedded across all city functions."*	Smart Cities Council (2014)
	"A city combining ICT and Web 2.0 technology with other organizational, design and planning efforts to dematerialize and speed up bureaucratic processes and help to identify new, innovative solutions to city management complexity, in order to improve sustainability and livability."	Toppeta (2010)
	"The use of information and communication technology to sense, analyze and integrate the key information of core systems in running cities."	IBM (2010)
	"A city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens."	Hall *et al.* (2000)
Integrative society development	*"A smart city brings together technology, government and society to enable the following characteristics: smart cities, a smart economy, smart mobility, a smart environment, smart people, smart living, smart governance."*	Institute of Electrical and Electronics Engineers (IEEE) (2015)
	"Smart City offers sustainability in terms of economic activities and employment opportunities to a wide section of its residents, regardless of their level of education, skills or income levels."	Indian Government (2014)

	"A city to be smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance."	Caragliu *et al.* (2011)

Although the theory of technological determinism advocates that the key force for human activities is technology, it is not the only factor of social development. Therefore, the theory of technological determinism has been criticized heavily as it over-evaluates the importance of technology (Kline, 2015). Technology applications are not regarded as an end but as a means of solving teething problems of cities. Social construction of technology responds to the purported theory of technological determinism by arguing that the true value of technology depends on the proper way by which technology is embedded in its social context. The relationship between technology and society or human activities is intertwined instead of merely exhibiting a cause-and-effect pattern, and technological development should be viewed as a complex social field (Murphie & Potts, 2003). The pervasive use of ICT alone cannot make a city smart (Hollands, 2008) because it is merely one of the important inputs for improving the planning and living of a city together with sustainability of the economy, society, and environment (Neirotti *et al.*, 2014). Therefore, the more recent definitions of SC emphasize integrative society development, referring broadly to human capital, knowledge economy, and governance within an urban environment, rather than merely managing a city on a technocratic and technological basis (Kourtit *et al.*, 2012; Kitchin, 2014).

Based on the review of the existing definitions of SC, this study proposes its own concept of SC, which emphasizes technology and social integration and suits the scope of this research. The concept is that a SC improves citizens' quality of life and social integration through the application of advanced information technologies, effective governance, and proactive solutions, which mitigate potential pitfalls.

1.1.2 Potential pitfalls of SCs

Relying on technologies alone to build SCs may cause undesirable effects that cannot be underestimated (Graham & Marvin, 2001; Caragliu et al., 2011). As stated by Edwards (2016), *"Smart cities are not a panacea for all ills, and they bring their own problems."* Information insecurity is one of the problems aggravated in SCs, where cyber-attacks, system bugs, malicious hacking, and system brittleness proliferate increasingly (Townsend, 2013). For example, with various services becoming accessible via smart mobile phones (e.g., digital map and online shopping), the number of new mobile malware variants increased by 54% from 2016 to 2017 (Symantec, 2018). From 2016 to 2017, attacks on the Internet of Things (IoT) increased by 60% (Symantec, 2018). In 2016, an average of 24,000 malicious mobile attacks were blocked per day (Symantec, 2018). Cybercrime can cost the global economy over USD375 billion to USD 575 billion per year (McAfee Inc., 2014). The consequence is not only financial losses but also digital vandalism and disruption of normal city functions. For example, a cyberattack in Haifa, Israel, caused serious traffic interruptions for eight hours (Paganini, 2013). The warning system of Dallas City was hacked in 2017. All 156 emergency sirens of the city blared for hours, causing chaos and fear among citizens.

Thousands of calls overwhelmed the 911 emergency operators. As seen in these cases, security issues occurring at the city scale may cause catastrophes, and hence, data security issues are becoming increasingly complicated and prominent in SCs.

Personal privacy leakage is another potential pitfall in SC development. More than 500,000,000 personal records were reported stolen in 2015 (Symantec, 2016). It is a staggering number, but it may not show the full picture because some companies may not report all data breaches. In SCs, end users interact directly with the IoT environment frequently. Enormous volumes of data collected by sensor networks can possibly be used to extract users' personal information and violate individuals' privacy (Price *et al.*, 2005; Pavlou, 2011). In London, a project for installing smart trash bins with sensors that recorded not only the volume of rubbish being placed but also how people use public space caused a massive uproar, as people were worried about how their personal data can be used inadvertently (Moskvitch, 2016). The digital world is projected to grow richer with 50 billion "things" being connected to the Internet by 2020, even exceeding the population worldwide (Cisco, 2015). Kitchin (2014) argued that *"the ubiquitous collection of data about all city processes may threaten to stifle rights to privacy, confidentiality, and freedom of expression."* People need to deliberate whether they are willing to trade privacy for efficiency or convenience in SCs. Meanwhile, controls over public data collection and processing are called for to ensure citizens' privacy.

The expeditious and independent development of SC and their pilot projects trigger the syndrome of information islands. This problem widely exists in the form of information/data silos and incompatibility among various smart projects and systems, including traffic management, health care, and e-government systems. Instead of enhancing efficiency, it leads to unnecessary replications of construction and waste of resources. In China, where SCs began to flourish in this decade, the bottleneck of data sharing and integration poses challenges to the healthy development of SCs. It leads to unnecessary replication of construction, and hence waste of resources. In Nanjing, for example, due to incompatible data formats and standards between metro and bus systems, the local authority incurred an additional cost of RMB100 million for the all-in-one traffic card (Li, 2010). Another case of information island can be found in Shenzhen, where the Safe City project was temporarily cancelled due to difficulty in sharing video information using incompatible surveillance systems among different districts (Li, 2010).

One more problem brought about by the development of SCs is digital divide. With the development of smart systems, an increasing number of services will be made available through smart devices and the Internet. However, some social groups without the corresponding technology skills (e.g., the elderly and people with low educational attainment) may be deprived of the benefits of the use of these services. According to the latest United Nations eGovernment Survey, digital divide permeates countries at different developmental stages; groups with different levels of income and skills and genders; and populations with different classes and abilities (United Nations, 2014). The UK, although a global leader in technology innovation, also faces digital divide

(House of Commons, 2016). In the UK, 23% of adults (12.6 million) do not have fundamental digital skills (Ipsos MORI, 2015). Approximately half these individuals are disabled, 63% are over 75 years old, and 60% are without educational qualifications. If no appropriate action is implemented, 7.9 million people worldwide will lack digital skills by 2025, as reckoned by the Centre for Economics and Business Research (2015). The gap in digital skills caused losses amounting to £63 billion a year in terms of potentially additional GDP (Koss *et al.*, 2012). To alleviate the negative impact of digital divide in the UK, the Digital Engagement Council was established in early 2016 with the digital strategy to facilitate cross-sector cooperation in closing the gap.

1.1.3 Prevailing assessments of SC performance

The use of an assessment framework helps city managers and stakeholders understand the current performance of their cities and areas that need improvement. In an imperfect world such as ours, how to avoid the pitfalls identified at the start must be emphasized. To examine whether these pitfalls have been considered carefully, seven SC performance assessment frameworks (shown in Table 1-2) were selected according to the following criteria, as proposed by Ahvenniemi *et al.* (2017): (1) the framework is for measuring city smartness; (2) it utilizes detailed indicators and methods of evaluation or ranking, and (3) it covers different domains of city functions (for example, waste management and energy). One framework was proposed by SC pioneer IBM, and another one was developed by the International Organization Standardization (ISO). Some frameworks are at national or a wide regional level, such as China, European countries, and Gulf States, whereas one is at the city level (Shanghai). A more recent scheme “CITYkeys” in EU is also included. “CITYkeys” aims at providing a comprehensive framework to fill the gaps in the existing frameworks.

The seven target frameworks possess different emphases and criteria. For instance, the Gulf States Smart Cities Index by Navigant Research (2016) emphasizes strategy (i.e., each city’s vision, goals, and objectives) and execution (actual achievements), whereas the ISO/TS 37151:2015 Smart Community Infrastructures scheme (principles and requirements for performance metrics) by International Organization for Standardization (ISO) (2015) is based on the typical needs of residents, city managers, and the environment. Despite different emphases and criteria, these systems and frameworks, taken as a whole, help in the understanding of SC from different perspectives, highlighting lessons learned from existing projects and providing proactive suggestions for future development. Table 1-2 shows the frameworks’ criteria about four pitfalls (i.e., system information insecurity, personal privacy leakage, information islands, and digital divide). As this section examines whether the four common pitfalls are considered by existing SC assessment tools, it suffices to briefly list relevant assessment criteria that are conducive to the avoidance of relevant pitfalls and the provision of positive intervention measures rather than a comprehensive analysis of each framework. As shown in Table 1-2, few assessment schemes include all four pitfalls as the assessment criteria (except ISO/TS 37151:2015 and CITYkeys). Even though several assessment schemes mention some pitfall areas, the scope of their criteria is narrow (e.g., merely using Internet accessibility and computer availability to measure digital divide).

Table 1-2 Examples of assessment framework to-date for smart city's performance

	Performance assessment document	**System insecurity**	**Privacy leakage**	**Information island**	**Digital divide**
1	Smart cities: Ranking of European medium-sized cities (Giffinger & Pichler-Milanović, 2007)	--	--	--	-International accessibility; -Computer availability in households.
2	How Smart is your city? Helping cities measure progress, IBM Institute for Business Value (Dirks *et al.*, 2009)	--	--	--	-High-speed broadband, Wi-Fi.
3	Smart city index system 1.0, Pudong New Area, Shanghai, 2012	--	--	--	-Coverage of High-speed broadband, Wi-Fi and Internet; -The level of digitalization of citizens' life; - Proportion of public propagandists for smart cities.

4	ISO/TS 37151:2015 Smart community infrastructures -- Principles and requirements for performance metrics (International Organization for Standardization (ISO), 2015)	-Internet and data security: the data and system should be protected by preventing unauthorized access and data leakage.		-Interoperability of services provided by different infrastructure.	-Service accessibility: all citizens are able to benefit from services; -Service quality: the procedure is easy for citizens to use.
5	Smart city - The evaluation model and the evaluation index systems of foundation, Part1: General framework, "GB standards", China, 2015	-Internet security management; -Monitoring, warning, emergency; -Information system control, security of critical data.	--	-The degree of public service integration; -The level of cross-departmental collaboration; -Information resource sharing and open platform establishment.	- Degree of the Convenience and efficiency of services used by citizens and industries in multiple ways.
6	CITYkeys indicators for smart city projects and smart cities (Bosch *et al.*, 2016)	- Improved cybersecurity: To assess the efforts made in the project to ensure and/or improve cybersecurity.	- Improved data privacy: To measure whether regulations on data protection are complied with and how proper	- Interoperability: To measure a system's (or a product's) capacity of working with other systems.	-Improved digital literacy: To assess the effort made to improve digital literacy, in terms of information, communication, content-

			procedures to protect personal or private data are implemented.		creation, safety and problem-solving.
7	Gulf States Smart Cities Index Assessment of Strategy and Execution for 10 Cities (Navigant Research, 2016)	--	--	-Open data policy; -Stakeholder engagement.	- Improvements in skills and education regarding the use of digital technologies; - The engagement across multiple communities.

1.2 Research aim and objectives

1.2.1 Knowledge gaps

Gap 1: Lack of systematic and empirical research on potential pitfalls of SCs.

Most previous studies regarding SCs focus on promoting system accessibility and availability and on proposing concepts and theoretical frameworks for the development of SCs. Despite increasing research on SC, systematic and empirical research on the potential pitfalls of SC development concerning technological and non-technological aspects remains lacking. Thus, identification of challenges and proposal of proactive solutions are hindered.

Gap 2: Absence of pitfall avoidance measures in the existing performance assessments for SCs.

To date, existing assessment schemes of SC development mostly focus on the positive and functional aspects of SCs but sparingly evaluate the possible downsides (Details are given in the literature review section.). A SC cannot claim to be successful by solely measuring how much it has done or what it aims to achieve if it does not feature any design against possible pitfalls. Hence, this research aims to bridge these knowledge gaps.

1.2.2 Aim and objectives

This study is aimed at identifying potential pitfalls with possible causes and adverse effects, and recommending proactive measures to help guide the implementation of SC progressively. Three research objectives have been proposed to fulfill the identified knowledge gaps. To fulfil the first gap (lack of systematic and empirical research on potential pitfalls of SCs), this research has identified (1) potential pitfalls in the development of SCs, and (2) possible causes and adverse effects of such pitfalls. To address the second gap (absence of pitfall avoidance measures in the existing performance assessments for SCs), this research provides recommendations to mitigate/prevent the associated problems, such that future assessment schemes may take them on board when evaluating the performance of SCs.

1.3 Research design

A research design refers to a detailed plan describing how the study will be conducted to realize the research objectives (Monette, 2014). Fig. 1-1 shows the steps and methods employed to fulfill the research objectives. This research mainly undergoes three phases, namely, identification of pitfalls through a comprehensive literature review; analysis of possible causes and adverse effects through a questionnaire survey and three case studies; and proposal of recommendation for better SC development based on findings obtained from the questionnaire survey and the three case studies.

Specifically, based on an extensive literature review, the research first identifies potential pitfalls in the development of SC in preparation for a questionnaire survey (questionnaire survey #1) to gain a general understanding of pitfalls in SC development. Questionnaire survey #1 targets experts in the SC domain. Its content covers the rating of possible causes, adverse effects, and mitigation measures of each pitfall in terms of its likelihood, severity, and effectiveness. Then, four common pitfalls are identified and studied within the context of several Hong Kong SC projects. The first case study is a questionnaire survey (questionnaire survey #2) meant to investigate how users perceive these pitfalls within the context of mobile apps that provide real-time parking information. Several interviews are conducted in Hong Kong, with (1) stakeholders participating in smart parking projects (interview group #1) to determine why only a few carpark operators are willing to provide their real-time vacancy information to the government's platform; and (2) disadvantaged groups and organizations helping the disabled (interview group #2) to find out the rationale behind the digital divide and possible solutions. The second case study looks into the pitfall of system information insecurity by analyzing the reliability of smart parking information systems. Through the use of fuzzy fault tree analysis (FFTA), this work investigates the possible mechanisms of service non-availability and relative importance of events causing service non-availability. The third case study uses social network analysis (SNA) to investigate the interrelationships of barriers faced by different stakeholders involved in the project of open data, which is key to bridging information islands in emerging SCs. In the end, the feasibility and effectiveness of obtained recommendations for emerging SCs are validated by independent experts in Hong Kong.

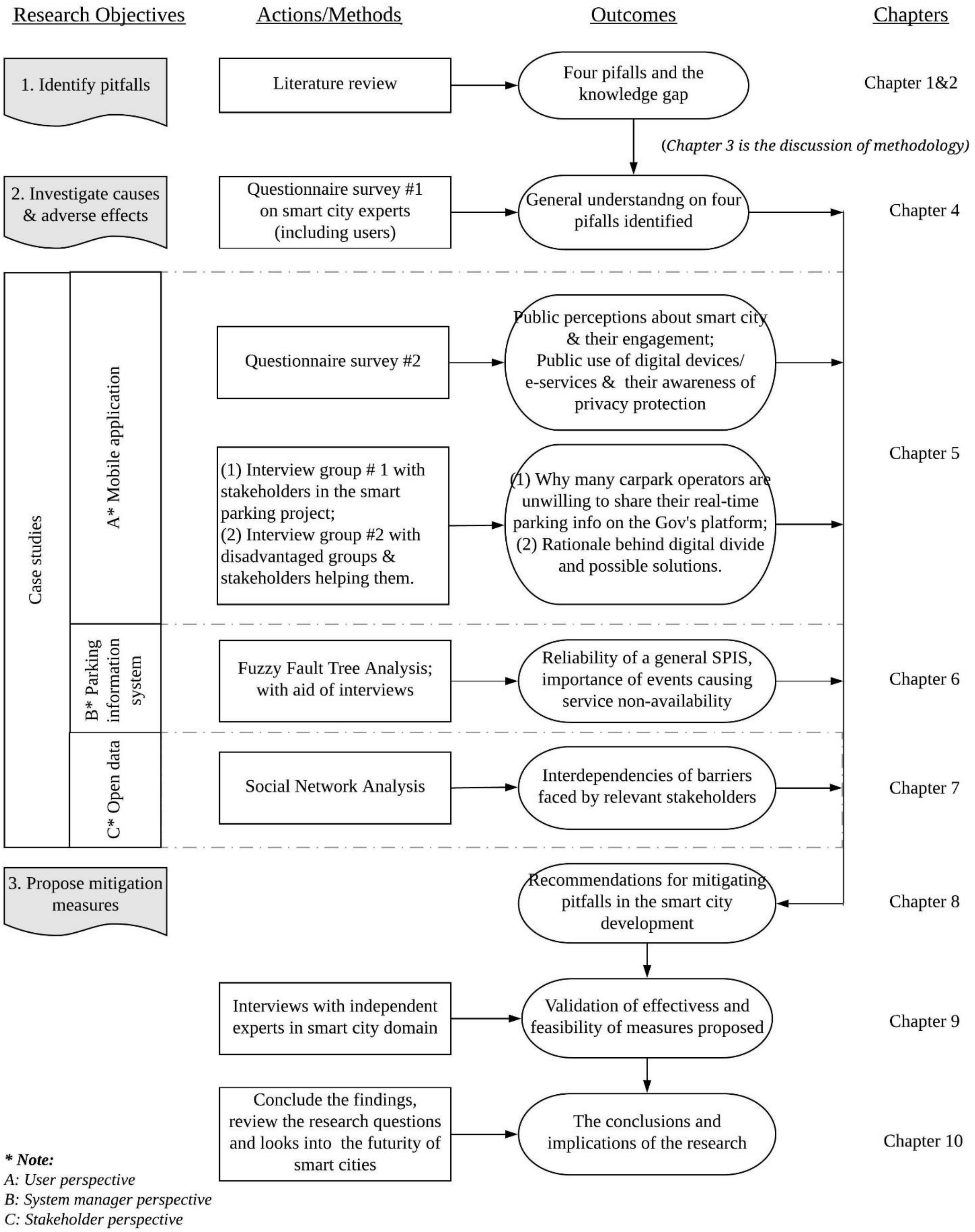

Research Objectives
Actions/Methods
Outcomes
Chapters
1. Identify pitfalls
Literature review
Four pifalls and the knowledge gap
Chapter 1&2
(Chapter 3 is the discussion of methodology)
2. Investigate causes & adverse effects
Questionnaire survey #1 on smart city experts (including users)
General understandng on four pifalls identified
Chapter 4
Case studies
A* Mobile application
Questionnaire survey #2
Public perceptions about smart city & their engagement; Public use of digital devices/ e-services & their awareness of privacy protection
(1) Interview group # 1 with stakeholders in the smart parking project; (2) Interview group #2 with disadvantaged groups & stakeholders helping them.
(1) Why many carpark operators are unwilling to share their real-time parking info on the Gov's platform; (2) Rationale behind digital divide and possible solutions.
Chapter 5
B* Parking information system
Fuzzy Fault Tree Analysis; with aid of interviews
Reliability of a general SPIS, importance of events causing service non-availability
Chapter 6
C* Open data
Social Network Analysis
Interdependencies of barriers faced by relevant stakeholders
Chapter 7
3. Propose mitigation measures
Recommendations for mitigating pitfalls in the smart city development
Chapter 8
Interviews with independent experts in smart city domain
Validation of effectivess and feasibility of measures proposed
Chapter 9
Conclude the findings, review the research questions and looks into the futurity of smart cities
The conclusions and implications of the research
Chapter 10
* Note:
A: User perspective
B: System manager perspective
C: Stakeholder perspective

Figure 1-1. Research roadmap

1.4 Structure of the thesis

This thesis contains ten chapters. Figure 1-1 shows the relationship and flow between these chapters. Chapter 1 presents the aim and objectives of the research after introducing the research background and knowledge gaps identified. It ends by outlining the research roadmap and thesis structure. Chapter 2 is a comprehensive literature review on the potential pitfalls of SCs. It introduces the evolution of the definition of SC and the current trend of related studies. Then previous research on four pitfalls (i.e., system information insecurity, personal privacy leakage, information islands, and digital divide) is reviewed to identify knowledge gaps. Chapter 3 presents a discussion on the methods used in the research (semi-structured interviews, questionnaire surveys, case studies, FFTA, and SNA) and how they are structured to achieve the research objectives. Chapter 4 presents the data analysis of questionnaire survey #1 from the SC experts. Chapters 5, 6, and 7 explain the case studies, namely, public use of mobile applications and perception about pitfalls identified; a reliability analysis of a smart parking information system; and SNA of stakeholder-related barriers in open data development. Chapter 8 summarizes the recommendations for mitigating pitfalls in SC development. In Chapter 9, the feasibility and effectiveness of targeted recommendations for emerging SCs are validated by independent experts in Hong Kong. Chapter 10 finally draws conclusions from the key findings, states the contributions and limitations of this research, and proposes suggestions for future research.

1.5 Summary

This chapter presents an overall picture of this study. It first introduces the background of SCs by showing its evolving definitions and by reporting pitfalls which happen worldwide. Then, the research aim and objectives of this study are proposed to address current knowledge gaps. The research roadmap and thesis structure show the holistic process by which research questions are identified and resolved. The next chapter presents an extensive literature review on the potential pitfalls of SCs.

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

A literature review is a summary of current knowledge on a research topic, including important findings and theoretical and methodological contributions to a specific topic. *"All research needs to be informed by existing knowledge in a subject area"* (Rowley & Slack, 2004). As a collection of existing knowledge, a literature review not only helps in understanding the current progress but also suggests possible areas for further research. The objectives of this literature review are to identify common pitfalls brought about by SCs and to review existing literature on each pitfall. The literature review draws on a variety of sources, including journal papers, conference proceedings, books, government and industry reports, standard documents, and newsletters. The first part of this chapter is the content analysis of a collection of appropriate literature for the purpose of identifying pitfalls. The following parts review existing studies on the identified pitfalls for an investigation of their possible causes, adverse effects, and possible solutions. Finally, findings from the literature review are summarized. Part of the literature review is acknowledged to be extracted from a publication with the candidate as the first author[1], as well as another accepted manuscript[2] (with the

[1] Ma, R., Lam, P. T., & Leung, C. K. (2018). Potential pitfalls of smart city development: A study on parking mobile applications (apps) in Hong Kong. *Telematics and Informatics*, 35(6), 1580-1592.

[2] Lam, P. T., & Ma, R*. (2018). Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study. *Cities*, https://doi.org/10.1016/j.cities.2018.11.014 (accepted on 16 Nov 2018).

candidate as the corresponding author).

2.2 Identifying pitfalls of SCs

To identify common pitfalls of SCs, a comprehensive search was performed mainly on peer-reviewed journal papers in English published from 2000 up to present. *Web of Science* was searched with "smart city" as the topic and title to retrieve relevant literature from SCI and SSCI databases. In view of the multidisciplinary nature of SCs and of the objective of identifying general pitfalls existing in SCs, papers focusing on specific technical domains, such as telecommunication, chemistry, physics, computer software engineering, forestry, and electronic engineering, were excluded. Highly cited papers were extracted from areas such as urban studies, management, public administration, planning development, and social sciences interdisciplinary. Similar steps were followed in searching *ScienceDirect* and *Google Scholar* to add suitable yet less-cited papers (as they were only lately published). In total, 88 papers were initially identified. Most of them were published 2011 onward, as shown in Figure 2-1. The last step was a content analysis of these papers for identification of the common pitfalls brought about by SC.

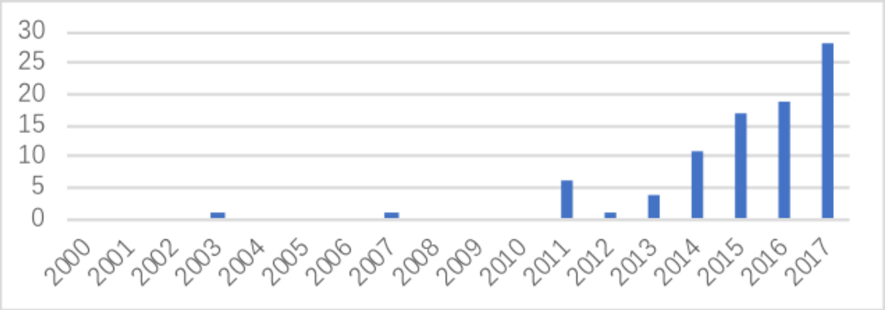


Figure 2-1 Eighty-eight journal articles gained by initial search

Twenty-one articles published in quality journals (e.g., *Cities*, *GeoJournal*, *International Journal of Information Management*, *Technological Forecasting*, and *Social Change*) and a popular journalistic work on SC by Townsend (2013) were used to identify four common pitfalls, namely, system information insecurity, privacy leakage, information islands, and digital divide. The mention of these pitfalls by the chosen papers is shown in Table 2-1. The identified pitfalls include technical and social issues in SCs. This framework echoes the suggestion of considering technical and societal components for the development of SCs (Caragliu *et al.*, 2011; Nam & Pardo, 2011). Some of the pitfalls identified appear to already exist, albeit not as frequently and seriously as when multiple technologies are fully operated in established SCs.

Table 2-1 Key studies of SC highlighting the preponderance of the four pitfalls

Key publications on SC	System information insecurity	Privacy leakage	Information islands	Digital divide
(Hollands, 2008)	-	-	-	√
(Caragliu *et al.*, 2011)	-	-	-	√
(Allwinkle & Cruickshank, 2011)	-	√	√	-
(Chourabi *et al.*, 2012)	√	√	√	√
(Batty *et al.*, 2012)	√	√	√	√
(Townsend, 2013)	√	√	-	-
(Batty, 2013)	-	√	-	-
(Galdon-Clavell, 2013)	-	√	√	-
(Lee *et al.*, 2014)	-	-	√	-
(Viitanen & Kingston, 2014)	-	√	√	√
(Yigitcanlar & Lee, 2014)	-	√	√	√
(Kitchin, 2014)	√	√	-	-
(Neirotti *et al.*, 2014)	√	-	-	√

(Angelidou, 2014)	√	√	√	√
(Walravens, 2015)	-	√	√	√
(Calzada & Cobo, 2015)	-	-	-	√
(Albino *et al.*, 2015)	-	-	√	√
(Hashem *et al.*, 2016)	√	√	√	-
(Vanolo, 2016)	√	√	-	√
(Cassandras, 2016)	√	√	√	-
(Anthopoulos, 2017)	√	-	-	√
(Colding & Barthel, 2017)	√	-	-	√

Furthermore, these four common pitfalls have been corroborated currently by Boorsma (2017), book author of *A New Digital Deal* and the North European Director of a global IT corporation. Based on lessons learned from his 15-year practice in the domain of SC development, Boorsma (2017) summarized 12 pitfalls using a hierarchy and categories different from those in this literature review. However, eight of Boorsma's pitfalls can be subsumed under the categorization of this study by their nature, as shown in Table 2-2. For instance, "Legacy IT infrastructure" with vulnerability and limited capacity is regarded as a cause of system information insecurity (Cerrudo, 2015) and information islands (Huijboom & Van den Broek, 2011; Janssen *et al.*, 2012). "Dichotomy of top-down and bottom-up approach" may aggravate the digital divide by ignoring the importance of public participation and users' true demands. As the focus of this study is to investigate the pitfalls brought about by SC development rather than to establish appropriate objectives of SC development, all pitfalls within Boorsma's "unclear objectives and myopia" are considered to be out of the scope of this study due to subjectivity. In an early work, Boorsma (2016) also emphasized the urgency of dealing with two other pitfalls: improving information security, given that 2.5 million cyber security threats need to be resolved per second worldwide, and addressing the problem of personal information leakage before the benefits of big data can be reaped.

Table 2-2 The 12 pitfalls of SC efforts by Boorsma (2017)

(left hand column added by the author)

1. Information islands	(1) "Over reliance on public sector" (2) "Organization silos" (3) "Legacy IT infrastructure" (4) "Scattered pilots without plan to scale" (5) "Closed architecture"
2. Digital divide	(6) "Digital divides" (7) "Large cities' lock-ins excluding smaller communities" (8) "Dichotomy of Top-Down and Bottom-Up approach"
3. Unclear objectives and myopia (regarded as subjective comments; hence out of the scope of this study)	(9) "Confusion brought by the too broad definition of SC" (10) "Ending up as technology demonstrations" (11) "Solutions becoming the objective rather than a means" (12) "Unclear objectives"

In the following sections, each pitfall is analyzed for an examination of their possible causes, adverse effects, and mitigation measures.

2.3 System information insecurity

The requirements of ensuring information security basically revolve around three factors: confidentiality, integrity, and availability (CIA for short) (Elmaghraby & Losavio, 2014). Confidentiality is prevention of leakage of information to unauthorised users. This is closely related to privacy and is achieved by applying encryption or preventing unauthorized access to specific data. Integrity means the guaranteed trustworthiness of data and settings. Availability indicates the correct performance/functions of a system for the desired purpose. The challenge of securing an SC lies in its inherent interconnection of intelligent objects such as smartphones, IoT, and service platforms (Braun et al., 2018). Vulnerabilities of any object will risk the overall security landscape of an SC. Cyber-attacks, such as protocol attacks and denial-of-service (DoS) attacks, can target every component or network communication in an SC. In particular, supervisory control and data acquisition systems for monitoring various urban infrastructure, sensors, and controllers of IoTs; radio-frequency identification tags; and communication networks are prone to such attacks (Kitchin, 2016). Smart software that maintains a persistent connection between devices and a city-wide network (Mahmoud & Ahmad, 2009) can also be hacked to trigger system-wide failures and malfunctions and then breach the integrity of exchanged information and confidentiality of users' information (McClure *et al.*, 2001). Despite rampant cybercrimes, people often regard security as an afterthought rather than a priority (HP Inc., 2014; Cerrudo, 2015; Kitchin, 2016). According to a study, 70% of common IoT devices are fragile in terms of password security, encryption, and user access control (HP Inc., 2014). Globally, approximately 200,000 traffic controllers in use are vulnerable to cyber-attacks. For example, data originating from traffic sensors in San Francisco remained unencrypted even after one year of installation (Cerrudo, 2015). In this case, the products themselves were not inherently vulnerable; rather, the vendors had insufficient security awareness, given that components produced according to accepted industry standards do not provide adequate security (Ghena *et al.*, 2014). Additionally, errors in design can exacerbate security problems. In November 2014, a power supply failure resulting from a design error caused trading at the Singapore Stock Exchange to come to a standstill for nearly three hours (Mah, 2015).

Table 2-3 Causes, effects and mitigation measures against information insecurity

Possible causes
Weak security and encryption, security being an after-thought (HP Inc., 2014; Cerrudo, 2015; Kitchin, 2016).
Cyber-attacks (Markey & Waxman, 2013; Townsend, 2013; Cerrudo, 2015).
Large and interdependent systems with many stakeholders involved, making it difficult to ensure end-to-end security (Kitchin, 2016).
Errors in design (Mah, 2015).
Poor management and operation models of outsourcing products and services (Cordella & Willcocks, 2010; Berghmans & Van Roy, 2011; Ghena *et al.*, 2014).
Limited security sponsorship and management support in the development of smart systems (Cloud Security Alliance, 2016).
Using insecure legacy systems and poor maintenance (Cerrudo, 2015; Kitchin, 2016).
Human errors and negligent staff (Finney, 2014; Cerrudo, 2015; Kitchin, 2016).
Adverse effects
A system-wide failure and non-availability of essential services (McClure *et al.*, 2001; Finney, 2014; Haughn & Gibilisco, 2014).
Breaching the confidentiality of users' information (Ferraz & Ferraz, 2014).
Economic loss (Mok, 2014; Yadron, 2016).
Mitigation measures
Management controls over operation and design (Scarfone, 2009).
General technical countermeasures such as frequent backup, anti-virus programs, software updates, firewalls against intruders (Rodosek & Golling, 2013; Lewis, 2015).
Employing/developing well-defined standards for developing and managing ICT services (Lyytinen & King, 2006; Khatoun & Zeadally, 2017).
Improving security awareness and availability safeguards, conducting continuous vulnerability assessment (Symantec, 2016).
Developing a cyber-security strategy and recovery plan (Symantec, 2016).

Table 2-3 summarizes the possible causes and adverse effects of information security and the proposed mitigation measures against them. Although numerous studies have looked into information security of individual technologies, such as sensors (Chan & Perrig, 2003; Gungor *et al.*, 2010), IoT (Zhang *et al.*, 2011), cloud computing (Okuhara *et al.*, 2010), and software (Sen *et al.*, 2013), systematic research on information security involving the technological and management issues of an application in an urban scenario is still lacking. In a SC, where various systems are interconnected and perform different roles collaboratively, concerns about information security need to go beyond individual subjects. Within the scope of SCs, information security is still in its initial phases of research (Ferraz & Ferraz, 2014). The problem of data insecurity on smart systems appears to remain unsolved unless a holistic approach is implemented by concerned stakeholders, including city managers, system providers, and system users.

2.4 Privacy leakage

Personal information refers to *"any recorded information about an identifiable individual"* (Cavoukian *et al.*, 2010), including a person's name, location, contact details, transactional history, and social network. Personal information can be easily intruded due to the intensive application of ICTs that are collecting and processing data in SCs (Price *et al.*, 2005; Pavlou, 2011; Markey & Waxman, 2013). Typical scenarios of individual privacy intrusion include information tracking (during the exchange process), which destroys the anonymity of information origin, and unauthorized citizen tracking, which may disclose involved personal identities (Ferraz & Ferraz, 2014). Some convenient services, such as free Wi-Fi, may enable access to users' profile during connection because open networks without encryption make all data traffic visible to any deliberate eavesdropper physically nearby (Porta, 2018). Concurrently, Wi-Fi access points with the aid of video cameras in some retail stores can monitor customers' movement and purchase behaviors by following Wi-Fi signals from customers' smartphones even when they do not connect to the network (Clifford & Hardy, 2013). In addition, data over-collection was identified by a study as a severe hazard in SCs with mobile applications that collect more user data than its original function while within permission scope (Li et al., 2016). Though some service providers claim to safely keep data contained, these practices are still problematic as they usually do not obtain people's consent first. Citizens living in SCs should feel secure enough; otherwise, they will lose interest, and SCs will be obsolete (Braun et al., 2018).

Some scholars have argued for strengthened protection of citizens' privacy in SCs, especially in terms of sensitive information about their identity, location, energy consumption, and possessions (Martínez-Ballesté *et al.*, 2013). SCs cannot rely on traditional privacy protection approaches to withstand data mashing and over-collection (Braun et al., 2018). Technical studies have already focused on solutions such as cloud computing (Khan *et al.*, 2014) and other privacy enhancing technologies (Rebollo-Monedero *et al.*, 2014). Policy makers use privacy impact assessments as a tool for examining the privacy risk of specific technologies or applications and analyzing mitigation measures (Wright & De Hert, 2012). However, reliance on specific technical solutions is not enough to address users' privacy concerns (Van Zoonen, 2016). Passive approaches cannot be competent enough for data protection (Li et al., 2016). Table 2-4 summarizes the possible causes and adverse effects of personal information leakage and proposed mitigation measures against it from the policy perspective.

Table 2-4 Causes, effects and mitigation measures against personal information leakage

Possible causes
Heterogeneity and ubiquity of IoT-enabled system without providing notice and seeking consents of targets (Chan & Perrig, 2003; Kitchin, 2016; Rahman *et al.*, 2016).
Unauthorized access to systems (Ferraz & Ferraz, 2014).
Insufficient awareness and knowledge on data protection of users (Kitchin, 2016).
Absence of strict standards/regulations to protect personal information (Chatzigiannakis *et al.*, 2016; Meola, 2016).
Adverse effects
Information exposure, citizen tracking and even impersonation (Martínez-Ballesté *et al.*, 2013; Ferraz & Ferraz, 2014).
Risking public trust towards the society and posing threat to democracy (Poole, 2014).
Economic loss (Symantec, 2016).
Mitigation measures
Establishing standards on how public data could be collected and used (ARUP and RIBA, 2013).
Utilizing education and training to help improve users' knowledge and awareness of information privacy; and informing developers their responsibilities and best exercises (Kitchin, 2016).
Legislation to allow users to control their own data and create a regulatory environment (Kozlov *et al.*, 2012; Edwards, 2016).
Employing Privacy by Design (PbD) (European Union Agency for Network and Information Security (ENISA), 2014; Edwards, 2016; Kitchin, 2016).
Conducting Privacy Impact Assessments (PIA) (Edwards, 2016).

2.5 Information islands

Information islands or information silos denote information systems that are isolated and incompatible mutually. This problem persists in the form of information/data isolation and incompatibility among various systems, organizations, and departments. This phenomenon can result from technological and non-technological factors. A European study of SCs stated that information islands result from a “lack of universal open or proprietary standards for exchange of data” (Edwards, 2016). Other causes lie in the difficulty of integrating data from legacy systems, insufficiency of cooperation, and imbalance between the interests of different sectors. A significant cause that deserves considerable attention at an early stage is the difficulty of engaging with various stakeholders, which include users, technical consultants, public and private data providers, and research institutes (Yanrong & Whyte, 2014). This factor obstructs the ongoing development of city-wide open data platforms, which are key to resolving information islands. Open data refers to “*data that can be freely used, re-used, and redistributed by anyone for any purpose*” (Open Knowledge International, 2015). It enables wide data integration, especially data redevelopment. However, its adoption has encountered various barriers in terms of legislation, technology, operation, and use (Janssen *et al.*, 2012; Barry & Bannister, 2014). This area, especially underlying processes pertaining to these barriers, deserve additional attention. Information islands negatively affect SC development through such problems as redundant construction, resources waste, and inconvenience for residents (Zou & Wang, 2008). This phenomenon reduces the efficiency of SC development and the benefits that residents could enjoy.

Table 2-5 Causes, effects and mitigation measures of information islands

Possible causes
Incompatible data standards and formats (Masip-Bruin *et al.*, 2013; Agudelo & Barrera, 2014).
Difficulty of engaging with a broad spectrum of stakeholders (Yanrong & Whyte, 2014).
Insufficient cooperation and communications among stakeholders (Odendaal, 2003; Johnston & Hansen, 2011).
Independent development and non-integrated planning of IT application systems (Yanrong & Whyte, 2014).
Closed government culture and risk-averse policy (Huijboom & Van den Broek, 2011; Janssen *et al.*, 2012; Conradie & Choenni, 2014).
Adverse effects
Replicated facilities, resources wasting and overlapping investment (Zou & Wang, 2008; Yanrong & Whyte, 2014).
Reducing the efficiency of smart cities (Li, 2010).
Causing inconvenience in residents' life (Li, 2010).
Mitigation measures
Sharing interoperable protocols among tech suppliers (Edwards, 2016).
Formulating open standards and improving data quality (Masip-Bruin *et al.*, 2013; Yanrong & Whyte, 2014).
Promoting cross-sectional collaboration among different interfacing organizations (Harris & Baumann, 2015).
Planning the process of systems and data integration at the design stage (Yanrong & Whyte, 2014).

Table 2-5 above summarizes the possible causes and adverse effects of information islands and the proposed mitigation measures. Several scholars have suggested sharing interoperable protocols among technology suppliers (Edwards, 2016); formulating inclusive and open standards for applications and technologies, such as application programming interfaces (Yanrong & Whyte, 2014); and redeveloping data for value-added use via open platforms (Masip-Bruin *et al.*, 2013; Colmenar *et al.*, 2014). Other issues, such as data selection, data heterogeneity, data security, data quality, and data processing also need to be considered (Masip-Bruin *et al.*, 2013). Given that information islands are a management and planning problem rather than a technological concern, employing cross-departmental governance has been highlighted for guaranteeing collaboration among different stakeholders (Yanrong & Whyte, 2014).

2.6 Digital divide

Numerous studies about digital divide problems have been published since the 1990s (Zhao *et al.*, 2014). "Digital divide" initially denoted unequal accessibility to digital equipment and information technologies among various groups (Gunkel, 2003). Initially, it was observed as a binary difference between those who had Internet connection and those who did not (Riggins & Dewan, 2005). However, with the penetration of the Internet and digital devices increasing in most developed countries, the relevance of a digital divide in terms of physical access has started to diminish. Hargittai (2001) suggested distinguishing an "Internet access divide" from "skills divide" (second-level digital divide), with the latter indicating capability gaps in using the Internet and digital devices. The concept of digital divide kept evolving. It went beyond physical accessibility to focus on the skills needed in using technologies and then even the outcome of Internet use as the third-level digital divide (Van Dijk, 2005). Therefore, digital divide also emerges when digital skills and Internet use do not produce benefits for all citizens (Van Deursen et al., 2016).

Digital divide widens the existing social gap (Van Dijk, 2005; Witte & Mannon, 2010). The multifaceted nature of digital divide indicates that what matters most is the manner of using ICT to bring about positive socio-economic effects for citizens rather than merely owning a computer (Welsh Government Social Research, 2011). Countermeasures are needed to prevent the continuous widening of the digital divide. Otherwise, skilled people can utilize ICTs to improve their quality of life, whereas the less-skilled will struggle to adapt to the trend of SCs (Van Deursen & Van Dijk, 2009). Most works on digital divide depict social exclusion based on demographic characteristics (Van Dijk & Hacker, 2003; Van Dijk, 2006, 2012), finding that Internet/device access and digital skills/use can be influenced by gender, age, education level, and geography. According to Scheerder et al. (2017), factors other than demographic characteristics, including social and cultural determinants (e.g., digital support and cultural capital), demand attention because they can be regarded as prerequisites for benefitting from the use of the Internet and digital devices by the society as a whole. Qualitative methodology, such as interviews, can be used to obtain extensive understanding and explanations on the support demanded most by Internet users and how to make Internet users benefit more (Scheerder *et al.*, 2017).

Based on the literature review, Table 2-6 summarizes the possible causes and adverse effects of digital divide and proposes mitigation measures against them. Existing studies on the use of computers and smartphones lay the foundation for ongoing research on SCs. However, the digital divide varies among different services and devices (Thomas & Streib, 2003) due to different motivations, purposes, and required skills (Bélanger & Carter, 2009). Factors affecting their use may not be the same either (Masip-Bruin *et al.*, 2013; Zhao *et al.*, 2014). Therefore, a contextual study of the digital divide is needed to fill this gap.

Table 2-6 Causes, effects and mitigation measures of digital divide

Possible causes
Insufficient provisions of physical access to Internet and digital services (Cullen, 2001; Bélanger & Carter, 2009).
Computer ill-literacy and lack of skills (Cullen, 2001; Bélanger & Carter, 2009; International Telecommunication Union, 2011).
Poor quality of services (Cuervo & Menéndez, 2006).
Personal attitude barriers and weak information awareness of citizens (Botha *et al.*, 2001; Andreasson & Jian, 2015).
Lack of special care for disadvantaged groups (Van Dijk & Hacker, 2003; Van Dijk, 2006).
Lack of training programs for unskilled citizens (Cullen, 2001; Fuchs, 2009).
Insufficient engagement initiatives from the society (Cheang & Lei, 2015).
Adverse effects
Widening social and economic inequality (Reffat, 2003; Welsh Government Social Research, 2011).
Reducing the effectiveness of smart cities (Van Deursen & Van Dijk, 2009).
Mitigation measures
Increasing network coverage and the penetration of digital devices (Cullen, 2001; Chang & Yang, 2010; Andreasson & Jian, 2015).
Providing financial support for computer acquisition/Internet access (Botha *et al.*, 2001; Cullen, 2001), and decreasing telecommunications charges (Andreasson & Jian, 2015).
Providing education and training, facilitate social learning to the public (Cairney & Speak, 2000; Chang & Yang, 2010; Andreasson & Jian, 2015).
Improving public services for disadvantaged groups and enhancing their information literacy (Andreasson & Jian, 2015).
Motivating digital inclusion initiatives of both citizens and private sectors (Cheang & Lei, 2015).

2.7 Summary

This study presents a comprehensive literature review on the possible pitfalls of SCs worldwide, including system information insecurity, personal privacy leakage, information islands, and digital divide. Despite the increasing number of studies on SCs, systematic and empirical research on the pitfalls of SC development concerning technological and non-technological aspects is still lacking. Thus, efforts to aid the government and city managers in understanding relevant challenges, avoiding potential problems, seeking improvement measures, and even setting assessment standards are hampered. This literature review serves as a foundation and underlying framework for conducting further research.

CHAPTER 3 METHODOLOGY

3.1 Introduction

The previous chapter identified four pitfalls, including their possible causes, adverse effects, and mitigation measures based on a comprehensive review of literature. This chapter mainly discusses the methods used to accomplish the research objectives. This chapter focuses on "how" these methods fit the purpose of the study. The process of collecting and analyzing data includes qualitative and quantitative methods, such as questionnaire surveys, case studies, semi-structured interviews, fuzzy fault tree analysis (FFTA), and social network analysis (SNA). Statistical techniques, such as mean score (MS) ranking, and tests, such as Cronbach's alpha, Kendall's W, Chi-square (test of independence), and Spearman's rank correlation are used to analyze the survey data.

3.2 Questionnaire survey

The questionnaire is one of the principal research instruments used to collect information in a standardized format from a group of respondents in social science. The questionnaire enables data collection with a sampling frame within a defined period of time and allows respondents to complete it at their convenience. A questionnaire has two general formats, namely, close-ended questions that are used to collect responses in a pre-designed format (typically from given multiple choices) and open-ended questions that are adopted to collect unstructured statement based on the free will and experience of the respondents. Close-ended questions can generate statistical results for analysis, which fit the purpose of this study. A small number of open-ended questions are incorporated to allow respondents to comment and provide them with opportunities to discuss issues that were missed by the close-ended questions.

A total of three questionnaire surveys were planned for this study. The first one was developed based on the literature review. This questionnaire was administered to allow the respondents to rank the following items: (1) the occurrence likelihood (OL) and severity (SE) of the possible causes of pitfalls; (2) severity of adverse effects; and (3) effectiveness of mitigating measures identified from the literature review. The purpose of ranking is to understand the four pitfalls and lay a foundation for making recommendations. Experts with rich experiences in SC projects were selected from government, industry, and academic/research institutions. The questionnaire is attached in Appendix 1, which is entitled Survey Questionnaire: *A study of the potential pitfalls in the development of smart cities.*

The Delphi method was considered in the selection of research methods to gain reliable rankings. However, this method was eventually discarded. A series of “ranking-type” Delphi surveys was proven useful in producing a rank-order list of factors based on group consensus (Schmidt *et al.*, 2001), but it required rapport with experts. This method is suitable for studying complicated issues that are highly uncertain, controversial, and speculative (Okoli & Pawlowski, 2004). Other research methods, such as panel discussions, focus group meetings, and workshops, were also considered to obtain a general understanding of the pitfalls in the development of SCs. However, these methods were considered suitable for collecting data and insights that are only accessible through interactions and engagements among a specific group of people (Lindlof & Taylor, 2010), or for studying the diversity of opinions in an open-ended topic. Conversely, questionnaire surveys and semi-structured interviews were considerably efficient and useful for gaining firsthand data across a wide range of stakeholders involved with SC development, whereas the issues that require responses are focused and specific in nature. The second questionnaire survey was targeted at users of a mobile parking application. The survey collected data on: (1) citizens' expectations on mobile apps that disseminate information of real-time parking vacancies; (2) citizens' use of information or digital services; and (3) their understanding of SC. A pool of drivers who reside across Hong Kong were invited to answer the Survey Questionnaire (English Version): *Mobile Application for Finding Parking Vacancy* (Appendix 2). A Chinese version of the questionnaire was also prepared to facilitate respondents in the Hong Kong community, where Chinese is mainly used. This survey forms part of the three case studies. Chapter 5 will discuss the first case study in detail.

3.3 Case study

Case study is a useful approach to examine a complex and unique phenomenon in terms of the "why" and "how" aspects, particularly when the subject phenomenon needs to be examined under certain contextual conditions (Yin, 2009; Thomas, 2011). The case study method is considered suitable and useful because the current research aims to explore "how" SC projects are carried out in Hong Kong based on its background. The method is used to investigate if and how the four pitfalls, namely, system information insecurity, personal privacy leakage, information islands, and digital divide, exist within the context of specific projects/systems. At the beginning of this research (Section 1.1.1), a definition of SC concerning both technology and its management has been proposed. Based on that definition, projects for which ICTs are used to improve the performance of public services and citizens' quality of life are considered as SC projects for the purpose of discussion in this thesis. The following three case studies were therefore conducted: (1) an investigation of users' perception about SCs and the use of mobile applications/digital services; (2) a reliability analysis of smart parking information system (SPIS); and (3) the interrelationships of barriers faced by stakeholders in an ongoing open data project. Smart parking and open data applications have become fostered in the ongoing SC development of Hong Kong. The use of real-time parking information may improve drivers' efficiency of finding parking spaces as well as alleviate traffic congestion. The release of open data improves government transparency, motivates citizens' participation, and unlocks enterprises' innovations. Therefore, these cases can be regarded as SC projects in this research. To achieve the objectives of this research, the identified pitfalls will be analyzed within the context of specific projects/systems so as to investigate if effective governance and proactive solutions have been incorporated in SC projects.

3.4 Data analysis techniques used in questionnaire surveys

Various techniques, such as MS ranking and tests, such as Cronbach's alpha, Kendall's W, chi-square test of independence, and Spearman's rank correlation, will be used to analyze the data obtained through the questionnaire surveys.

3.4.1 Mean score (MS) Ranking

MS was employed to measure the relative importance (ranking) of various items under the identified causes, effects, and mitigation measures of each pitfall. A five-point Likert scale will be used to calculate the MS of each item using Statistical Package for Social Sciences (SPSS). The following formula will be used to compute MS:

$$\text{Mean Score} = \frac{\sum(f\ x\ s)}{\text{N}}\ (1 \leq \text{MS} \leq 5). \qquad \text{(Eq.3-1)}$$

Where N = Total number of respondents concerning that factor;

f = Frequency count of each rating (1-5) for each factor;

s = Score given to each factor by the respondents, ranging from 1 to 5.

The meaning of 1 to 5 in the survey on the pitfalls of smart cities:

For OL of the causes: 1= “Very low”, 5 = “Very high”.

For SE of a cause if it occurs: 1 = “Very low”, 5 = “Very high”.

For SE of the adverse effects: 1 = “Very low”, 5 = “Very high”.

For effectiveness of mitigation measures: 1= “Least effective”, 5= “Most effective”.

A “don’t know” choice will be provided in case of ignorance to avoid distortion in the results.

3.4.2 Cronbach’s alpha test

This type of test is applied to evaluate the internal consistency and reliability of questionnaire responses (Santos, 1999). The values of alpha coefficients range from 0 to 1, that is, the higher the value, the more reliable the generated scale (Santos, 1999). On the basis of previous research, Nunnally (1978) recommended 0.6 as the acceptable reliability coefficient for non-validated items; Tuckman and Harper (2012) and Robin and Poon (2009) suggested a score of 0.5 for attitude/perception assessment. In this research, Cronbach's alpha test will be used to assess internal consistency among the responses (hence, reflecting upon the questionnaire design) under the adopted Likert scale of measurement regarding the occurrence likelihood (OL) and severity (SE) of pitfalls in SCs and effectiveness of the countermeasures. The following formula will be used to compute Cronbach's alpha (Lavrakas, 2008):

$$\alpha = \frac{n}{\mathrm{n}-1}\left(1 - \frac{\sum V_i}{V_{test}}\right). \qquad \text{(Eq.3-2)}$$

Where n = number of questions;

V_i = variance of scores on each question; and

V_{test} = total variance of overall scores on the entire test.

3.4.3 Kendall’s W-test

Kendall’s coefficient of concordance *W* is used to measure the degree of agreement and consistency of responses within a certain group of related sub-questions. The values for *W* range from 0 (perfect disagreement) to 1 (complete agreement) (Daniel, 1978). A high value of *W* at a predefined significance level indicates a justifiable degree of association among the respondents on the sub-questions (Siegel & Castellan, 1956). The value of Kendall’s coefficient of concordance *W* for each attribute can be computed by the following formula (Siegel & Castellan, 1956):

$$W = \frac{\sum_{i=1}^{n}(\overline{Ri} - \bar{R})^2}{\mathrm{n}(n^2-1)/12}. \qquad \text{(Eq.3-3)}$$

Where n = Number of number of sub-questions in a group;

$\overline{Ri}$ = Average of the ranks assigned the ith attribute; and

$\bar{R}$ = Average of the ranks assigned across all attributes.

Kendall's W test is only applicable when the number of sub-questions in any section is less than or equal to seven. The chi-Square test will be used if the number of sub-questions exceeds seven (Siegel & Castellan, 1956).

3.4.4 Chi-Square test of independence

The chi-square test for association (denoted by χ^2) was deployed to test whether any dependence existed between two categorical variables. Null hypothesis (H_0): *an association between the two categorical variables is missing*. Alternative hypothesis (H_α): *an association exists between the two categorical variables*. χ^2 is computed as follows:

$$\chi^2 = \sum_{i=1}^{R}\sum_{j=1}^{C}\frac{(O_{ij}-E_{ij})^2}{E_{ij}}. \qquad \text{(Eq.3-4)}$$

Where R is the number of rows in the table (number of items under categorical variable A) and C is the number of columns (number of items under categorical variable B). O_{ij} and E_{ij} are respectively the observed and expected cell count in the ith row and jth column of the table. E_{ij} can be calculated as:

$$E_{ij} = \frac{\text{row i total} * \text{column j total}}{\text{total grand}}. \qquad \text{(Eq.3-5)}$$

The obtained χ^2 value is compared with the critical value from the χ^2 distribution table with degrees of freedom of $(R - 1) * (C - 1)$ and a selected confidence level. If the obtained χ^2 value exceeds the critical χ^2 value, then the null hypothesis will be rejected, which means an association exists between the two categorical variables.

3.4.5 Spearman's rank correlation test

This test was conducted to assess the degree of association between two ordinal variables. Demographic variables (e.g., age and education level) were converted into ordinal variables for Spearman's rank correlation test. The correlation coefficient is calculated as follows:

$$r_s = 1 - \frac{6\sum {d_i}^2}{\mathrm{n}(n^2-1)}. \qquad \text{(Eq.3-6)}$$

Where n = The number of items to be ranked; d_i = difference in paired ranks.

$r_s > 0$ implies positive agreement among ranks;

$r_s < 0$ implies agreement in the reverse direction;

$r_s = 0$ indicates no agreement.

3.5 Semi-structured interviews

This type of interview is an interactive conversation, wherein the interviewer prepares a set of questions and topics in advance and decides on the point of discussion. However, this process allows more flexibility compared with the structured interview and is likely to change according to the interviewee’s reaction and interaction between the interviewer and interviewee (Fylan, 2005). Fylan (2005) claimed that semi-structured interview is suitable for figuring out “why” rather than “how many” or “how much” due to its flexible nature. Thus, this tool fits the purpose of this study. Semi-structured interviews were conducted on: (1) sixteen disadvantaged groups and five organizations working on helping the disabled, to understand the digital divide problem and derive possible solutions; (2) six stakeholders in the smart parking project to disclose the reasons as to why private car-park operators might be unwilling to open up their data through an integrated platform (as in the first case study); (3) five technical stakeholders who were directly involved in smart parking projects to obtain a generalized configuration of the SPIS (as in the second case study); and (4) twenty stakeholders in an open data project to identify key barriers in the project and their interdependencies (as in the third case study; the information collected from the interviews was used for SNA). After the interview requests are accepted, a set of questions will be sent out to the interviewees in advance for preparation. During the interviews, the interviewees were asked additional questions according to their situations and background as revealed during the active interactions.

3.6 Fuzzy Fault Tree Analysis (FFTA)

FFTA is used to study the reliability of the smart parking information system (SPIS) by investigating the causes and probability of service non-availability. Fault tree analysis (FTA) is a deductive analytical approach to identifying basic events that cause failure and determine their probabilities of occurrence. Since it was first introduction in 1961, this method has been applied in the reliability analysis of various systems, such as chemistry, electronics, and power (Mahmood *et al.*, 2013). This method relies on the translation of a physical configuration into a logic structure (Lee *et al.*, 1985), which reveals various situations that occur in a system that would result in failure (Shi *et al.*, 2014).

The conventional reliability analysis by FTA requires input of precise values of failure probabilities. However, obtaining the exact probability values of root causes would be difficult in the analysis of service failure of a SPIS due to the lack of empirical data, vague characteristics of events, or dynamic technology. Instead, the fuzzy analysis method is effective in estimating the probabilities of basic events that occur when little empirical information is available (Onisawa, 1990). Fuzzy logic can cope with uncertainty by expressing failure probabilities in the form of linguistic judgments (Zadeh, 1999). Experts with rich knowledge and experience in a specific domain provide a rough estimation of failure probabilities by giving descriptions, such as "low," "high," and "very high." The fuzzy methodology can then be used to define these linguistic terms in mathematical logic. In earlier bodies of research, FFTA has been used to analyze the failure rates of various systems and projects, such as explosion hazard of oil storage tanks (Shi *et al.*, 2014), contamination of a chemical cargo (Senol *et al.*, 2015), critical risks in Build–Operate–Transfer road projects (Thomas *et al.*, 2006), and failures in building a bridge (Pan & Wang, 2007).

3.6.1 Conducting FFTA

The first step of FFTA is establishing a fault tree. The "top event" should be defined first due to its criticality. Intermediate events, which may lead to the top event, will be defined and resolved further into constituent basic events (Shi *et al.*, 2014). Logic operators, such as AND and OR, are used to link basic and intermediate events, which reveal how these identified events combine and lead to the top event. Table 3-1 introduces the aforementioned key components that form a fault tree.

Table 3-1 Key components of a fault tree

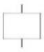
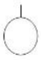
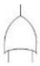
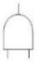
Key Component	Symbol	Description
Top event		An unexpected event, the target of FTA.
Intermediate events		An event that can be further broken into other events.
Basic/root events		The lowest event that cannot be developed further.
OR gate		The output occurs if any input occurs.
AND gate		The output occurs only if all inputs occur.

Table 3-2 briefly illustrates the process of conducting FFTA. The remainder of this section introduces the process of qualitative and quantitative analyses of FFTA in detail.

Table 3-2 FFTA of service non-availability of the SPIS

Main step	Details
1. Building the fault tree	Define the top undesired event; Define intermediate events by resolving the top event; Define basic events below the intermediate events; Link all types of events together by logic gates.
2. Qualitative analysis	Identify minimal cut sets (MCSs) by the Boolean algebra rules; Analyze structure importance.
3. Quantitative analysis	Obtain experts' linguistic expressions about the probability of each event occurring; Convert linguistic terms into fuzzy numbers via a trapezoid membership function; Calculate the failure rate (reliability) of the system; Compare the significance of basic events.

3.6.2 Qualitative analysis

3.6.2.1 Deriving minimum cut sets (MCSs)

A cut set contains basic events causing the system failure. It can be called a MCS only when they cannot be further reduced. MCSs may be obtained by analyzing the fault tree' structure.

3.6.2.2 Structure importance (SI) analysis

This analysis is to assess the influence of a basic event on the top event according to the fault tree structure instead of taking into account its occurrence probability (Huang *et al.*, 2016).

$$SI(i) = \sum_{R_i} \frac{1}{2^{n_i - 1}}. \qquad \text{(Eq.3-7)}$$

where SI(i) is the structure importance of a basic event X_i. n_i is the number of basic events in the MCSs which include X_i. R_i denotes the amount of MCSs consisting of X_i.

3.6.3 Quantitative analysis

3.6.3.1 Occurrence probability of basic events

Linguistic terms given by experts may be converted into fuzzy numbers based on a fuzzy logic system (Chen & Hwang, 1992). In this study, linguistic terms (e.g., 'very low', 'medium', and 'high') were transformed into trapezoidal fuzzy numbers through membership functions (shown in Figure 3-1). The α-cut was used to represent a respondent's confidence about his or her judgments in the form of an interval set of values out of a fuzzy number (Shi *et al.*, 2014). Corresponding α-cuts of trapezoidal fuzzy numbers (Eq. 2) are shown in Table 3-3. The obtained α-cuts were prepared for the aggregation of experts' opinions in the next step.

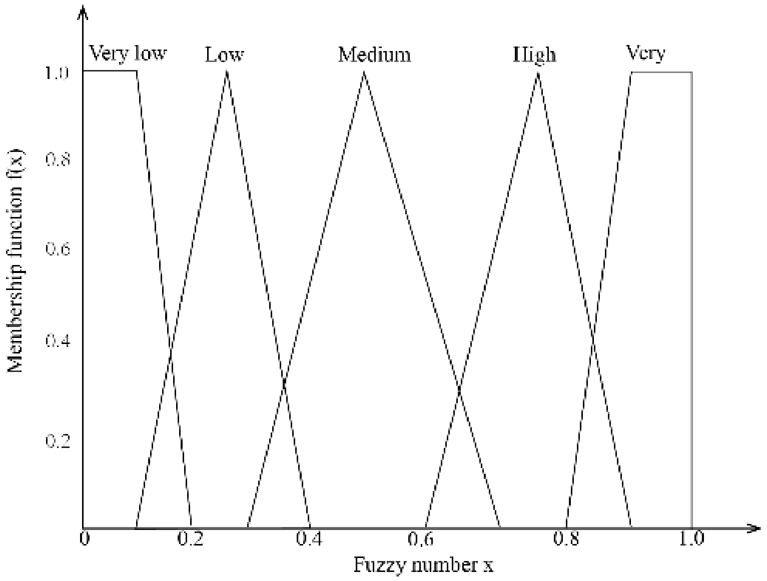


Figure 3-1 Trapezoidal fuzzy numbers

Table 3-3 α-cuts of fuzzy membership functions

Linguistic term	Fuzzy membership function (Eq. 2)	α-cut
very low (VL)	$f_{VL}(x) = \begin{cases} 1 & (0 < x \leq 0.1) \\ \frac{0.2-x}{0.1} & (0.1 < x \leq 0.2) \\ 0 & (otherwise) \end{cases}$	[0.2-0.1α, 1]
low (L)	$f_{L}(x) = \begin{cases} \frac{x-0.1}{0.15} & (0.1 < x \leq 0.25) \\ \frac{0.4-x}{0.15} & (0.25 < x \leq 0.4) \\ 0 & (otherwise) \end{cases}$	[0.15α+0.1, 0.4-0.15α]
medium (M)	$f_{M}(x) = \begin{cases} \frac{x-0.3}{0.2} & (0.3 < x \leq 0.5) \\ \frac{0.7-x}{0.2} & (0.5 < x \leq 0.7) \\ 0 & (otherwise) \end{cases}$	[0.2α+0.3, 0.7-0.2α]
high (H)	$f_{H}(x) = \begin{cases} \frac{x-0.6}{0.15} & (0.6 < x \leq 0.75) \\ \frac{0.9-x}{0.15} & (0.75 < x \leq 0.9) \\ 0 & (otherwise) \end{cases}$	[0.15α+0.6, 0.9-0.15α]
very high (VL)	$f_{VH}(x) = \begin{cases} \frac{x-0.8}{0.1} & (0.8 < x \leq 0.9) \\ 1 & (0.9 < x \leq 1.0) \\ 0 & (otherwise) \end{cases}$	[0.1α+0.8, 1]

3.6.3.2 Aggregation of experts' opinions

Respondents differ in their levels of expertise. Their opinions need to be evaluated based on their experience and knowledge in a specific domain (Senol *et al.*, 2015). The weighting for each expert is computed by:

$$\mathrm{W_i} = \frac{\text{Weighting score of expert i}}{\text{Sum of weighting scores of all experts}}. \qquad \text{(Eq. 3-8)}$$

The given weights for each expert will be used in the step of aggregation which is to combine individual experts' opinions into a single output fuzzy set. A suitable and common method is the linear opinion pool introduced by Stone (1961):

$$A_i = \sum_{i=1}^{n} W_j f_{ij} \quad \text{(j=1, 2, …, n).} \qquad \text{(Eq. 3-9)}$$

where A_i is the aggregated fuzzy set of basic event X_i. n is the number of basic events. W_j is the weight of expert j and f_{ij} represents the α-cut of his or her judgment towards X_i. The corresponding membership function of A_i is Eq. 5 (Lin & Wang, 1997) and depicted as Figure 3-2.

$$f_A(x) = \begin{cases} f_A^L(x) & (a \le x \le b) \\ 1 & (b \le x \le c) \\ f_A^R(x) & (c \le x \le d) \\ 0 & (otherwise) \end{cases} \qquad \text{(Eq. 3-10)}$$

with a≤b≤c≤d≤1, A = (a, b, c, d) denotes the trapezoidal fuzzy number, $f_A(x)$ denotes the trapezoidal membership function of basic event X_i, 'a' in $f_A^L(x)$ and 'b' in $f_A^R(x)$ are respectively the lower (left) and upper (right) bounds of the available area for the data in question, values in interval [b, c] are the most probable values of $f_A(x)$.

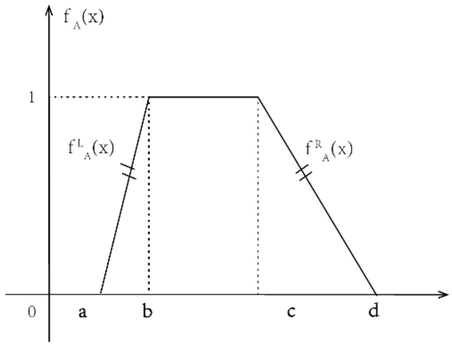


Figure 3-2 Aggregated fuzzy membership function $f_A(x)$

3.6.3.3 De-fuzzification process

This process is aimed at converting a fuzzy number into a Fuzzy Probability Score (FPS) which is a crisp value representing an expert's perception towards the most likely score about the occurrence of an event (Shi *et al.*, 2014). Left and right fuzzy ranking methods introduced by Chen and Hwang (1992) were deployed to determine FPS because it is intuitive and easy to implement (Lin & Wang, 1997).

$$\mathrm{FPS} = \frac{\mu_R + (1-\mu_L)}{2}. \qquad \text{(Eq. 3-11)}$$

where $\mu_L = \frac{1-\mathrm{a}}{1+\mathrm{b}-\mathrm{a}}$. and $\mu_R = \frac{\mathrm{d}}{1+\mathrm{d}-\mathrm{c}}$. (Eq. 3-12)

3.6.3.4 Transforming FPS into Fuzzy Failure Probability (FFP)

The FPS needs to be transformed into FFP to determine the occurrence probability of basic events. This conversion ensures the compatibility between the true value of occurrence probability and FPS. Onisawa (1988) defined FFP as:

$$FFP = \begin{cases} \frac{1}{10^k} & (FPS \neq 0) \\ 0 & (FPS = 0) \end{cases} \qquad \text{(Eq. 3-13)}$$

where $k = [\frac{1-\mathrm{FPS}}{\mathrm{FPS}}]^{1/3} \times 2.301.$ (Eq. 3-14)

3.6.3.5 Occurrence probability of the top event

The occurrence probability of the top event (TE) can be computed by formula:

for AND gate: $P(TE) = \prod_{i=1}^{n} FFP(x_i)$. (Eq.3-15)

for OR gate: $P(TE) = 1 - \prod_{i=1}^{n}\{1 - FFP(x_i)\}$. (Eq.3-16)

where P(TE) is the occurrence probability of the top event. FFP(x_i) is the occurrence probability of basic event X_i. n is the number of basic events.

3.6.3.6 Importance analysis

Importance analysis measures the significance of each basic event in terms of its contribution to making the top event occur. Besides structural importance, there are 2 other importance analyses of basic events, i.e. probability importance analysis and critical importance analysis. They rely on the failure probability obtained by the previous steps. Probability Importance (PI) measures the marginal influence of a basic event to the occurrence of a top event, that is, how the occurrence probability change of the basic event will influence that of the top event (Huang *et al.*, 2016). It can be computed by:

$PI\ (X_i) = \frac{\partial \mathrm{P\ (TE)}}{\partial X_i}$. (Eq.3-17)

where $PI\ (X_i)$ is the probability importance of the basic event X_i. P(TE) denotes the probability function of the top event.

However, the occurrence probability of an event with high PI may be low so that its direct influence on the top event should be adjusted to a lower level. This is reflected by the parameter Critical Importance (CI) which evaluates the relative change ratio of the occurrence probability of the top event divided by that of a basic event (Huang *et al.*, 2016).

$$CI\ (X_i) = \frac{\mathrm{P}\ (X_i)}{\mathrm{P\ (TE)}} PI\ (X_i). \qquad \text{(Eq.3-18)}$$

where $CI\ (X_i)$ refers to the critical importance of basic event X_i. $PI\ (X_i)$ is the probability importance of X_i. $P(X_i)$ is the occurrence probability of X_i, and P(TE) is the probability of the top event.

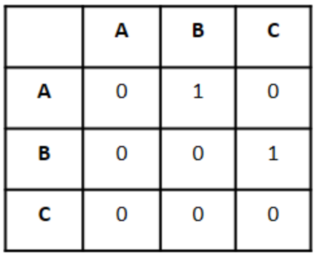
By using FFTA, the reliability analysis of a central carparking information system may be derived for a better understanding of the risk of system non-availability, as a case study to illustrate the system insecurity pitfall of SC projects.

3.7 Social Network Analysis (SNA)

A social network comprises of a set of nodes in a structure, where a few of the nodes are linked by one or more relations (Knoke & Yang, 2008). In this context, SNA is a quantitative instrument used to visualize node interactions and investigate their relational structures based on which managers can take actions for enhancing project performance especially for inter-organizational projects (Solis *et al.*, 2012), such as green building (Yang & Zou, 2014), urban redevelopment (Yu *et al.*, 2017), and major public engineering works (Mok *et al.*, 2017). In existing studies, nodes within a network may represent stakeholders (Prell *et al.*, 2009; Leon *et al.*, 2017), their responsibilities (Lin *et al.*, 2017), or concerns (Mok *et al.*, 2017). Given its powerful functions of identifying and visualizing interdependencies among a set of factors and exploring the implications of identified relationships (Wasserman & Faust, 1994), SNA was applied to investigate the interrelationships among the barriers faced by different stakeholders in the open data project. SNA mainly comprises the following three steps:

3.7.1 Identification of barriers and their interdependencies

This step was processed through desktop studies and semi-structured interviews with stakeholders. The identified barriers are represented by the nodes of the network. The design structure matrix, which was established by Steward (1981), was then applied to represent interdependencies among each pair of barriers. Figure 3-3 demonstrates the structure matrix. For instance, “1” at row A and column B indicates an influence from A to B. “0” means no interrelation between two nodes.



	A	B	C
A	0	1	0
B	0	0	1
C	0	0	0

Figure 3-3 Sample structure matrix for SNA

The following two sections introduce a range of parameters that analyze a network in the network- and link/node-level analyses. Link and node level analysis may be derived using SNA to achieve an enhanced understanding of the relative position of the barriers faced by various stakeholders in the open data project, as well as their inter-relationships. This process is an example of analysis of the potential pitfalls of SC projects.

3.7.2 Network level analysis by SNA

(1) *Density*: the ratio of the existing links in a network to the maximum amount of links if all nodes are connected with one another (Wasserman & Faust, 1994). The ratio ranges from 0 to 1. The denser the network, the more interdependencies exist in the

network.

(2) *Cohesion*: "*the distance, or the number of links, to access nodes in a network"* (Prell *et al.*, 2009). This concept is based on the shortest path and shows the overall complexity of a network (Yang & Zou, 2014).

3.7.3 Link and node level analyses

(1) *Degree centrality*: the extent to which a node directly interacts with others in the network. This concept pertains to the number of out-coming relations from a node in the network, i.e., *out* degree; or incoming relations to a node, i.e., *in* degree (Parise, 2007). The ego size of a node is the sum of out- and in-degree relations, whereas degree difference is the subtraction result of *in* degree from *out* degree.

(2) *Status centrality*: the number of the direct neighbors of a node, as well as other nodes that connect to the node in question through these direct neighbors (Katz, 1953). This concept differs from degree centrality, which only considers immediate neighbors (first degree nodes). Status centrality measures the overall impact of a node in the network.

(3) *Betweenness centrality*: how often a node/link falls between other node/link pairs based on the shortest distance (Kim *et al.*, 2011). A node/link with high betweenness centrality acts as a gatekeeper in the network to control the relation passing through (Yang & Zou, 2014).

(4) *Brokerage:* how frequent a node acts as a coordinator, gatekeeper, representative, itinerant or liaison in a triad (Gould & Fernandez, 1989). Stakeholder type can be set as the partition vector to compute this indicator. "X," "Y," and "Z" represent different

nodes in a network:

- “X” can be called a coordinator when it obtains connection from “Y” in the same partition and sends out a connection to “Z” in the same partition.
- “X” becomes a gatekeeper when it gains connection from “Y” in a different partition and emits a connection to “Z” in the same partition with “X.”
- “X” becomes a representative if it receives a connection from “Y” with the same partition and emits a connection to “Z” with a different partition.
- “X” becomes an itinerant when it receives a connection from “Y” with a different partition and emits a connection to “Z” in the same partition with “Y.”
- “X” becomes a liaison when “X,” “Y,” and “Z” are in different partitions from one another.

3.8 Summary

This chapter presents an overview of the used research methodology in this study. This chapter discusses the reasons for the deployment of various methods and outlines their application processes. The next chapter presents a data analysis of the first questionnaire survey.

CHAPTER 4 POTENTIAL PITFALL IDENTIFICATION AND EVALUATION

4.1 Introduction

In the previous chapter, the possible causes, adverse effects, and mitigation/preventative measures of SC pitfalls have been identified based on a comprehensive literature review. This chapter reports on the first questionnaire survey, which was designed to obtain a better understanding on these pitfalls and lay a foundation for case studies in the next stage as well as for evaluating the effectiveness of the proposed mitigation measures. More specifically, this chapter aims to obtain relative rankings on issues identified from the literature review, including: (1) the occurrence likelihood (OL) and severity (SE) of possible causes of each pitfall, (2) SE of the associated adverse effects, and (3) the effectiveness of the proposed mitigation/preventative measures. To set a contextual background for evaluation, the following section provides an overview of the current SC development in Hong Kong. The data collection and analysis processes are first described, followed by a discussion on the factors of significant rankings. This chapter ends with a summary of the key findings.

4.2 Background information of SC development in Hong Kong

4.2.1 Overview

The Hong Kong government has been committed to building a "Smarter Hong Kong, Smarter Living" since the publication of the 2014 Digital Strategy 21 (after three updates in 2001, 2004 and 2008). The government has proposed a set of SC initiatives that includes expanding the coverage of Wi-Fi, further digitizing government operations, and widely employing IoT (Development Bureau, 2015). By leveraging ICTs, the strategy aims at stimulating business innovation, boosting the ICT industry, and digitizing public services (Commerce and Economic Development Bureau, 2013). The overall development plan that underpins the SC strategy includes six themes, namely, smart mobility, smart living, smart environment, smart people, smart government, and smart economy (Office of the Government Chief Information Officer, 2017). These themes reflect current bottlenecks in Hong Kong's development and smart solutions to address them. The Chief Executive announced in the 2015 Policy Address that Kowloon East (KE) was to be established as a pilot area for testing the feasibility of making Hong Kong a SC. A series of proof of concept (PoC) trials have been conducted in KE so far to evaluate the effectiveness of smart solutions and analyze the practicability of a wide deployment to city scale. A few examples of PoC include crowd management system, water quality alert system, and energy efficiency data acquisition system. Hong Kong ranked at 68th and lagged behind other Asian cities/regions, such as Singapore (second), Tokyo (sixth), and Seoul (21st) in the Easy Park Group's 2017 Smart Cities Index. This index analyzed data for over 500 cities worldwide based on 19 factors, such as transportation, sustainability, and governance. Relatively speaking, Hong Kong can only be regarded as an "emerging smart city."

4.2.2 Identified pitfalls in Hong Kong's emerging SC development

Several observations were made on the identified pitfalls in Hong Kong. The number of botnet events (that is, a network of interconnected IoT devices is hacked) was found to rise evidently by 77% from 2,635 in the third quarter of 2016 to 4,656 in the fourth quarter of the same year (HKCERT, 2017). Nearly half (41%) of the botnet events result from the “Mirai” malware, which used infected IoT devices to make distributed denial of service (DDoS) attacks to a large scale. From its first outbreak in October 2016 to March 2017, “Mirai” infected approximately 2,000 connected devices in Hong Kong (Ho, 2017). If additional IoT devices are deployed without caution, the city should likely cope with further similar hackings, which would render the maintenance of proper city functions difficult.

Citizens’ privacy would be threatened when personal data are collected and used without transparency or prior consent of data owners. The Octopus card in Hong Kong enables electronic payments in all public transportation and a number of retailers. This card is one of the world’s most frequently used smart cards and handles over 14 million transactions every day (Octopus Cards Limited, 2016). However, Octopus Cards Limited collected personal information, such as citizen ID and passport numbers and month-and-year of births without the consent of cardholders (South China Morning Post, 2010). In 2010, the Octopus Cards company admitted selling personal information of one million cardholders to private entities for HKD 44 million. This saga faced criticism and distrust because the effect of information leaks is extremely difficult, if not impossible, to remediate.

The problem of information islands persists in Hong Kong’s government departments.

A one-stop Hong Kong database portal will be available by approximately 2023. Numerous public data, such as transport and building information, are managed by entities using various standards and formats. This brings inconvenience to citizens and hinders innovation in an era of big data. A consultant study on Smart City Blueprint for Hong Kong (Office of the Government Chief Information Officer, 2017) claimed that one of the major challenges of becoming “smart people” is the fact that existing services are backed by their ICT infrastructure that are legacy and duplicated, hence obstructing data integration and transfer across the related bureaus/departments (B/Ds).

Although Hong Kong is a well-developed city, a digital gap among groups remains. The latest Hong Kong Thematic Household Survey Report No. 64 reported that nearly half (47.9%) of people aged 65 and over 10 did not possess a smartphone in 2017. Among people aged 10 and over, the elderly (people aged 65 and over) had the lowest rate of knowing how to use personal computers at 37.4%. An increasing number of government services are digitized in cities worldwide. However, whether or not the (potential) users possess the required digital skills should be carefully considered. Digitizing certain services, such as applications for welfare and social housing, will be ironic because these services are needed by people who have relatively poor digital literacy or experience problems in accessing a computer (Maxwell, 2018).

4.3 Data collection

4.3.1 Questionnaire design and expert selection

The questionnaire was developed based on the literature review, which identified the causes of pitfalls, their adverse effects, and possible mitigating measures. A sample of the questionnaire is attached for viewing in Appendix 1, Survey Questionnaire: *A study of the potential pitfalls in the development of smart cities.* Part A of the questionnaire covers the respondents' background, followed by a brief introduction of each potential pitfall to ensure a common understanding among the respondents. To examine if respondents have sufficient knowledge about SCs, the following question was added at the end of the respondent background section: "How much do you know about smart cities?" The remaining part of the questionnaire was designed to collect data in the form of a five-point Likert scale about the respondent's evaluation of: (1) OL (1 = very low, 5 = very high) and SE (1 = not severe at all, 5 = extremely severe) of each pitfall; (2) adverse effects of each pitfall (1 = not severe at all, 5 = extremely severe); and (3) effectiveness of possible mitigation measures against the pitfalls (1 = not effective at all, 5 = extremely effective).

Targeted expert respondents were sourced from SC conference brochures and company/organization directories based on whether their occupations and educational background were in fields related to ICT and SC. Specifically, the questionnaires were mainly distributed to people working in: (1) the information technology (IT) unit/section of government departments; (2) NGOs closely related to SC development and supporting disadvantaged groups; (3) research institutes on urban development, social services, and technology; (4) known private consultancies and project management teams of SC projects in various areas (e.g., energy, construction, urban planning); and (5) private companies that develop technological innovation and smart economies. Snowball technique was used to solicit a sufficient number of targeted respondents by specifying that recipients should have a certain level of expertise in SC. Several questionnaires were sent by post with stamped self-addressed return envelopes to increase the response rate. A minority were sent via emails when only email addresses were available.

4.3.2 Questionnaire survey

A pilot study was carried out to verify the clarity of questions. The actual questionnaire survey was conducted during June 2017 to November 2017 on experts in the domain of ICT and SC. Out of 296 questionnaires distributed in Hong Kong, 58 valid replies were received. Eight respondents claimed to know extremely little about SC. Thus, they were excluded from further analysis. As a result, 50 valid questionnaires were used for the data analysis. Table 4-1 shows the key demographics of the respondents. Most of the respondents were technology developers and engineers (38.0%) and approximately 64.0% of respondents had over 10 years of working experience. Respondents also included senior consultants and project managers of ICT development (e.g., IoT, big data, and A.I.) in reputable technology companies, principal (software) engineers from public entities, and senior researchers from institutes in the urban and construction technology development domains.

Table 4-1 Profile of respondents of the Questionnaire Survey #1

Demographic Type	Detail	Sample size	Percentage
Region of work	Hong Kong	50	100%
Highest education level	College or diploma	2	4.0%
	University and above	48	96.0%
	Total	*50*	*100%*
Type of organization	Public sector or related organization	29	58.0%
	Non-government organization (NGO)	1	2.0%
	Private sector	20	40.0%
	Total	*50*	*100%*
Nature of work	Technology development/engineering	19	38.0%
	Project management	9	18.0%
	Marketing/sale	1	2.0%
	Customer service	4	8.0%
	Academic	9	18.0%
	Consultancy/advisory	8	16.0%
	Total	*50*	*100%*
Working experience	Less than 2 years	2	4.0%
	2-4 years	3	6.0%
	5-10 years	13	26.0%
	Over 10 years	32	64.0%
	Total	*50*	*100%*
Knowing about SC	I have some knowledge about it.	29	58.0%
	I know it very well.	21	42.0%
	Total	*50*	*100%*

4.4 Data analysis

4.4.1 Reliability analysis and Kendall's coefficient of concordance

Upon receipt of returns, data analysis was conducted using the SPSS statistical package.

Cronbach's alpha reliability test was performed to assess the internal consistency of the survey instrument using a five-point Likert scale. The Cronbach coefficient of this study reached 0.927, which satisfied the minimum threshold level of 0.7 as recommended by Santos (1999). Hence, responses were suitable for further analysis via Kendall's concordance and mean score ranking. Kendall’s coefficient of concordance (W) was then calculated to measure the level of agreement among respondents who rated the OL, SE, and effectiveness. If the number of factors within a group of questions exceeds seven, then the significance of W should be determined based on the Chi-square value with a degree of freedom of $\mathrm{N} - 1$, otherwise, W will depend on the *p*-value generated by SPSS. The value of W ranges from 0 (“no agreement”) to 1 (“complete agreement”). The greater the W, the higher the level of agreement reached, provided that a predetermined level of statistical significance level is attained.

4.4.2 Risk impact ranking of possible causes of pitfalls

The technique of mean score ranking (as introduced in Chapter 3) was used to evaluate the key factors by comparing their relative importance (Chan et al., 2003). The rankings of OL and SE of possible causes that trigger pitfalls were directly derived from the mean scores. Risk impact (RI) is a joint function of OL and SE (Ameyaw & Chan, 2015). RI can be computed as follows:

$\mathrm{RI} = (\mathrm{OL} \times \mathrm{SE})^{0.5}$. (Eq.4-1)

4.4.2.1 Causes of system information insecurity

Table 4-2 shows the RI ranking of factors that lead to system information insecurity.

Table 4-2 Ranking of causes of system information insecurity

Possible causes	OL	SE	RI	Rank
Cyber-attacks.	3.87	4.35	4.15	1
Weak security and encryption, security being an after-thought.	3.44	4.14	3.86	2
Large and interdependent systems with many stakeholders. involved, making it difficult to ensure end-to-end security.	3.62	3.86	3.82	3
Poor management and operation models of outsourcing products and services.	3.60	3.51	3.60	4
Human errors and negligent staff.	3.44	3.44	3.52	5
Errors in design.	3.29	3.58	3.51	6
Using insecure legacy systems and poor maintenance.	3.29	3.60	3.48	7
Limited security sponsorship and management support in the development of smart systems.	3.18	3.63	3.44	8
Kendall's W	.066	.213	-	-
Chi-Square	20.866*	63.976*	-	-
Asymp. Sig.	.004	.000	-	-

* Chi-Square > critical value (14.07) at 0.05 level, hence the answers to this group are associated with statistical significance.

Cyberattack is a risky cause of system information insecurity, with the highest OL and SE. Triangulation with existing literature showed that the Hong Kong Computer Emergency Response Team (HKCERT) reported 6,506 cybersecurity complaints that occurred in Hong Kong in 2017. This figure indicates an increase of 7% from 2016. The increase in cyber-attacks coincides with a spike in malware attacks. Cyber-attacks in Hong Kong can cause an economic loss that is projected to reach USD 32 billion annually within the next few years and as much as approximately 10% of Hong Kong’s gross domestic product (Shen, 2018). The second risky factor is “weak security and encryption.” Although this factor’s occurrence probability ranked fourth, the consequence is extreme (second) should it happen. Literature revealed that 70% of common IoT devices were fragile in terms of password security, encryption, and user access control (HP Inc., 2014). Hence, poor security design and encryption make smart components vulnerable to many possible attacks. The third most risky factor is “large and interdependent systems.” That is, a large system or utility network is composed of many intertwining parts, which are owned and controlled by various stakeholders. Thus, securing every aspect is difficult (Cerrudo, 2015).

4.4.2.2 Causes of personal information leakage

Table 4-3 shows that the top causes of personal information leakage include the “absence of strict standards/regulations to protect personal information.” Big data analytics and profiling that are prevalent in SCs add to the risk of privacy leakage through, for example, excessive collection of personal data and discovery of named individuals from anonymous data. During the fifth Privacy Sweep of the Global Privacy Enforcement Network (GPEN) in 2017, the Privacy Commissioner for Personal Data (PCPD) in Hong Kong found that the privacy policies of 30 customer loyalty and reward programs lacked transparency in their broad and vague privacy policies. Customers do not possess strong control over their personal data in terms of data deletion, data sharing, and profiling.

Table 4-3 Ranking of causes of personal information leakage

Possible causes	OL	SE	RI	Rank
Absence of strict standards/regulations to protect personal information.	3.91	4.04	4.02	1
Insufficient awareness and knowledge on data protection of users.	3.83	4.00	4.02	1
Heterogeneity and ubiquity of IoT-enabled system without providing notice and seeking consents of targets.	3.70	3.62	3.73	2
Unauthorized access to systems.	3.24	4.04	3.70	3
Kendall's W	.119	.081	-	-
Asymp. Sig.	.001*	.012*	-	-

* significant at 0.05 level

The second riskiest cause of personal information leakage is “insufficient awareness and knowledge on data protection of users.” A previous survey on the privacy awareness of smartphone users was commissioned by PCPD (2012) in Hong Kong. The survey revealed that only 36.0% of respondents who installed mobile apps knew what information their apps could access from within their phones. Before answering the questionnaire, more than half of those respondents (70.3%) did not know that apps might secretly access information that app developers had not said they would. Only 13.2% of the respondents used encryption to protect personal information that is stored in their phones. Irrespective of the lack of protection regulations, this cause pertains to the behaviors of users, which calls for further proactive preventative measures on the part of the authorities.

4.4.2.3 Causes of information islands

Table 4-4 shows that the ranking of OL and SE of information islands is non-significant in Kendall's W-test. This notion means that the respondents did not reach a consensus in their given scores for this group of questions. The problem of information islands arises from management and planning slacks rather than technological in nature (Yanrong & Whyte, 2014). Therefore, another method should be used to examine the stakeholder-related rationale instead of ranking the relative importance of possible causes. To supplement this claim, a SNA was conducted afterward to investigate the barriers of resolving information islands via a citywide open data platform and complex interdependencies among those barriers (see Chapter 7).

Table 4-4 Ranking of causes of information islands

Possible causes	OL	SE
Incompatible data standards and formats.	3.73	3.65
Difficulty of engaging with a broad spectrum of stakeholders.	3.92	3.74
Insufficient cooperation and communications among stakeholders.	3.94	3.76
Independent development and non-integrated planning of IT application systems.	4.08	3.65
Closed government culture and risk-averse policy.	4.08	3.93
Kendall's W	.025	.013
Asymp. Sig.	.318#	.675#

# not significant at, 0.05 or 0.01 level.

4.4.2.4 Causes of digital divide

Table 4-5 reveals the ranking of possible causes that lead to digital divide. The top factor is “personal attitude barriers and weak information awareness of citizens” with the highest OL (mean score = 3.55). Besides being influenced by relatively fixed demographic factors (e.g., gender, income, and age), people hold their beliefs and attitudes toward a technological innovation over time and shape their digital behavior accordingly (Dutton & Blank, 2015). One of the attitude barriers that contributes to digital divide might be concerns about privacy leakage. People might doubt the social benefits of the Internet and regard it as an intrusion into their personal information (Dutton & Reisdorf, 2017). Another example of attitude barriers is insufficient confidence or certain pre-conceptions; for example, "computers are for 'brainy' people, for males, for the young" (Botha et al., 2001). This finding reflects the need for calls to narrow digital divide and for concerted efforts from the psychological perspectives by constructing a trustworthy environment and positive mindset among users in the long run.

Table 4-5 Ranking of causes of digital divide

Possible causes	OL	SE	RI	Rank
Personal attitude barriers and weak information awareness of citizens.	3.55	3.32	3.47	1
Lack of training programs for unskilled citizens.	3.30	3.02	3.21	2
Lack of special care for disadvantaged groups.	3.13	3.00	3.16	3
Insufficient engagement initiatives from the society.	3.21	2.98	3.15	4
Poor quality of services.	2.83	3.34	3.13	5
Computer ill-literacy and lack of skills.	2.83	3.34	3.09	6
Insufficient provisions of physical access to the Internet and advanced services.	2.34	3.64	2.98	7
Kendall's W	.258	.156	-	-
Asymp. Sig.	.000*	.000*	-	-

* significant at the level of 0.01.

The second cause is "lack of training programs for unskilled citizens." This cause is closely related to the second-level digital divide, "skill divide," which indicates that gaps of capability exist in the use of the Internet and digital devices ("Internet access divide" belongs to the first level, as introduced in the literature review, Section 2.6 in Chapter 2) (Hargittai, 2001). A number of projects provide IT training in Hong Kong. For example, a subsidy of HKD 0.3 million was provided in 2000 by the Social Welfare Department to develop 43 ICT-related projects, such as basic training on the use of Octopus cards (a value-storing smart card for electronic payments in Hong Kong), automated teller machines, and web surfing. However, additional trainings to build up capability are needed, such as that needed for outdoor navigation, and online booking, and enjoy the benefits brought about by SCs. The third factor is the "lack of special concerns for disadvantaged groups." Digital inequalities continue to exist because several people are lagging behind. Understanding the status of disadvantaged groups and keeping special concerns for them, such as maintaining in-person services in certain well-publicized places is necessary.

Hong Kong is a well-developed city with quality infrastructure and a high penetration rate of smartphones and Internet. According to the Thematic Household Survey Report No. 64, the proportion of people aged 10 and over who have Internet access increased from 87.5% in 2016 to 89.4% in 2017. In 2016, the smartphone penetration rate reached 85.8%, which increased to 88.6% in 2017. Hence, the occurrence likelihood of "insufficient provisions of physical access to the Internet and advanced services" is relatively low (mean score = 2.34). However, the severity of its adverse effects (once it happens) was acknowledged by the survey respondents (3.64, the highest mean score in SE). A reflection that could be made by other emerging SCs is that accessibility to the Internet and digital devices lays the foundation for narrowing the digital divide.

4.4.3 Ranking of severity of pitfalls

Table 4-6 shows that the mean scores of pitfall severity (if the pitfall occurs) range from 3.35 to 4.15, which suggest that the consequences of these pitfalls are moderate to high.

Table 4-6 Ranking of severity of pitfalls

Consequence of each pitfall	Pitfall related	SE	Rank
Breaching the confidentiality of users' information.	A	4.15	1
A system-wide failure and non-availability of essential services.	A	4.04	2
Risking public trust towards the society and posing threat to democracy.	B	4.02	3
Information exposure, citizen tracking and even impersonation.	B	4.02	3
Reducing the efficiency of smart cities.	C	3.89	4
Replicated facilities, resources wasting and overlapping investment.	C	3.70	5
Economic loss #1.	A	3.57	6
Economic loss #2.	B	3.48	7
Reducing the efficiency and effectiveness of smart cities.	D	3.46	8
Causing inconvenience in residents' life.	C	3.41	9
Widening social and economic inequality.	D	3.35	10
Kendall's W	-	.111	-
Chi-Square	-	56.102*	-
Asymp. Sig.	-	.000	-

*Chi-Square > critical value (23.209) at 0.01 level.

Note: A-system information insecurity; B-privacy leakage; C-information islands; D-digital divide.

The most severe effect of these pitfalls is "breaching the confidentiality of users' information" due to system insecurity. Confidentiality forms an essential part of information security. In July 2018, a cyberattack that targeted Singapore health authorities stole the personal profiles of 1.5 million patients. A month later, Hong Kong's Department of Health became a victim. The ransomware locked certain files with encryption (Lo, 2018). Another recent major cyberattack in Hong Kong was the unauthorized access of 380,000 Hong Kong broadband network customers' personal data, such as details of over 40,000 credit cards (Lo, 2018). The loss of users' information caused by system insecurity can be widespread, thereby bringing severe consequence to citizens. "A system-wide failure and non-availability of essential services" that is brought to the information system was considered the second most severe consequence. The operation of important services has increasingly become dependent on information systems, such as traffic control, disaster warning, and stock exchange. If the services of these "mission-critical" systems are disrupted by cyber-attacks, human errors, or other problems, then the panic and loss of money and public trust cannot be underestimated.

The negative effects brought about by personal information leakage were listed as the third most severe results, such as risking public trust toward the society and posing threat to democracy (mean score = 4.02), causing information exposure, citizen tracking, and even impersonation (mean score = 4.02). Privacy is a fundamental facet recognized in the United Nations Declaration of Human Rights. As SCs may pose threats to citizens' privacy, further effort should be paid to protect it.

Information islands reduce the efficiency of SCs (4th SE) and cause replicated facilities, waste of resources, and overlapping provisions (5th SE). This problem remains acute in Hong Kong’s transport information. Several platforms/mobile apps have been launched by the Transport Department and other government agencies. For example, “HKeRouting” provides driving routes and disseminates real-time parking vacancy information on a small proportion of privately operated car parks (less than 2% by June 2017). At the time of writing, only 135 (9.3%) parking lots out of 1,465 that were listed in “HKeRouting” can inform users if they have vacancies or not. In addition, 112 of these car parks actually indicate the number of spaces in “real-time” (7.6%) (Edmunds, 2018). “HKeMobility,” which is the new “all-in-one” app for journey planning with an investment of HKD 600,000 (USD76,500), is similar to the previous “HKeTransport”. “HKeMobility” does not provide arrival times for services run by major carriers, such as the Kowloon Motor Bus Company (KMB), New World First Bus, Citybus, and Mass Transit Railway (Leung, 2018). Users need to switch to the companies’ own apps to search for relevant information. This non-integration of information reduces the efficiency that was promised by SCs and negates the intensive use of resources.

Unexpectedly, the consequences brought about by digital divide were not ranked highly, especially “social inequality and exclusion.” However, its mean score (3.35) remains above moderate. A probable reason for this finding may be because Hong Kong is an emerging SC, where not all services are digitized. Although social inequality continues to exist, the Internet and digitization accelerate and reinforce it (Witte & Mannon, 2010). “Higher-status” groups may gain access to more information and benefit more than disadvantaged and excluded individuals (Van Deursen & Van Dijk, 2014). City managers should pay attention to the long-term impacts of the growing digital divide.

4.4.4 Ranking of preventative/mitigation measures against pitfalls

4.4.4.1 Measures against system information insecurity

According to Table 4-7, “developing a cybersecurity strategy and recovery plan” is the top effective solution to ensure information security, followed by “improving security awareness and availability safeguards, conducting continuous vulnerability assessment.” Smart cities call for improved protection measures and supportive innovation in cyberspace and economic prosperity. Cyber security strategies are necessary for cities and organizations, which entail a series of objectives and principles that need to be implemented. For example, within the Hong Kong government, extensive IT security policies and relevant practice guides are in place for use by government B/Ds and agencies. Such guides include Baseline IT Security Policy, Practice Guide for Cloud Computing Security, and Practice Guide for Security Risk Assessment & Audit (OGCIO, 2017). Nevertheless, security violations cannot be totally mitigated despite numerous security solutions and policies that are in place because criminal skills are also evolving (Chouffani, 2016). Preparing for recovery plans within an organization would limit the damage of the incident and isolate the affected components. Continuous assessment and an alert mindset can help organizations stay ahead of criminal activities. Another important measure is “employing/developing well-defined standards for developing and managing ICT services.” Various standards were proposed by different standardization organizations at the global, regional, and national levels, such as the ISO, Institute of Electrical and Electronics Engineers (IEEE), and the European Telecommunications Standards Institute (ETSI). These standards suit different scopes of work. For instance, ISO/IEC 27001, specifies effective information security management that covers an information system's life cycle; IEEE 2700-2014 defines performance parameters for sensors; and ETSI TS 102 690 introduces the end-to-end machine-to-machine functional architecture. The appropriate adoption of standards helps to optimize system security in SCs.

Table 4-7 Ranking of preventative/mitigation measures against system information insecurity

Mitigation measure	Effectiveness	Rank
Developing a cybersecurity strategy and recovery plan.	4.19	1
Improving security awareness and availability safeguards, conducting continuous vulnerability assessment.	4.04	2
Employing/developing well-defined standards for developing and managing ICT services.	4.04	2
General technical countermeasures such as frequent backup, antivirus programs, software updates, fire walls against intruders.	3.92	3
Management controls over operation and design.	3.67	4
Kendall's W	.090	-
Asymp. Sig.	.002*	-

* significant at 0.01 level

4.4.4.2 Measures against personal information leakage

According to Table 4-8, the most effective preventative measures to protect users' privacy are "legislation allowing users to control their own data" and "establishing ethical standards on how public data may be collected and used." This result echoes with the fact that the ranking of possible causes of this pitfall regarding the absence of common standards and solutions to protect personal information is the riskiest one. In

Hong Kong, an independent data privacy regulatory framework was enacted in the Personal Data (Privacy) Ordinance (PDPO) to regulate the private and public sectors that collect, store, process, or use personal data. With more data being collected ubiquitously in SCs, several important issues could be added into this principle-based regulation to ensure privacy protection, such as the right to erasure ("right to be forgotten"), distinguishing sensitive personal data from non-sensitive ones, regulating data processors directly, and requiring consent as a pre-requisite for the collection of personal data (currently, consent is a pre-requisite only when personal data are used for a new purpose). These issues are included in the EU's General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which became enforceable on May 2018. The GDPR also includes "employing Privacy by Design (PbD)," which is the third effective solution in the survey. PbD is a holistic concept that promotes embedding privacy as a default into any product and service design, operational processes, and management of ICT, across the entire life cycle of the information system. This approach is featured by being proactive rather than reactive. This approach seeks to render privacy integral to organizational priorities, project objectives, and work standards without compromising functionality. It can be observed that "Utilizing education to improve users' knowledge and awareness of protecting their privacy" and "informing developers their responsibilities and best exercises" were not ranked as the most effective measures. By contrast, the ranking of "insufficient awareness and knowledge on data protection of users" was ranked as the top risk of privacy leakage. This finding is due to the fact that improving people's awareness is a long-term task.

However, regulation is a direct and efficient tool to protect their privacy before they become aware of the importance of privacy and other effective ways to protect it.

Table 4-8 Ranking of preventative/mitigation measures against personal information leakage

Mitigation measure	Effectiveness	Rank
Legislation to allow users to control their own data and create a regulatory environment.	4.19	1
Establishing standards on how public data could be collected and used.	4.06	2
Employing Privacy by Design (PbD).	4.04	3
Utilizing education and training to help improve users' knowledge and awareness of information privacy and security, and informing developers their responsibilities and best exercises.	3.96	4
Conducting Privacy Impact Assessments (PIA).	3.83	5
Kendall's W	.067	-
Asymp. Sig.	.012*	-

* significant at 0.05 level

4.4.4.3 Measures against information islands

Table 4-9 presents the ranking of preventative/mitigation measures against information islands, which is non-significant in Kendall's W-test. As discussed in Section 4.4.2.3, SNA would be further conducted (in Chapter 7) to investigate the barriers faced by various stakeholders in building an open data platform and complex interdependencies among those barriers. Mitigation measures could then be obtained accordingly.

Table 4-9 Ranking of mitigation measures against information islands

Mitigation measure	Effectiveness
Sharing interoperable protocols among tech suppliers.	4.11
Formulating open standards and improving data quality.	4.26
Promoting cross-sectional collaboration among different interfacing organizations.	4.11
Planning the process of systems and data integration at the design stage.	4.02
Kendall's W	.038
Asymp. Sig.	.150*

* not significant at, 0.05 or 0.01 level.

4.4.4.4 Measures against digital divide

The ranking of preventative/mitigation measures against digital divide is not statistically significant as shown in Table 4-10. Several initial solutions could be made based on the ranking of possible causes of digital divide. “Personal attitude barriers and weak information awareness of citizens,” “lack of training programs for unskilled citizens,” and “lack of special concerns for disadvantaged groups” are the top three risks that trigger digital divide. Therefore, removing attitude barriers, providing digital training, and expressing genuine concerns (e.g., catering to the information needs of disadvantaged groups) might be implemented as mitigation measures against digital divide. The literature review (Section 2.6 in Chapter 2) suggested that qualitative methods, such as interviews, may be used to acquire an in-depth understanding of the type of support that is ultimately needed by disadvantaged groups (Scheerder et al., 2017). Therefore, in the first case study (Section 5.5.6.2 in Chapter 5), interviews with several disadvantaged groups and people helping the disabled were conducted to derive possible solutions that will narrow the digital divide.

Table 4-10 Ranking of preventative/mitigation measures against digital divide

Mitigation measure	Effectiveness
Increasing network coverage and the penetration of digital devices.	4.04
Providing financial support for computer acquisition/Internet access, and decreasing telecommunications charges.	3.82
Providing education and training, facilitate social learning to the public.	3.73
Improving public services for disadvantaged groups and enhancing their information literacy.	3.71
Motivating digital inclusion initiatives of both citizens and private sectors.	3.89
Kendall's W	.034
Asymp. Sig.	.190#

# not significant at 0.05 or 0.01 level.

4.5 Summary

The first questionnaire survey was targeted at experts in the SC domain to obtain a general understanding of pitfalls in SC development. The results show that cyber-attacks, weak security, and interdependency of systems were the riskiest causes of system insecurity, which would bring severe consequences to the society (compared with other pitfalls) by compromising the confidentiality of users' information and leading to a system-wide failure and non-availability of essential services. Developing a cybersecurity strategy and recovery plan are the most effective solutions against system insecurity. The top two risks that cause privacy leakage include the absence of strict standards/regulations to protect personal information as well as insufficient awareness and knowledge on data protection of users. Measures that protect citizens' privacy and improve public trust toward the society include a strict legislation that enables owners to control their data with increased digital rights and embedding privacy as a default across the entire information life cycle of any information system (deploying Privacy by Design). The third pitfall, namely, information islands, negatively influence the society by reducing the efficiency of SCs and causing replicated facilities, waste of resources, and overlapping provisions. However, the ranking of possible causes and mitigation measures of this pitfall is not statistically significant probably due to its complex nature. Therefore, SNA will be used to obtain the stakeholder-related mechanism behind the slow process of data integration (Chapter 7). Attitude barriers, insufficient training programs, and special concerns for disadvantaged groups are the top three risks that result in digital divide. Besides the provision of advanced digital training that caters to the needs of SCs, the narrowing of digital divide relies on constructing a trustworthy environment and positive mindset among users. The interview method may be used to achieve an in-depth understanding and explanation for the type of support that is needed by disadvantaged groups (Chapter 5). This expert-based questionnaire lays the foundation for the following chapters within which the four pitfalls will be examined within the context of several SC case studies in Hong Kong.

CHAPTER 5 A SURVEY ON THE PUBLIC USE OF MOBILE APPLICATIONS

5.1 Introduction

The preceding chapter depicts a general understanding on four potential pitfalls in terms of their possible causes, their adverse effects, and the effectiveness of proposed mitigation measures through a questionnaire survey. In this chapter, the public use of smart parking mobile applications (apps) is selected as the contextual background for demonstrating the potentiality of the identified pitfalls. Part of the data was collected through Questionnaire Survey #2 to investigate how users perceived these potential pitfalls within the context of mobile apps providing real-time parking information. Subsequent interviews were conducted to ascertain the reasons for the non-integration of real-time parking information and explore possible ways to avoid neglecting disadvantaged groups (particularly the elderly and disabled people) from the SC initiatives. First, the current situation of parking information in Hong Kong is introduced. The data collection procedure is then described, followed by a discussion and analysis of the main findings. This chapter ends with a summary. The results of Questionnaire Survey #2 were extracted from a publication with the candidate as the first author, as described in the footnote[3].

[3] Ma, R., Lam, P. T., & Leung, C. K. (2018). Potential pitfalls of smart city development: A study on parking mobile applications (apps) in Hong Kong. *Telematics and Informatics*, 35(6), 1580–1592.

5.2 Background information of smart parking in Hong Kong (Case study 1)

Smooth mobility becomes increasingly needed for metropolises, such as Hong Kong (with a population of over 7 million), which must cope with heavy vehicular and pedestrian flows daily. From 2006 to 2016, although the total number of parking spaces in Hong Kong increased by 9.5%, it was considerably below the growth rate of licensed vehicles (34.8%), particularly private cars (48.7%). The ratio of parking spaces to vehicle population consequently decreased from 1.32 to 1.05 (Hong Kong Legislative Council Panel on Transport, 2017). This ratio cannot satisfy the need of a private car, which requires more than one parking space on average because it moves between residence and destination. When vehicles cruise around for parking spaces, they contribute to road traffic congestion because they compete for road use, as highlighted in a report by the Hong Kong Transport Advisory Committee (2014). Therefore, real-time parking vacancy information for drivers is helpful for alleviating road congestions, pollutions, and accidents, with this aim forming a major part of the Smart Mobility projects in Hong Kong. As mobile apps have currently become more popular than computer-based browsers (Walravens, 2015; Unal *et al.*, 2017), several apps for disseminating real-time parking vacancy information have been developed by the government (e.g., eRouting and MyKE) and private entities (e.g., Sino Parking, LINK, and Wilson Parking) in Hong Kong. Most apps developed by private property owners only provide data of their own carparks, whereas eRouting attempts to deliver citywide parking information (without full participation from carpark operators yet) and MyKE is restricted to the Kowloon East district (with an area of 488 hectares), which was earmarked for pilot testing on SC projects in the Chief Executive's 2015 Policy Address.

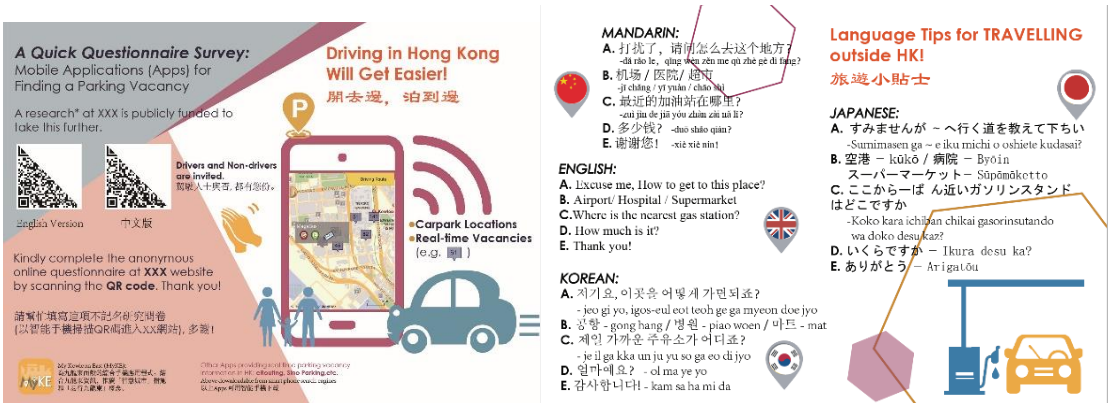
5.3 Survey design and data collection

Given the importance of mobility and the general desire of road users for smooth traffic flows in Hong Kong, a questionnaire survey targeting Hong Kong citizens as ICT end-users was undertaken to investigate their perceptions about the potential pitfalls identified. This questionnaire survey was followed up by 27 interviews with relevant stakeholders (six for information islands and 21 for digital divide) to probe further into the phenomenon, resulting in several recommendations for improving the current situation.

5.3.1 Questionnaire survey

A questionnaire survey was distributed from late June to early October 2017 to members of the public as (potential) users of smart parking systems. The questionnaire is provided under Appendix 2, Survey Questionnaire (English Version): *Mobile Application for Finding Parking Vacancy*. Part A of the questionnaire concerns the background information of respondents, and Part B collects data about (1) public expectations on smart apps for finding real-time parking vacancies, (2) their use of mobile information services, and (3) their understanding on SC.

QR codes printed on cards with traveling tips were used in this survey to distribute the questionnaires widely and increase the response rate. The codes are more convenient to share than web links and allow questionnaire responses to be captured automatically instead of requiring respondents to return completed hardcopy replies. Currently, the use of QR codes has become commonplace in Hong Kong and it facilitates various activities, such as e-payment, street-side marketing, transactions of airport express and entertainment tickets (e.g., to Disneyland and Ocean Park), and for distributing fast food restaurant menus. Hence, using QR codes does not present a problem for people in Hong Kong. A random sample of respondents was requested to complete the online questionnaire (with the options of English and Traditional Chinese formats) by scanning a QR code on a colorful survey card (Figure 5-1), designed with Asian language tips for traveling (to attract respondents).



A Quick Questionnaire Survey:
Mobile Applications (Apps) for Finding a Parking Vacancy

A research* at XXX is publicly funded to take this further.

English Version　中文版

Drivers and Non-drivers are invited.
駕駛人士與否，都有您份。

Kindly complete the anonymous online questionnaire at **XXX** website by scanning the **QR code**. Thank you!

請幫忙填寫這項不記名研究問卷
(以智能手機掃描QR碼進入XX網站)，多謝！

My Kowloon East (MyKE): [illegible]

Other Apps providing real time parking vacancy information in HK: eRouting, Sino Parking,etc.
Above downloadable from smart phone search engines
以上Apps 可用智能手機下載

Driving in Hong Kong Will Get Easier!
開去邊，泊到邊

- Carpark Locations
- Real-time Vacancies (e.g. 51)

MANDARIN:
A. 打扰了，请问怎么去这个地方？
-dǎ rǎo le，qǐng wèn zěn me qù zhè gè dì fang?
B. 机场 / 医院/ 超市
-jī chǎng / yī yuàn / chāo shì
C. 最近的加油站在哪里？
-zuì jìn de jiā yóu zhàn zài nǎ lǐ?
D. 多少钱？ -duō shǎo qián?
E. 谢谢您！ -xiè xiè nín!

ENGLISH:
A. Excuse me, How to get to this place?
B. Airport/ Hospital / Supermarket
C.Where is the nearest gas station?
D. How much is it?
E. Thank you!

KOREAN:
A. 저기요, 이곳을 어떻게 가면되죠?
- jeo gi yo, igos-eul eot teoh ge ga myeon doe jyo
B. 공항 - gong hang / 병원 - piao woen / 마트 - mat
C. 제일 가까운 주유소가 어디죠?
- je il ga kka un ju yu so ga eo di jyo
D. 얼마예요? - ol ma ye yo
E. 감사합니다! - kam sa ha mi da

Language Tips for TRAVELLING outside HK!
旅遊小貼士

JAPANESE:
A. すみませんが ～へ行く道を教えて下ちい
-Sumimasen ga ～ e iku michi o oshiete kudasai?
B. 空港 － kūkō / 病院 － Byōin
スーパーマーケット－ Sūpāmāketto
C. ここから一ば ん近いガソリンスタンドはどこですか
-Koko kara ichiban chikai gasorinsutando wa doko desu kaz?
D. いくらですか － Ikura desu ka?
E. ありがとう － Arigatōu

Figure 5-1 Survey card for case study 1 (front and back)

A pilot test was undertaken to verify the clarity of questions before the formal survey. The survey cards were then distributed via the author’s network of acquaintances in Hong Kong by applying the snowballing technique and specifying that recipients should preferably be holders of driving licenses. Besides QR codes, hardcopy questionnaires were distributed to respondents who do not commonly use smart phones, such as aged persons and occupational drivers. In total, 4,800 questionnaires (including cards with QR codes and hardcopies with full questions) have been distributed in 3 multi-story properties in the New Territories in Hong Kong, carparks in 3 educational institutes, and several offices in the public sector. In total, 793 valid replies were received, representing a response rate of 16.5%. Table 5-1 shows the key demographics of the respondents. Most respondents were drivers (82.5%) and approximately 60% of drivers had more than 10 years of driving experience. Non-drivers were also included because a section of the survey was about SC in general. The overall response rate of 16.5% is considered acceptable for mass public surveys, given the large number of valid responses (Holbrook *et al.*, 2005).

Table 5-1 Key demographics of respondents (Questionnaire Survey #2)

Demographic type	Detail	Number of respondents	Percentage
Gender	Male	595	75.0%
	Female	198	25.0%
	Total	*793*	*100.0%*
Age	18 to 30	75	9.5%
	31 to 45	282	35.6%
	45 to 60	377	47.5%
	Above 60	59	7.4%
	Total	*793*	*100.0%*
Highest education level	Primary education	24	3.0%
	Secondary education	127	16.0%
	College or diploma	110	13.9%
	University and above	532	67.1%
	Total	*793*	*100.0%*
Driving experience	Not at all (non-drivers)	139	17.5%
	Less than 1 year	33	4.2%
	1~3 years	52	6.6%

	4~10 years	95	12.0%
	More than 10 years	474	59.8%
	Total	*793*	*100.0%*

5.3.2 Semi-structured interviews

Section 3.5 of Chapter 3 provides an introduction to the semi-structured interviewing method. In this research, semi-structured interviews were conducted on stakeholders in the smart parking projects to ascertain why private carpark operators might be unwilling to release their data via an integrated platform.

It was considered that citizens with low education level and disabilities might have difficulties in reading the questionnaire. Besides that, Table 5-1 shows that few responses were obtained from females (25%) probably because male drivers are considerably more prevalent in Hong Kong. For example, 40,000 taxi drivers operate in Hong Kong, but only approximately 6,100 taxi licenses (15.25%) are owned by women (Li, 2017). To obtain a balanced view, therefore, interviewing was adopted to involve sixteen elderly females (non-drivers) with primary education and below, and five people helping disadvantaged groups (three of them were visually impaired, and one was physically disabled) to understand the situation of the excluded groups further as well as what support is needed by most by them.

5.4 Data analysis

Various statistical tools were applied in this research via the Statistical Packages for the Social Sciences, including Cronbach’s alpha reliability test, Kendall’s concordance analysis, the chi-square test of association, and Spearman’s rank correlation test.

Section 3.4 of Chapter 3 has introduced all tests. Cronbach's alpha test was conducted to evaluate the reliability of questions asking respondents to rate the importance of seven factors using a five-point Likert scale, when they were deciding whether to use a parking app. The Cronbach coefficients ranged from 0.886 to 0.912, thereby satisfying the minimum threshold level of 0.7 suggested by Santos (1999). Therefore, responses relying on the five-point Likert scale were found to be reliable and internally consistent. Kendall's coefficient of concordance (*W*) was then adopted to measure the level of agreement among respondents who rated the importance of the seven factors. The *W*-value was 0.08, which indicates a statistical relevance but a low level of agreement. The chi-square test for association was used to discover any dependence between two categorical variables, such as whether respondents worry about privacy leakage and whether they have the habit of reading privacy conditions when downloading mobile apps. Spearman's rank correlation test was performed to assess the association between demographic variables (e.g., age and education level) and the respondents' participation level in SC initiatives, and the values were converted into ordinal variables.

5.5 Key findings

5.5.1 Public understanding about the SC initiative

To ascertain the state of SC development in Hong Kong, a question was designed to assess public understanding about the SC initiative. Overall, 37.5% respondents knew nothing about SC, and even 60.3% of well-educated respondents (with a university level of education and above) had no idea about it. Approximately 13.6% heard about SC but had no interest. Moreover, 41.4% respondents were interested but uninvolved in SC. Only approximately 5% participated in the SC initiative through public forums or others. Hence, the SC concept was not yet popular among Hong Kong citizens. This finding is unsurprising because the government only started to promote SC approximately 2 years ago.

5.5.2 Use of parking apps in Hong Kong

Respondents were then asked whether they knew about any mobile apps for finding a parking vacancy in Hong Kong. Among the existing carparking apps surveyed, “W” was most known to respondent drivers (13.0%), whereas “S” was known to only 5.9%, and MyKE and eRouting were each familiar to less than 5%. This trend is probably because “W” is one of the largest and oldest private parking operators in Hong Kong with around 300 car parks distributed citywide. “S” only provides carparking information in the shopping malls and other premises that they owned. As for MyKE, 6,500 downloads were recorded among 2.2 million valid license holders as of September 2017 (Transport Department, 2017), and over half of the parking spaces in KE were reportedly covered (Energzing Kowloon East Office, 2017). The overall picture is that parking apps are not yet popular in Hong Kong, as this survey indicated that 72.8% of respondents were not aware of any. Hence, the use of parking information apps to enable smart mobility in Hong Kong remains at the initial stage.

5.5.3 System information insecurity

This study posed two questions about drivers’ decisions for using a parking app and their concerns over SCs to understand the public perception on the issue of system information insecurity. Results based on relative frequencies showed that system reliability, information accuracy, and privacy protection were ranked as the top three factors influencing respondents' decisions to use an app. These three factors accord with the most widely applicable information security model consisting of confidentiality, integrity, and availability, known as the CIA triad (Elmaghraby & Losavio, 2014). "Confidentiality" refers to privacy (stated as "It doesn't seem to leak my personal information" in the survey). "Integrity" indicates the trustworthiness of data and settings ("Its information is accurate/up to date"). "Availability" concerns the correct performance of a system for the desired purpose ("It is stable/reliable"). The respondents' emphasis on these three factors of information security reflects their concerns about SCs, because "Information insecurity (e.g. cyber-attacks, system break-down)" was a concern for a sizable portion of respondents (about 30%). System security attracts considerable attention from citizens. However, fostering such security relies on experts and relevant stakeholders. Users at the receiving end can only voice their concerns or refrain from using untrustworthy systems.

5.5.4 Personal information leakage

Personal information leakage was ranked as the top concern about SCs with 36.1% responses, indicating that citizens are worried about their privacy. The chi-square test revealed a slightly positive association (significant at 0.01 level) between their worry about personal information leakage and their behavior of reading disclaimers/conditions when downloading/installing mobile apps. Conversely, 42.6% of the respondents who expressed their worries about personal information leakage responded that they had never read disclaimers/conditions when downloading and installing mobile apps. Most mobile apps state in the conditions that users’ data would be used by the app developer for other (unknown) legal purposes or that some external/third parties can access users’ data. User ignorance of these conditions likely facilitates the possible intrusion and misuse of personal information.

Respondents were also asked about the types of information that they were unwilling to disclose when downloading or using mobile apps. Among four common information types (i.e., location, email address, phone number, and social media accounts, such as Facebook and WeChat), phone number gained the highest responses (30.9%), possibly because calling is the most instant and direct way of bothering a person. Location, however, received the least responses (19.8%). Current smart parking systems mainly rely upon users’ location information, which is conveyed through a networked infrastructure and eventually stored at a central database (Krumm, 2009). In several systems, unauthorized parties can identify users’ behavior patterns by extracting their location information during a period (Chatzigiannakis *et al.*, 2016). In combination with behavioral patterns, other information (e.g., email address, resident address, and social media account) inputs required by some systems or services can be used to identify the users. Therefore, users should be cautious about their location privacy when using mobile apps.

5.5.5 Information non-integration

Given that different apps each provide incomplete parking vacancy information in

Hong Kong, a question was asked: “Would you mind if you have to use different Apps for finding parking vacancies when going to different districts in Hong Kong?” Answers were based on a five-point Likert scale (1 = “do not mind at all” to 5 = “very much”). Around 66% of respondent drivers selected 3 and higher. This outcome indicates that users prefer a coherent platform (e.g., a single platform) that integrates citywide parking information. Existing parking apps developed by different entities provide vacancy information on their own carparks or target areas. For instance, users have to switch from “MyKE” to another app to find parking vacancies when they leave Kowloon East or use “S” when they cannot find available parking slots nearby in the “W” app. Furthermore, the candidate tried searching for parking vacancies at places that were included in some parking apps but obtained various vacancy numbers in different apps.

To ascertain why only few carpark operators were willing to share their real-time vacancy information, six face-to-face interviews were conducted with key stakeholders involved in the Hong Kong smart parking projects (Table 5-2). All interviewees participated in the smart parking projects coordinated by the Hong Kong government, and they communicated regularly with private carpark operators, who declined to be interviewed.

Table 5-2 Interviewees’ profile for information islands

Interviewee’s role	Nature of the organization	Yr. of experience
Chief technology officer	Public research institute	Over 10 years
Project Manager	Public sector	5-10 years
Project manager	Public sector	5-10 years

Senior engineer	Public sector	Over 10 years
Academic researcher	Tertiary institution	5-10 years
Vice-president for technology	Private sector (a potential data provider)	Over 10 years

Through these interviews, six major concerns of private carpark operators were identified as follows: (1) The programs cannot increase carpark operators’ benefits. (2) Expenses (e.g., for facility procurement, upgrading of legacy system, and extra manpower) mean that they must set aside extra budgets. (3) Once the apps indicate “full” in the parking information, no one would come to wait. This trend may decrease the benefits obtainable by commercial premises. (4) Disclosing carpark usage may leak business conditions. (5) They intend to develop/have others develop their own apps to acquire further profits. (6) Complicated data ownership issues may occur in an integrated platform.

5.5.6 Digital divide

5.5.6.1 Survey findings

This research examines the issue of digital divide by investigating the following: (1) the frequency and difficulty involved in citizens using current e-services or mobile services based on a five-point Likert scale and (2) their understanding of government schemes that help disadvantaged groups and their participation in the Hong Kong SC initiative. Overall, the mean score of use frequency was 3.4 out of 5, and that of difficulty level was 2.7, which indicates a general ability of using e-services or mobile services. However, 67.1% of the respondents had university-and-above education. Hence, observing how the ability of using ICTs varies with different demographic groups is necessary.

Table 5-3 Spearman's correlation test

	Age	Education level
Frequency of using e/mobile services	CC: -0.166**	CC: 0.179**
Difficulty of using e/mobile services	CC: 0.35	CC: -0.140**
Participation in SC initiative	CC: -0.003	CC: 0.140**

Note: CC: Correlation Coefficient.

**: Correlation is significant at the 0.01 level (2-tailed).

Spearman’s rank correlation coefficient (Table 5-3) showed a negative correlation between the age and frequency of using electronic/mobile services, with a significance level of 0.01. No correlation appeared to exist between the age and difficulty of using these services because the correlation coefficient (0.347) was insignificant at any threshold (i.e., p = 0.01, 0.05, 0.1). Thus, older respondents used less electronic/mobile services and hence did not have much experience on the difficulty. For another demographic parameter, a positive correlation was found between the education level and frequency of using e-services or mobile services, which was statistically significant at 0.01. Conversely, a negative correlation existed between the education level and difficulty of using e-services or mobile services, which was also statistically significant at 0.01. Therefore, the more educated people were, the more often they used mobile apps and found less difficulty in using these services, whereas the less educated used less e-services or mobile services and found difficulty in using them. This finding was echoed by the results of the chi-square test, which indicated that respondents with lower education levels were more concerned with their lack of ability to use advanced information technologies in SCs than those with higher education levels. This research also found a positive correlation between the education level and participation in the SC initiative with a significance level of 0.01. Therefore, poorly educated groups were practically excluded from the SC development in terms of using smart services and understanding the initiative.

5.5.6.2 Interview Findings

Sixteen interviews on the elderly and poorly educated people were conducted during several community workshops and events from September to October 2017, each lasting around 30 min. Most of the female interviewees were aged between 61 and 70, and three were 71 and above (Table 5-4). Fourteen interviewees owned touch screen smartphones, and only two used “dumbphones,” which cannot operate advanced services. The interviewees seldom used electronic devices/services (e.g., electronic map and online banking) except for contacting their acquaintances by calling or sometimes chatting and sharing photos via WhatsApp. They felt uneasy in using current electronic devices due to: (1) poor eyesight for reading computer and phone screens, (2) difficulties in following interactive voice responses, and (3) poor digital literacy. Although 11 interviewees had heard about trainings and workshops offered by their community centers and relevant organizations, only three of them had participated once without completing the activities. Some non-participants considered attending such training unnecessary as they often asked for help from their family members, friends, and in-person services when encountering difficulties in using electronic services/devices. Such workshops were not perceived as useful by participants and non-participants. The digital divide among these interviewees concerns the abilities and benefits of using ICTs rather than their physical accessibility. Although this group may have a relatively lower need for electronic services/devices in their daily life than the younger and better educated groups, cultivating their IT literacy before city services are further digitalized would be beneficial. IT training for the elderly must be grounded and diversified by, for instance, teaching them how to navigate through interactive maps and reading online daily news to enhance their mobility and life quality.

Table 5-4 Interviewees' profile for digital divide issues
(less-educated senior people)

Demographic	Type	Number of respondents	Percentage
Gender	Female	16	100%
Age	45 to 60	3	18.75%
	61~70	10	62.50%
	Above 71	3	18.75%
	Total	*16*	*100%*
Highest education level	Primary education	15	93.75%
	Secondary education	1	6.25%
	Total	*16*	*100%*
Whether using a smartphone	Yes	14	87.5%
	No	2	12.5%
	Total	*16*	*100%*

Besides the elderly and poorly educated people, other disadvantaged groups who may suffer from the digital divide include those with visual, physical, and hearing impairments. The Office of the Government Chief Information Officer (OGCIO) has helped develop several schemes, such as Web/Mobile App Accessibility, to instigate current advances available for all, as well as promote a series of assistive technologies for people with disabilities, such as touchscreen text input applications for the visually impaired and intelligent homes for people with physical disabilities. However, 67.8% of the survey respondents did not know of any group being helped by the government in the use of IT. Most respondents might not be disadvantaged themselves, but society awareness about supports being provided to the disadvantaged groups within the SC trend should exist if such initiatives were practiced widely. Interviews were conducted with five people helping disadvantaged groups in Hong Kong to learn further about how disadvantaged groups fare amidst technological advancements (Table 5-5). Three of them were visually impaired, and one was physically disabled.

Table 5-5 Interviewees' profile for digital divide issues

(people helping disadvantaged groups in Hong Kong)

Interviewee's role	Nature of the organization	Yr. of experience
Chief manager (Physically disabled)	NGO	Over 10 yrs
Founder (Visually impaired)	Private sector	5-10 yrs
Director	NGO	Over 10 yrs
Chief manager (Visually impaired)	NGO	Over 10 yrs
IT developer (Visually impaired)	Private sector	Over 10 yrs

Some interviewees thought that the provision of basic IT training and education would be effective for arousing the learning interest of the excluded groups. However, numerous current community training programs for the disadvantaged people were outdated, with some only teaching basic life skills, excluding ICT use. An interviewee suggested keeping in-person services in the long run at some common places that also provide electronic services, such as underground stations and banks. This recommendation was presented because a certain portion of people would always be unwilling or unable to use electronic/mobile services. Moreover, although the government developed several platforms or apps to help the disadvantaged, maintaining and updating these facilities further and involving additional efforts from the private sector were important.

5.6 Summary

The first case study focused on the public use of mobile apps. Part of the data was collected through Questionnaire Survey #2 to investigate how users perceived these pitfalls within the context of mobile apps providing real-time parking information. It was found that the SC concept was not yet popular among Hong Kong citizens. System insecurity and privacy leakage were found to cause concern among the app users, but their awareness regarding protecting personal data leaves much room for improvement. Lack of collaboration among private carpark operators resulted in islands of real-time parking information. Separate interviews indicated that the digital divide existed widely among disadvantaged groups and that the problem cannot be solved by mere provision of ICT facilities but also hands-on training and special care for these groups. Overall, technologies alone cannot render a city smart or smarter. Using ICTs to serve all citizens that matter is a suitable way. This chapter extends the importance of this study by examining the pitfalls within the context of mobile apps from the perspective of Hong Kong citizens. From the analysis, pitfalls regarding the safe use of smart services and the lack of competence in harnessing smart devices, such as personal privacy leakage and the digital divide, are highlighted as being more prevalent than expert/practitioner-oriented issues, including system information insecurity and information islands. Therefore, in the next two chapters, pitfalls of system unreliability and information islands are examined further (particularly their rationale) from different perspectives rather than those of users.

CHAPTER 6 RELIABILITY ANALYSIS OF A SMART PARKING INFORMATION SYSTEM (SPIS)

6.1 Introduction

The previous chapter investigated how users perceived the potential pitfalls within the context of mobile apps that provide real-time parking information. It revealed that system insecurity became an important concern for citizens. However, a further analysis regarding the reliability of IT systems has more to do with experts than users at the receiving end. Therefore, this chapter presents the second case study, which contextualizes information insecurity within a smart parking information system (SPIS) due to its relevance in the ongoing global development of SCs. Multiple methods, including interviews and fuzzy fault tree analysis (FFTA), were employed to analyze the configuration and reliability of an SPIS. This chapter is structured as follows. Section 6.2 briefly reviews the concept of system reliability and describes suitable methods for analyzing such reliability. Section 6.3 presents the reliability analysis and the related results. Section 6.4 concludes the chapter by offering recommendations for improving system reliability. The data collection and analysis performed in this chapter have been extracted from a manuscript submitted to a refereed journal (see footnote below) for possible publication [4].

[4] Ma, R., Lam, P. T., & Leung, C. K. (2018). A reliability analysis of a smart parking information system: The case of Hong Kong. *Computers & Security* (undergoing the first review in August 2018).

6.2 Reliability analysis of ICT systems

Security has been largely ignored in previous studies, most of which have focused on the performance, stability, and robustness of physical systems (Ashibani & Mahmoud, 2017). The cybersecurity risks in SCs can be attributed to (1) the vulnerability of advanced Internet-based technologies and a "smartly" upgraded infrastructure to hacking and (2) the insecurity of the data collected and processed through such technologies and infrastructure (Kitchin & Dodge, 2017). These risks are closely related to each other as unauthorized access to data may occur owing to the inherent weaknesses of a system (Kitchin & Dodge, 2017). Therefore, information security problems converge toward system reliability. As a quality attribute, reliability refers to "*the probability that an item will perform a required function without failure under stated conditions for a stated period of time*" (Cardon, 1996). This attribute may also pertain to the performance of physical systems, such as electronic devices and construction equipment, and to the effectiveness of services systems, such as healthcare and banking systems (Gunes & Deveci, 2002). Reliability analysis is often conducted by determining failure rates. This type of analysis also requires a thorough understanding of the functional interdependency among several components and their associated failure modes (Mahmood *et al.*, 2013). FFTA was conducted in this study to identify those basic events that result in system failure and to determine their probabilities of occurrence. The rationale for choosing this method and the analysis process are discussed in detail in Section 3.6 of Chapter 3 (Methodology).

6.3 Reliability analysis of the SPIS (Case study 2)

Finding a parking space in Hong Kong is a common problem for drivers. A previous report shows that most incidents of traffic congestion in Hong Kong are caused by vehicles looking for parking spaces (Transport Advisory Committee, 2014). Apart from bringing inconvenience and inefficiency, looking for parking spaces also leads to air pollution and fuel wastage (Tasseron & Martens, 2017). Smart mobility has become an active area where various ICTs are used to facilitate the movement of pedestrians and vehicles around cities (Shin & Jun, 2014). One initiative is to help drivers find parking spaces by making real-time parking vacancy data accessible to the public (Hong Kong Innovation and Technology Bureau, 2017). Many existing SPISs are already in operation around the world, but Hong Kong has only started using such technology in the past two years. Given the unavailability of data related to the actual failure rates of an SPIS, FFTA was performed (1) to identify the basic events that could lead to service failure in an SPIS and analyze how service unavailability can occur in different ways; (2) to determine the occurrence probabilities of the identified basic events; and (3) to assess the overall reliability of an SPIS. An importance degree analysis was also performed to rank those factors that could lead to service unavailability and to provide useful insights for formulating effective mitigation measures.

6.3.1 General configuration of the SPIS

By conducting five interviews with stakeholders who were directly involved in smart parking projects (see their profiles in Table 6-1), a generalized configuration of an SPIS is laid out as shown in Figure 6-1.

Table 6-1 Profiles of the interviewees for the SPIS configuration

Occupation	Organization	Work experience
Engineer	Public sector	5-10 years
Project manager	Public sector	5-10 years
Chief researcher in IoT	Academic	5-10 years
Technical staff for information security	Academic	Over 10 years
Chief technology officer	Private research institution	Over 10 years

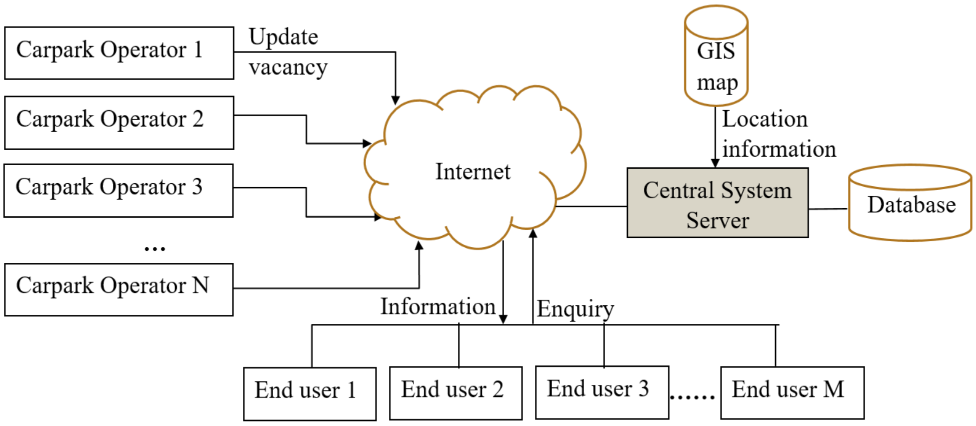


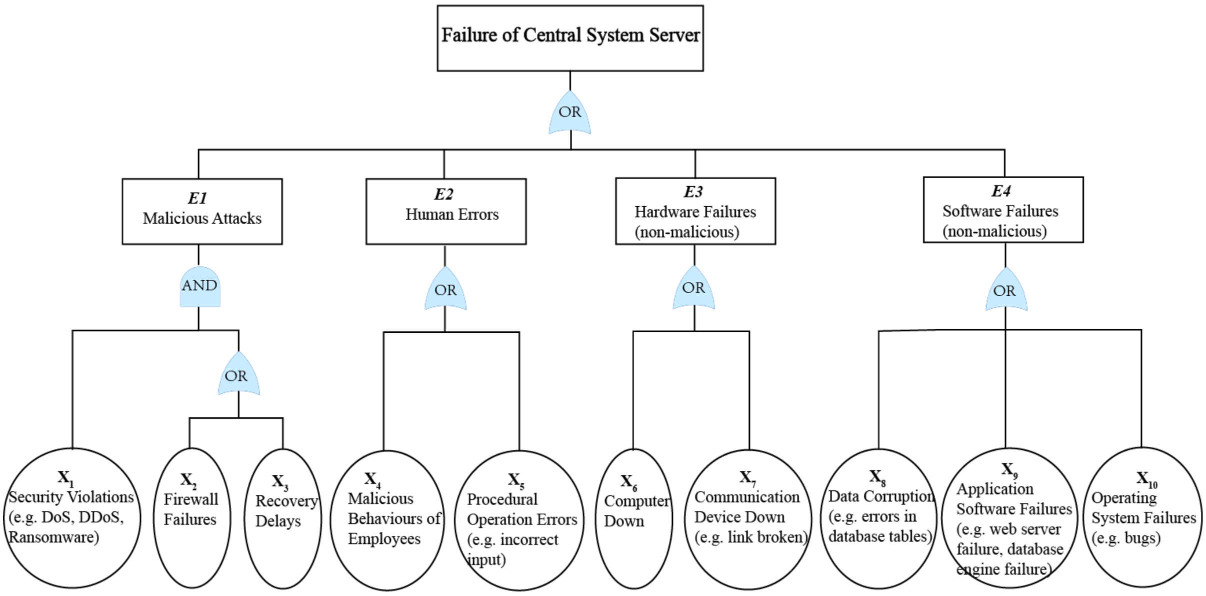
Figure 6-1 General configuration of an SPIS

In most SPISs, the parking server (commonly known as the “central server”) is the core component of the system that stores, manages, and disseminates parking information, including real-time vacancy data received from carparks and static data, such as location, opening hours, and charges. End users obtain parking information by using their Internet-connected devices. Carpark operators update their data on the number of parking space vacancies either manually or automatically. The manual approach allows carpark operators to update vacancy numbers by using a web application, while the automatic approach is realized via a periodic communication between the server of carpark operators and the parking central server without the need for human intervention. Although carpark operators may use different technologies, such as IoT and RFID, to update vacancy information based on their affordability and other factors, their selected technology does not change the overall structure that is meant to outline the communication among major components, such the central sever, computers at carparks, and the devices of users.

6.3.2 Building the fault tree for the SPIS

As shown in Figure 6-1, the failures at the side of the central parking server, the Internet, and individual carparks may lead to the malfunction of an SPIS. However, this case study focuses on the central server due to its criticality and for three other reasons. First, the reliability of citywide Internet depends on a broad range of complex factors, such as natural disasters and quality of regional infrastructures. Second, it is unlikely that malfunctions happen in all carparks at the same time so that the parking vacancy information city-wide becomes unavailable. Third, assessing the failure probability of hundreds of carparks operated by various hardware and software is impractical. Therefore, in this study, the failure in the central system server is identified as the top event.

Based on a review of technical references (Pertet & Narasimhan, 2005; Kitchin, 2016) and consultations with five stakeholders (see Table 6-1), the failure in the central system server (as the top event, TE) was resolved into four intermediate events, including malicious attacks, human errors, hardware failures, and software failures, all of which are connected by an OR gate. These four intermediate events were broken into 10 basic events as shown in Figure 6-2. Event X_1 (security violations) can only lead to a server failure when X_3 (recovery delays) or X_2 (firewall failures) occurs. Similarly, the basic events under human errors, hardware failures, and software failures can independently trigger a central server failure.



Failure of Central System Server
OR
E1
Malicious Attacks
AND
OR
E2
Human Errors
OR
E3
Hardware Failures (non-malicious)
OR
E4
Software Failures (non-malicious)
OR
X1
Security Violations (e.g. DoS, DDoS, Ransomware)
X2
Firewall Failures
X3
Recovery Delays
X4
Malicious Behaviours of Employees
X5
Procedural Operation Errors (e.g. incorrect input)
X6
Computer Down
X7
Communication Device Down (e.g. link broken)
X8
Data Corruption (e.g. errors in database tables)
X9
Application Software Failures (e.g. web server failure, database engine failure)
X10
Operating System Failures (e.g. bugs)

Figure 6-2 Fault tree of failures in the central server of the SPIS

6.3.3 Qualitative analysis

6.3.3.1 Obtaining minimum cut sets (MCSs)

The fault tree of failure in the central system server of the SPIS can be interpreted as:

$TE = E_1+E_2+E_3+E_4 = (X_1X_2) + (X_1X_3) +X_4+X_5+X_6+X_7+X_8+X_9+X_{10}.$

The above simplification yields the following nine MCSs:

$MCS_1= \{X_1, X_2\}$; $MCS_2= \{X_1, X_3\}$; $MCS_3= \{X_4\}$; $MCS_4= \{X_5\}$;

$MCS_5= \{X_6\}$; $MCS_6= \{X_7\}$; $MCS_7= \{X_8\}$; $MCS_8= \{X_9\}$; $MCS_9= \{X_{10}\}$.

Therefore, nine combinations can potentially cause the top event “failure in central system server.” For instance, MCS_1 shows that the simultaneous occurrence of events

X_1 (security violations) and X_2 (firewall failures) can result in the unavailability of an SPIS due to malicious attacks.

6.3.3.2 Structure importance (SI) analysis

A SI analysis is conducted based on Eq.3-7 in Chapter 3 (Methodology). The SI of events 1 to 10 is obtained as follows:

SI (X_1) = SI (X_4) = SI (X_5) = SI (X_6) = SI (X_7) = SI (X_8) = SI (X_9) = SI (X_{10}) = 1;

SI (X_2) = SI (X_3) =0.5.

This result implies that events X_2 (firewall failures) and X_3 (recovery delays) are relatively less important than the other events in terms of their structure. Unlike events X_4 to X_{10} that may independently trigger the top event, events X_2 and X_3 can only trigger the top event in combination with event X_1 (security violations).

6.3.4 Quantitative analysis

A questionnaire survey was conducted from August 2017 to November 2017 among experts in the domains of IT and electronic engineering. These experts were invited to rate the occurrence likelihood of events identified (X_1 to X_{10}) by giving their linguistic judgments, i.e., “very low,” “low,” “medium,” “high,” and “very high”. A sample of the questionnaire can be found in Appendix 3 (*Questionnaire Survey #3: Reliability analysis of the smart parking information system*). This questionnaire includes (1) a brief introduction of an SPIS and its configuration (Fig. 6-1) to ensure that all responses target the same system, (2) questions about the background information of the respondents; and (3) an assessment of the failure probability of the identified events in the form of linguistic expressions. Before the formal survey, a pilot test was conducted among in-house IT personnel to confirm that all questions are clear and understandable. Among the 112 questionnaires sent via email and post in Hong Kong, 34 valid replies were obtained on or before the cut-off date. It was realized that some experienced IT/electronic people may know little about SPIS which is relatively new in Hong Kong, but they could still evaluate the relative rates of occurrence of individual component failures (such as server failures). Therefore, only those respondents who have limited IT working experience (less than two years) and indicated that they know little about an SPIS were excluded from the analysis. Finally, the responses of 22 experts from heterogeneous organizations and work backgrounds (whose profiles are presented in Table 6-2) were elicited for the FFTA. This sample size is larger than those used in existing studies (Lavasani *et al.*, 2015; Senol *et al.*, 2015; Cheliyan & Bhattacharyya, 2017).

Table 6-2 Key background information of selected experts for FFTA

Background information	Type	Number of respondents	Percentage
Education level	University and above	22	100%
Type of organization	Public sector or related organization	14	63.7%
	Private sector	5	22.7%
	Non-Government Organization	3	13.6%
	Total	*22*	*100%*
Nature of work	Technology development/engineering	11	50.0%
	IT Project management	2	9.1%
	Consultancy/advisory	2	9.1%
	Academic	7	31.8%
	Total	*22*	*100%*

Working experience in info tech and electronic engineering	Less than 2 years	3	13.6%
	2-4 years	7	31.8%
	5-10 years	4	18.2%
	Over 10 years	8	36.4%
	Total	*22*	*100%*
The level of knowing about SPIS	Having some knowledge about it	19	86.4%
	Knowing it very well	3	13.6%
	Total	*22*	*100%*

6.3.4.1 Obtaining the occurrence probabilities of the basic events and the top event

The 22 experts were assigned with weights determined by (1) their working experience in the domains of IT and electronic engineering and (2) their knowledge of SPIS. The weighting criteria are given in Table 6-3.

Table 6-3 Expert weighting determining criteria

Criterion	Classification	Weighting score
Working experience in info tech and electronic engineering	Over 10 years	4
	5-10 years	3
	2- 4 years	2
	Less than 2 years	1
The level of knowing about SPIS	I know it very well.	2
	I have some knowledge about it.	1

Based on Eqs. 3-9 to 3-14 in Chapter 3, all ratings given by the 22 experts for each event were aggregated into a trapezoidal fuzzy number that was then transformed into fuzzy failure probability (FFP) after de-fuzzification as shown in Table 6-4. The top four basic events with the highest occurrence probability are X_5 (procedural/operation errors), X_1 (security violations), X_4 (malicious behaviors of employees), and X_3 (recovery delays). This result is consistent with the recent rapid increase in the number of cyber-attacks and the fact that security is being treated as an afterthought.

Table 6-4 Failure probability of the basic events

Basic event (X_i)	Aggregated fuzzy set (A_i): a, b, c, d	FPS (fuzzy probability score)	FFP (fuzzy failure probability)	Rank
X_1	0.2712, 0.4248, 0.4680, 0.6264	0.45449	0.00359	**2**
X_2	0.2448, 0.3448, 0.5048, 0.6256	0.43581	0.00311	7
X_3	0.2784, 0.4420, 0.4420, 0.6056	0.45015	0.00347	**4**
X_4	0.2552, 0.3900, 0.4980, 0.6448	0.45297	0.00355	**3**
X_5	0.2664, 0.4156, 0.5020, 0.6608	0.46594	0.00391	**1**
X_6	0.2440, 0.3532, 0.5244, 0.6552	0.44892	0.00344	6
X_7	0.2432, 0.3680, 0.5120, 0.6528	0.44970	0.00346	5
X_8	0.1728, 0.3080, 0.4160, 0.5632	0.38113	0.00197	8
X_9	0.1696, 0.2968, 0.4120, 0.5520	0.37376	0.00185	9
X_{10}	0.1608, 0.2820, 0.4260, 0.5632	0.37338	0.00184	10

The occurrence probability of the top event can be obtained as follows by using Eq.3-15 or Eq. 3-16 in Chapter 3:

P (TE)=1-(1-P1P2) (1-P1P3) (1-P4) (1-P5) (1-P6) (1-P7) (1-P8) (1-P9) (1-P10) = 0.0198.

This probability indicates that the operational reliability of such a system is 98.02%. This figure takes human errors into account as an independent attribute. The evaluation is based on the perceptions of knowledgeable respondents instead of historical statistics, which are yet to be collected over a long-term use of the SPIS. Most of the available statistics on system reliability mainly include the failure frequency of physical components (e.g., hard drives) that are obtained by conducting ex-factory machine tests, which do not take into account non-technological factors such as human errors. A server requires a power supply, software updates, and other maintenance operations. As revealed in this study, many factors may contribute to the unavailability of a server. According to Clapp (2010), a 98.0% reliability yields a downtime of 7.3 days per annum for a single central server. This percentage is acceptable in the context of an SPIS, especially when back-up servers are installed to provide redundancy (hence increasing reliability), subject to budget allowances of capital and operating costs. After analyzing the importance of the contributory basic events enumerated below, this study proposes some target measures for mitigating system unavailability.

6.3.4.2 Importance analysis of basic events

Table 6-5 shows the results of the importance analysis. Basic events X_5 (procedural/operation errors), X_4 (malicious behaviors of employees), X_7 (communication device down), and X_6 (computer down) have high probability importance (PI), thereby suggesting that the changes in their occurrence probability will influence that of the top event. In this sense, reducing the occurrence probability of human errors and hardware failures can significantly reduce the occurrence probability of a central server failure. However, the ranking for critical importance (CI) is different because this ranking considers both occurrence probability and PI. Basic events X_5 (procedural/operation errors), X_1 (security violations), X_4 (malicious behaviors of employees), and X_7 (communication device down) have a great direct influence on the occurrence of central server failure. Although X_1 (security violations) has a relatively low marginal influence (determined by PI) on central server failure, its high occurrence probability increases its direct effect on central server failure.

Table 6-5 Importance analysis of the basic events

Basic Event	Probability Importance (PI)	Rank	Critical Importance (CI)	Rank
X_1	0.97372	6	0.17574	**2**
X_2	0.00352	9	0.00055	10
X_3	0.00352	9	0.00061	9
X_4	0.98362	**2**	0.17549	**3**
X_5	0.98397	**1**	0.19352	**1**
X_6	0.98351	**4**	0.17014	5
X_7	0.98353	**3**	0.17116	**4**
X_8	0.98207	5	0.09759	6
X_9	0.98195	7	0.09140	7
X_{10}	0.98194	8	0.09109	8

6.4 Preventative measures against a central server failure in the SPIS

The failure of a SPIS may trigger several problems, including a rise in the number of cruising vehicles at the city scale, thereby setting off a chain reaction and consuming unnecessary resources. Apart from increasing carbon emissions, traffic congestion may bring inconvenience, reduce productivity, and prevent life-saving teams from reaching emergency sites. Solutions must be developed from different aspects to improve system reliability. The CI analysis provides effective suggestions for mitigating system breaches. The order of solving basic event problems may be obtained according to the following ranking as shown in Table 6-5: X_5 (procedural/operation errors), X_1 (security violations), X_4 (malicious behaviors of employees), and X_7 (communication device down).

Events X_5 (procedural/operation errors) and X_4 (malicious behaviors of employees) are human errors with extremely high failure probability, probability importance, and critical importance. The 2018 IBM X-Force Threat Intelligence Index showed that employee errors increased the misconfiguration of cloud servers by 424% in 2017. The devastating breaches caused by human errors in 2017 included the data breach of Australian Broadcasting Corporation, the power failure of a data center belonging to British Airways, and the massive outage of Amazon web services. Specifically, the IT outage of British Airways resulted in the cancellation of over 400 flights in a single day that left 75,000 passengers stranded and costed the company USD 112 million (Patrizio, 2017). Software-based systems have been proposed to replace traditional hardware-based platforms to address human errors that may accompany any complex manual task. However, this idea is still at the initial stage given the lack of a standard and clear blueprint on how to migrate to a highly automated network (Doyle, 2017). Apart from strict technical monitoring and management regulations to avoid insider attacks by employees (X_4), some effective measures for mitigating human errors include stipulating a well-defined security policy (such as preventing employees from accessing external websites and connecting their personal USB drives) and launching regular training programs for employees. An organization can enhance its defenses against cyber risks by instilling a security mindset into its people and by granting them the necessary skills (Sparapani, 2016). However, even the best-trained people may still commit procedural/operation errors (X_5), especially when they are in a rush or if they are in an exhausted state. Therefore, a recovery plan, a good operational governance for the staff, and a regular maintenance of each piece of equipment are necessary (Bigelow, 2011).

X_1 (security violations) has the second highest critical importance. According to a study of IBM and Ponemon Institute (2017) on the cost of data breaches, malicious attacks have higher costs compared with other incidents, such as system glitches and negligence. Security violation is an unpredictable external factor that cannot be entirely mitigated by planning. However, this violation only occurs as a result of firewall failures or recovery delays. Although the probability importance and critical importance of firewall failure and recovery delays are relatively low, mitigating their occurrence can effectively enhance the defense of the central system server against malicious attacks. Firewalls are used to restrict access based on pre-determined rules. Rule review can improve the effectiveness of the firewall policy by implementing broad access rules and a set of narrowly defined access rules (FireMon, 2016). In case of a breach, instant and effective responses are needed to limit the damages caused by the incident and to isolate the affected components. Apart from technical solutions, the recovery plan must clearly outline the division of responsibilities (i.e., who takes on which role). Regular drills of responding to hacking incidents must also be conducted by the operation entities of important citywide systems. Given that the skills of criminals are continuously evolving, the risk of breach will remain regardless of how many security solutions and policies are in place (Chouffani, 2016). System managers must also remain alert to potential criminal activities by renewing their recovery plans. Other effective technological solutions against security violations include deploying security by design, strong encryption, all-site backing up of data, and up-to-date anti-virus scanning.

Hardware failures (i.e. computer down and communication devices down) were highlighted in the importance analysis. The result that hardware failures were more likely to occur than software failures might be explained by the fundamental differences in the nature of these failures. A software system is not supposed to become less reliable as time goes on. However, the failure rate of hardware systems follows a bathtub curve distribution. Material aging and deterioration can also lead to failures even though the hardware system is not deployed into service (Chinnaiyan & Somasundaram, 2010). In this sense, system downtime cannot be entirely avoided. As an alternative, system managers can plan and prepare for such problems. Highly reliable technologies cannot entirely prevent servers from encountering failure but can help some servers to continue running despite the occurrence of faults (Bigelow, 2013). Therefore, dealing with the occurrence of server faults is more important than purchasing reliable machines for preventing these faults. The use of redundant power supplies and standby systems also ensures a favorable performance without disrupting the system service when one power supply or server fails (Bigelow, 2013).

6.5 Summary

System reliability is a quality attribute of information security that has been investigated within the context of an SPIS given the lack of empirical studies on information insecurity in the SC domain. The FFTA, aided by in-depth interviews with experts, revealed that the failure of the central system server of an SPIS may be caused by malicious attacks, human errors, and hardware and software failures. Ensuring a good operational governance, improving firewalls, renewing recovery plans against rampant malicious attacks, and reducing human errors by launching training programs have been proven to be necessary and effective in mitigating these problems. Although system downtime is inevitable, its occurrence can be reduced by launching proactive solutions, such as backing up their data and by providing redundant servers and power supplies. In sum, employing an integrated approach is necessary to mitigate system unreliability. The following chapter examines another pitfall, namely, information islands, by investigating the interrelationships among stakeholder-associated barriers in an open data project.

CHAPTER 7 SOCIAL NETWORK ANALYSIS (SNA) OF BARRIERS FACED BY STAKEHOLDERS IN OPEN DATA DEVELOPMENT

7.1 Introduction

In Chapter 4 ("*Potential Pitfall Identification and Evaluation*"), the rankings of possible causes of information islands and preventative/mitigation measures did not achieve a statistically remarkable agreement in the respondents' given scores. Such outcome is partly because the problem of information islands arises from management and planning slacks instead of being technological in nature. This chapter, therefore, investigates the barriers in the drive toward open data, which is the key for bridging information islands in emerging SCs. Literature review on the barriers of building open data (Section 7.2.2 in this chapter) indicates that barriers were often interrelated, and they produced chain effects to trigger conflicts and resistance. Therefore, social network analysis (SNA) was adopted in this case study to: (1) identify the barriers faced by different stakeholders in developing a citywide open data platform, which is often conducted for SCs, and (2) investigate the complex interdependencies among these identified barriers. Hong Kong was selected as a representative case due to its relatively low rank (24th) in the Global Open Data Index, with its slow progress in opening up data for citizen use and poor data quality. Section 7.2 introduces the movement toward open data in SCs and reviews the barriers hindering open data adoption. Section 7.3 examines the status of current open data development in Hong Kong. Sections 7.4 and 7.5 present the application of SNA in an open data project in Hong Kong and the subsequent findings. Sections 7.6 and 7.7 propose effective mitigation measures against the barriers and summarizes the chapter, respectively. Data collection and analysis performed in this chapter have been extracted from a manuscript submitted by the candidate to a refereed journal for possible publication[5].

7.2 Development of open data

7.2.1 Movement toward open data

Open data is defined by Open Knowledge International (2015) as "*data that can be freely used, re-used and redistributed by anyone for any purpose.*" This commonly-used definition describes openness in terms of accessibility, re-use, and wide participation. The movement toward open data resulted from the global trend of SC development. Such movement aims to make government data and other data readily accessible and usable by the public and other entities, thus to improve government transparency, motivate citizen participation, and unlock enterprise innovations (Harrison *et al.*, 2012; Gascó-Hernández *et al.*, 2018). Different groups can benefit from the use of open data. For example, open data enhances citizens' life quality by offering information about public facilities and services, such as bus arrival times, locations of nearby restaurants, and real-time parking vacancies (Kalampokis *et al.*, 2011). For city managers, open data provides them substantive evidence as the basis of decision-making (Arzberger *et al.*, 2004; Janssen *et al.*, 2012).

[5] Ma, R., Lam, P. T. (2018). Investigating the barriers faced by stakeholders in open data development: A study on Hong Kong as a "smart city". *CITIES* (under the second review in September 2018).

One of the main derivatives of the open data initiative is government data portal, which enables people to obtain government data covering a broad range of public services, including transport, health care, and the environment (Weerakkody *et al.*, 2017). Public sector information (PSI), as the main body of open data, helps achieve open governance (Kučera *et al.*, 2013) and has been regarded as a tool against government corruption (Linders, 2013). PSI increases government transparency and renders public departments accountable to the community (Janssen, 2011). The development of open data also boosts economic growth (Jaatinen, 2016). The European Commission estimated that the effective reuse of PSI can generate a sizeable economic value of up to 40 billion euros (European Commission, 2011). In all, open data can nurture a lively ecosystem wherein innovative products and services with economic and social benefits are created by various entities (Abella *et al.*, 2017).

7.2.2 Barriers of building open data

Numerous barriers impede the development of a citywide open data platform and the fulfillment of its potential. Barriers include aspects of technology, policy, economy, legislation, institution, and culture (Conradie & Choenni, 2012; Attard *et al.*, 2015). These barriers have been categorized into five types: legal and licensing, technical and operational, use level, institutional and governance, and economic. This categorization was developed on the basis of the study of Barry and Bannister (2014) and Janssen *et al.* (2012). The "legal and licensing" aspect covers privacy, policies/regulations, and ownership. "Technical and operational" issues mainly involve data quality, supporting infrastructure, and operational difficulties. The "use level" group is related to user abilities, incentives, and participation. The “institutional and governance” aspect concerns (risk-averse) culture, governmental structure, and stakeholder relations. The “economic” group is about expenses and profits. These five categories encompass the main barriers obstructing the adoption of open data from launching, through operation, to use.

Although several studies identified possible barriers of open data adoption, a deep understanding of the underlying processes pertaining to these barriers remains lacking (Conradie & Choenni, 2014). The barriers in the open data project are often interrelated and do not stand alone (Janssen *et al.*, 2012). They can produce chain effects to trigger conflicts and resistance (Mok *et al.*, 2017). What is more, technology adoption and development may be heavily influenced by the decisions of human agents (Orlikowski, 2000). Institutional or other human-related factors may enable or constrain the adoption of open data (Janssen *et al.*, 2012). A study on understanding stakeholders in a Chilean open government data project (Gonzalez-Zapata & Heeks, 2015) proved the usefulness of stakeholder analysis in the domain of open data by identifying stakeholders’ difference in incentives and capabilities. In open data development, the role of various stakeholders during the opening process should be handled properly (Janssen *et al.*, 2012); otherwise, it would pose challenges regarding accountability. Therefore, a study is needed to analyze the interrelationships among barriers from different stakeholders’ perspectives.

7.3 Background of open data in Hong Kong (Case study 3)

An open data platform for public and private entities was ideally expected to facilitate Hong Kong's SC blueprint (Tang, 2017). The open data initiative in Hong Kong was launched by the Office of the Government Chief Information Officer (OGCIO) in 2011 to provide PSI freely in digital and machine-readable format through the central PSI portal (*data.gov.hk*) as a one-stop platform. Most of the data available in the portal had been previously released by different departments on their own websites. As of April 2017, 7000 datasets with over 730 application programming interfaces (APIs) were released in 18 categories as provided by various bureaus/departments (B/Ds), public bodies, and private organizations. In 2018, a small portion of data has been geo-referenced. Such data include the locations of clinics registered under the Medical Clinics Ordinance, the locations of electric vehicle charging stations, and the average domestic household sizes classified by district. A parallel open data platform, namely, Data Studio Portal (*http://datastudio.hkstp.org/*), was launched by the Hong Kong Science and Technology Park in February 2017 to provide APIs for public use. This initiative was particularly intended for innovation and technology companies and start-ups to develop SC solutions. The Data Studio Portal was construed as a proof of concept and contributes to *data.gov.hk* by supplementing additional data (e.g., convenience store locations, supermarket daily prices, and crime spot records) from private entities.

Despite the aforementioned efforts, Hong Kong ranked only 24th in the Global Open Data Index (Open Knowledge International, 2016). The government spent HK$1.2 million in developing the PSI portal and an estimated HK$ 0.8 million for maintaining the portal from 2015 to 2016. By May 2018, over one-third of 71 governmental B/Ds did not provide data to the portal. Only two of the city's four major transport operators contributed data to the portal (Kao, 2018). One of the barriers of opening up data in Hong Kong is the reluctance of private entities to contribute to the Big Data environment, as identified in a consultant study for Hong Kong's Smart City Blueprint by PwC (2017). Similar to real-time parking vacancy data, this problem also exists in the opening of public bus operation data, as franchised bus companies in Hong Kong are not owned by the government (PwC, 2017). Therefore, the government has been criticized for being slow in opening up data for public use. Besides data insufficiency, other problems exist, including poor data quality (e.g., unclear schemas for datasets and non-reusable data format), problematic terms and conditions for data use, and a lack of public engagement (Edmunds, 2015). Overall, Hong Kong lags in the open data movement worldwide; as Edmunds (2015) who is Coordinator of the Open Science Working Group in Hong Kong once stated, *"while governments around the world are realizing greater policy review through scrutiny, supporting greater civic engagement, and realizing better efficiency by supporting Open Data, the government's revamp policy demonstrates that the Hong Kong government is just catching up with the past trends to publish government information data."*

7.4 Data collection for SNA

SNA, given its powerful functions for identifying and visualizing interdependencies among a set of factors and exploring the implications of identified relationships (Wasserman & Faust, 1994), was applied in this research to investigate the interrelationships among the barriers faced by different stakeholders in the open data project. Section 3.7 of Chapter 3 presents the rationale for selecting this method and the detailed process of analysis (Methodology). Data to be collected include (1) key participants in this open data project, (2) barriers relevant to each stakeholder, and (3) interdependencies among the barriers. Interviews were conducted with key participants to gather data for SNA. The key stakeholders identified include: the project initiator (i.e., the OGCIO in this case) (S1); data providers from the public sector (S2), the private sector (S3), and NGOs (S4); and data users (S5). The OGCIO serves as the coordinator to promote and support B/Ds in opening up PSI and to maintain close communication with different stakeholders, including industry players, professional groups, and the academia. Internet service providers were not included in this study, as access to the numerous competitive commercial operators by users and data providers is not a problem in Hong Kong.

Interviewees were selected in the light of the principle of stakeholder-based sampling because this research aims to identify barriers of open data development from the perspective of different stakeholders. The representation of five comprehensive stakeholder groups should avoid biased judgments. Eighteen face-to-face interviews were conducted from September 2017 to January 2018 in Hong Kong (each lasting 1–2 h), along with two written replies received in lieu of interviews. Table 7-1 shows the profile of interviewees and respondents. All interviewees had university-and-above education level as open data is for value-adding redevelopment, which is often conducted by knowledgeable people. In particular, data providers were senior managers and technology developers, with direct involvement in the development of the open data platform in Hong Kong. The group of open data users consisted of experienced mobile app developers, chief information managers, and senior researchers.

Table 7-1 Profile of interviewees and respondents for SNA

Demographic	Type	Number	Percentage
Highest education level	University and above	20	100%
Type of organization	Public sector or related organization	9	45%
	Non-government organization (NGO)	3	15%
	Private sector	8	40%
	Total	*20*	*100%*
Nature of work	Technology development	7	35%
	Project management	7	35%
	Consultancy	2	10%
	Academic	4	20%
	Total	*20*	*100%*
Working experience	Less than 5 years	2	10%
	5-10 years	3	15%
	Over 10 years	15	75%
	Total	*20*	*100%*
Role in the open data project	S1: project initiator	2	10%
	S2: data providers from public sector	5	25%
	S3: data providers from private sector	5	25%
	S4: data providers from NGO	3	15%
	S5: data users	5	25%
	Total	*20*	*100%*

Interviewees were individually asked whether they have encountered or accept the existence of barriers one by one (identified from the literature and earlier interviewees), and they were allowed to add new barriers on the basis of their experience. Table 7-2 presents the identified barriers and their sources. Twenty initial barriers were ascertained, among which four barriers (i.e., B7, B16, B19, and B20) were proposed by the interviewees. As B19 and B20 were identified by subsequent interviewees, they were coded last. However, one barrier may be the concern of one or multiple stakeholders. For example, all public, private, and NGO data providers had concerns about privacy violation and data misuse (B1), but the barrier of insufficient knowledge and skills in using open data (B9) only bothered users. Therefore, more than 20 barriers were drawn from the original list (Table 7-2). They were labeled as S_cB_d (where c = 1 to 5 and d = 1 to 20) to illustrate that stakeholder S_c can be affected by barrier B_d such that the open data project is impeded. For example, the barrier of S3B15 indicates that data providers from the private sector have competing interests and complicated relationships with other data providers.

Table 7-2 Barrier and stakeholders identified in the open data project

Barrier identified from the literature review (unless otherwise noted *)	Source	Stakeholder(s) having a concern with
● ***Legal & licensing***		
B1. (Concerns about) Privacy violation and data misuse.	(Huijboom & Van den Broek, 2011; Janssen *et al.*, 2012; Zuiderwijk *et al.*, 2012).	S2, S3, S4
B2. Lack of open data policy and strategy.	(Huijboom & Van den Broek, 2011; Janssen *et al.*, 2012; Kulk & van Loenen, 2012).	S1
B3. Data ownership, copyright, and licensing restrictions.	(McLaren & Waters, 2011; Molloy, 2011; Janssen *et al.*, 2012; Shadbolt *et al.*, 2012)	S2, S3, S4
● ***Technical & operational***		
B4. Poor data quality and insufficient user-	(Huijboom & Van den Broek,	S2, S4, S5

friendliness.	2011; McLaren & Waters, 2011; Janssen *et al.*, 2012; Lee & Kwak, 2012)	
B5. Poor supporting infrastructure/legacy software system.	(Huijboom & Van den Broek, 2011; Janssen *et al.*, 2012)	S2, S4
B6. Poorly documented metadata.	(Zuiderwijk *et al.*, 2012; Hossain *et al.*, 2016)	S2, S4
B7. Extra workload and lack of external support.	Interviewee *	S2, S3, S4
● ***Use level***		
B8. Too many requirements and conditions for using data.	(Blakemore & Craglia, 2006; Vickery & Wunsch-Vincent, 2006; Meijer & Thaens, 2009; Janssen *et al.*, 2012)	S2, S5
B9. Lack of necessary knowledge and skills to use it.	(Huijboom & Van den Broek, 2011; Janssen *et al.*, 2012; Lee & Kwak, 2012)	S5
B10. No incentive to use or perceived uselessness.	(Janssen *et al.*, 2012; Hossain *et al.*, 2016)	S2, S5
B11. Lacking user participation.	(Janssen *et al.*, 2012; Lee & Kwak, 2012)	S1, S2, S5
● ***Institutional & governance***		
B12. Risk-averse and closed policy.	(Huijboom & Van den Broek, 2011; Janssen *et al.*, 2012; Conradie & Choenni, 2014; Hossain *et al.*, 2016)	S1, S2
B13. Focus on the trendiness for data rather than meeting actual needs.	(Blakemore & Craglia, 2006)	S1, S2
B14. Scattered data management across various resources without consistent standards and clear responsibility.	(Vickery & Wunsch-Vincent, 2006; Janssen *et al.*, 2012; Linders, 2013; Conradie & Choenni, 2014).	S2, S3, S4
B15. Competing interest and complicated	(Janssen *et al.*, 2012)	S2, S3

relationship amongst stakeholders.		
B16. Lack of priority and clear incentives to provide data.	Interviewee *	S2, S3, S4
● ***Economic***		
B17. Datasets are expensive to open up and maintain.	(McLaren & Waters, 2011; Hossain *et al.*, 2016)	S2, S4
B18. Perceived loss of previous income earned by releasing licensed data.	(Huijboom & Van den Broek, 2011; Conradie & Choenni, 2014)	S2, S4
● ***Technical & operational (supplementary as interviews went on)***		
B19. Poor IT literacy.	Interviewee *	S2, S4
● ***Use level***		
B20. Insufficient accessibility to open data.	Interviewee *	S5

7.5 Data analysis

NetMiner, a specialist network analysis software, was used to analyze and visualize the network due to its user friendliness and graphic presentation (yielding the same functional results as other software packages).

7.5.1 Network level findings

In total, 43 barriers and 97 links were identified. The density of the overall network is 0.054, and the mean distance between two nodes is 4.908. Thus, this network is relatively sparse compared with the network of referenced projects, such as major public engineering (Mok *et al.*, 2017) and complex green building projects (Yang & Zou, 2014). It is due to the difference in nature that this study only focused on key stakeholders. The distance-based cohesion of the network (0.155) is higher than its density value, which means that the barrier interdependency is complex in terms of node reachability. Figure 7-1 depicts the barrier network. Node colors represent different stakeholder types, and the shapes indicate the barrier types. As summarized in Table 7-3, most barriers involve data providers from the public sector and NGOs (S2 and S4, respectively), and their respective natures are related to technical and operational and institutional and governance aspects.

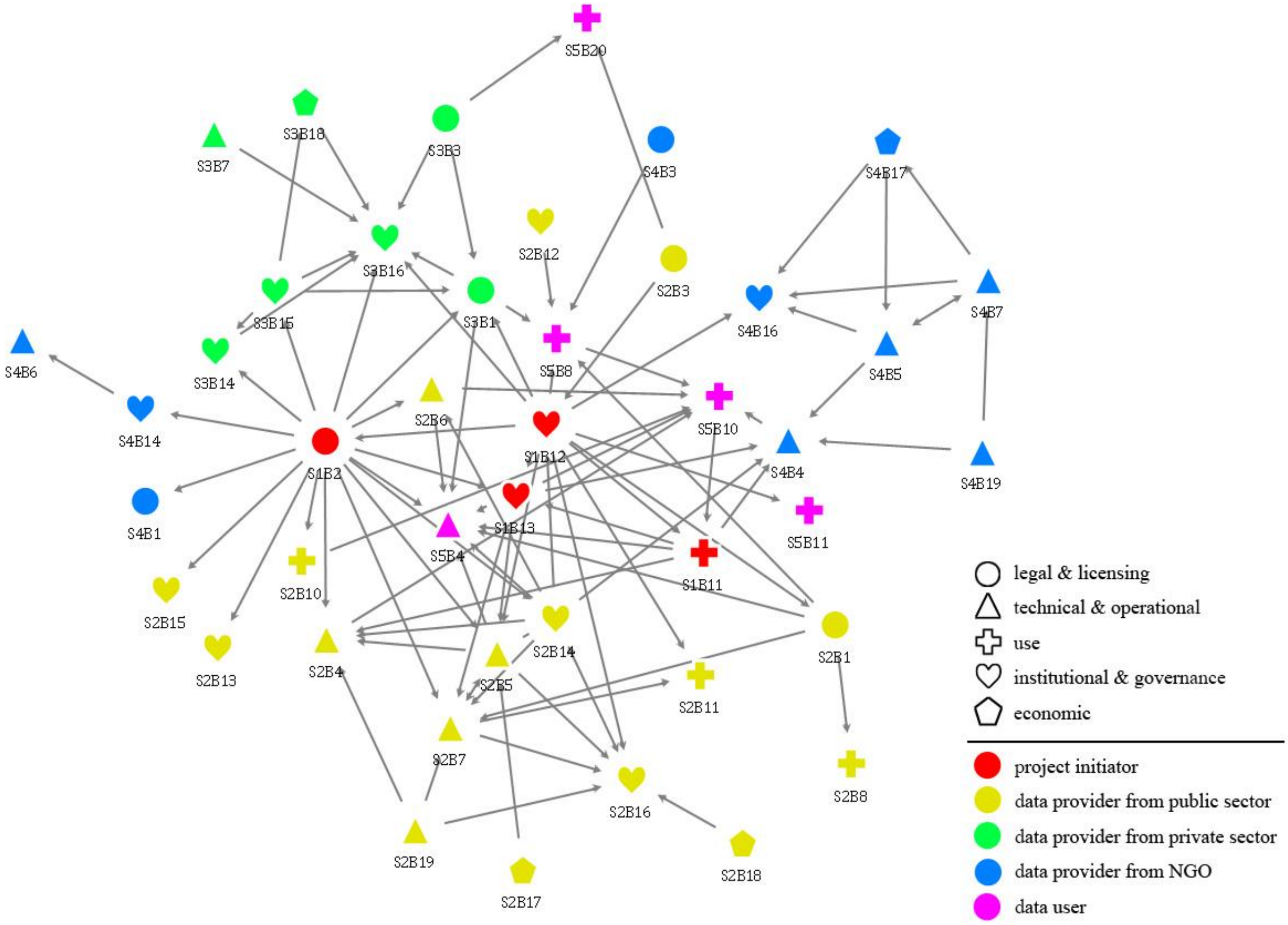


Figure 7-1 Network of the barriers faced by stakeholders in the development of an open data platform in HK

Table 7-3 Identified barriers and stakeholders

Category	Type	No. of barriers	Percentage
Nature of the barrier	Legal & licensing	7	16.3%
	Technical & operational	12	27.9%
	Use level	8	18.6%
	Institutional & governance	12	27.9%
	Economic	4	9.3%
	Total	*43*	*100%*
Stakeholder concerned	S1	4	9.3%
	S2	17	39.5%
	S3	7	16.3%
	S4	10	23.3%
	S5	5	11.6%
	Total	*43*	*100%*

7.5.2 Node level findings

Table 7-4 shows the top eight barriers in terms of the values of out-degree, degree difference, ego size, and out-status centrality. S1B2 (the initiator lacks open data policy and strategy), S1B12 (the initiator deploys risk-averse policy), and S2B14 (public data providers manage data in a scattered way) exhibit the highest values in most indicators. Thus, the effects that they exert on the other stakeholders are higher than those that they receive. Figure 7-2 depicts the out-status centrality of all barriers. The more central the location of a barrier, the more influence it exerts on the other stakeholders in the network. A high number of initiator-related barriers (in red) are located centrally. Therefore, the initiator plays the most crucial role by affecting others in this project. These barriers are more related to institutional and governance aspects (heart shape) than other categories.

Table 7-4 Ranking of barriers based on degree analysis

Rank	Barrier	Out-degree	Barrier	Degree difference	Barrier	Ego size	Barrier	Out-Status centrality
1	**S1B2**	**16**	**S1B2**	**15**	**S1B2**	**17**	**S1B2**	**4.024812**
2	**S1B12**	**12**	**S1B12**	**10**	**S1B12**	**14**	**S1B12**	**3.631537**
3	**S2B14**	**7**	**S2B14**	**4**	S2B5	10	**S2B14**	**2.129166**
4	S1B13	5	S2B1	3	S2B14	10	S2B5	1.445882
5	S2B5	5	S3B15	3	S2B7	9	S1B13	1.299789
6	S1B11	4	S2B19	3	S1B13	8	S1B11	0.954507
7	S2B1	4	S3B3	3	S3B16	8	S2B3	0.936401
8	S3B15	4	S1B13	2	S5B4	8	S2B1	0.839054

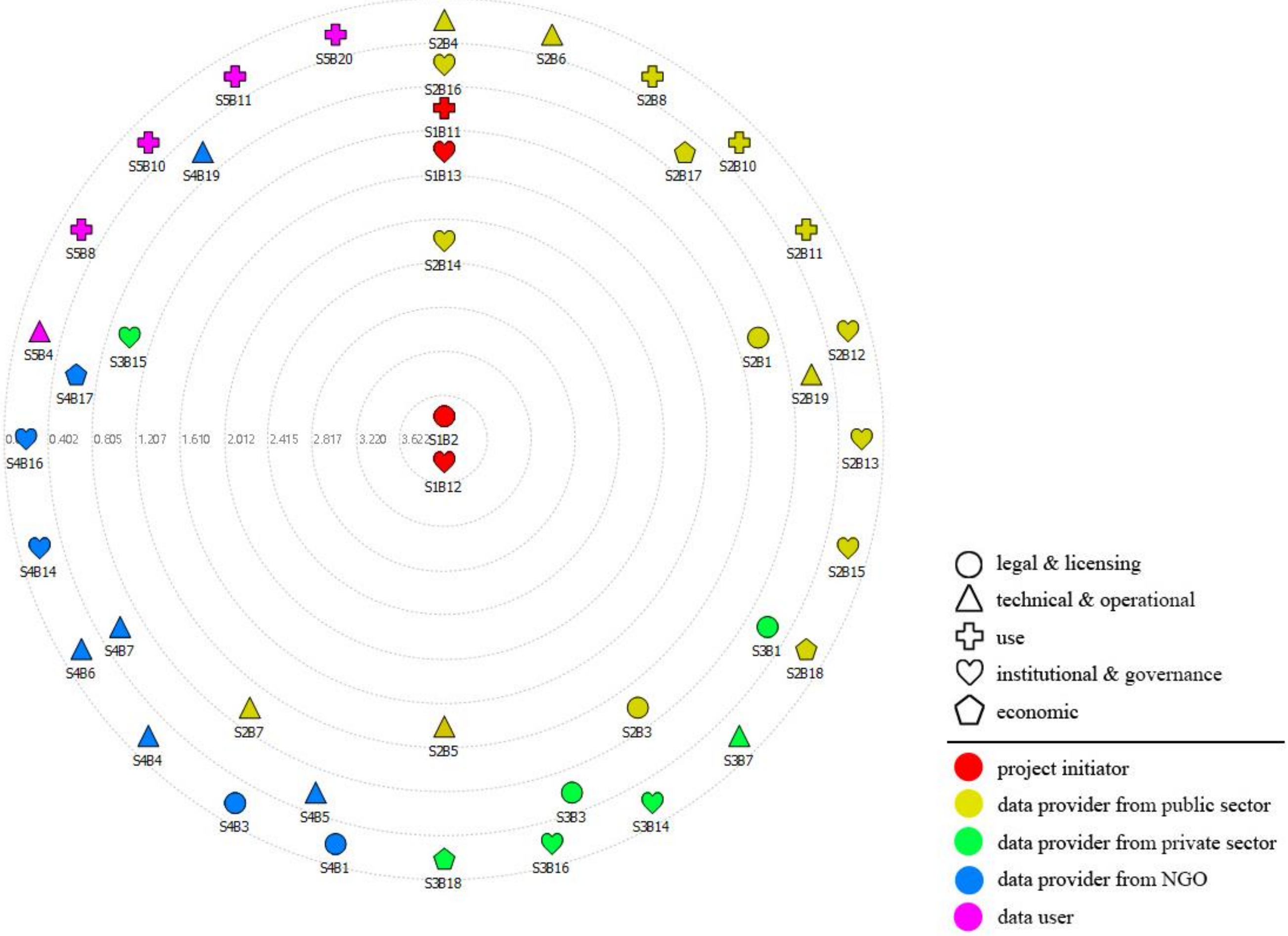


Figure 7-2 Barrier location in the out-status centrality map

Table 7-5 shows the ranking of barriers based on the betweenness centrality and brokerage. S2B14 and S1B12 are once again identified as important barriers due to their high betweenness centrality. Three newly identified barriers, namely, S1B11 (the initiator provides less public participation mechanism), S2B5 (public data providers own poor supporting infrastructure or use legacy software systems), and S5B10 (users lack incentives to use open data or perceive data as useless), play important roles in controlling the relations passing through them. Brokerage analysis, being slightly different from betweenness centrality, shows a barrier's capability of connecting various stakeholder groups as introduced in Section 3.7.3 of Chapter 3. That is, without these barriers, the interrelation among stakeholder groups could be interrupted (Yang & Zou, 2014). Two important barriers, namely, S1B2 and S1B13, play a single role as the representative for receiving influences from other initiator-related barriers, and they affect barriers related to other stakeholders. For example, the link S1B11→ S1B13→ S5B10 is concerned with the project initiator and data users. No published data on usage statistics in the Hong Kong open data portal exists. Thus, the relevance and usefulness of current data cannot be known. Users can only provide their feedback through a single link on the homepage. The insufficient public participation mechanism proposed by the initiator (S1B11) might cause him/her to chase the trendiness of the open data movement without understanding the true needs from other stakeholders (S1B13), particularly users, such that the published data are not perceived as useful by users (S5B10). The barrier of S2B14 (public data providers manage data in a scattered way) plays all types of roles (i.e., coordinator, gatekeeper, representative, itinerant, and liaison) in the network. Hence, S2B14 is active in transmitting influences among the group of public data providers as well as to other stakeholder groups. In Hong Kong, the OGCIO manages the open data portal, but no actor exists within each B/D to enforce the data quality and frequency of releasing and updating.

Table 7-5 Ranking of barriers based on betweenness centrality and brokerage

Rank	Betweenness centrality analysis		Brokerage analysis							
			Barrier	Partition Value	C*	G*	R*	I*	L*	Total
1	S2B14	0.270828	S1B12	Initiator	0	6	0	7	10	23
2	S1B12	0.260956	S2B5	Public provider	6	7	2	0	1	16
3	S1B11	0.228126	**S1B2**	**Initiator**	**0**	**0**	**12**	**0**	**0**	**12**
4	S2B5	0.223577	S2B7	Public provider	8	4	0	0	0	12
5	S5B10	0.221816	**S2B14**	**Public provider**	**4**	**1**	**5**	**1**	**1**	**12**
6	S1B13	0.213192	**S1B13**	**Initiator**	**0**	**0**	**9**	**0**	**0**	**9**
7	S1B2	0.141212	S1B11	Initiator	0	1	3	1	2	7
8	S5B8	0.079752	S3B1	Private provider	0	0	4	0	2	6
9	S4B4	0.065815	S5B10	User	0	0	1	1	4	6

(*Note: C-coordinator, G-gatekeeper, R-representative, I-itinerant, L-liaison.)

7.5.3 Link level findings

Table 7-6 shows the top eight links based on the betweenness centrality that measures the extent to which a link controls the connection passing through it. A high betweenness centrality for a link implies its crucial role in connecting several barriers. The continuity of the influences passing through different barriers can be observed between Links 2 and 1 (S2B5→ S2B14→ S1B12), Links 3 and 4 (S1B11→ S1B13→ S2B5), and Links 1 and 5 (S2B14→ S1B12→ S1B2). Then, a long link appears: S1B11→ S1B13→ S2B5→ S2B14→ S1B12→ S1B2. Therefore, Link 1 acts as the most important hub to connect other barriers and different stakeholders. A poor infrastructure and system render sharing and managing data in a centralized and standardized way difficult for the public sector (S2B5→ S2B14). As stated by an interviewee who is an engineer from the public sector, *“There is no well-built infrastructure to facilitate quality data collection and processing. Even within the same department, the poor system can’t facilitate data sharing sometimes.”* Another interviewee, a manager in the public sector, said: *“Even we manage certain public projects; however, we can’t publish or even hold comprehensive data about them as part of these projects will be managed or maintained by other departments from different domains after completion. Troubles would come if the open data coordinator or initiator pushes hard the data opening-up or integration.”* Thus, the initiator may implement a risk-averse policy in coordinating different public departments to avoid unnecessary problems (S2B14→ S1B12).

Table 7-6 Top eight links based on betweenness centrality

No.	Link	Betweenness Centrality	Link description
1	S2B14→ S1B12	446.367	Numerous public data providers (i.e., government B/Ds in this case) manage data in a scattered way, which leads the initiator to deploy a risk-averse policy in coordinating them to avoid unnecessary problems.
2	S2B5→ S2B14	384.833	Poor infrastructure and legacy systems used in the public sector render sharing and managing data in a centralized and standardized way difficult.

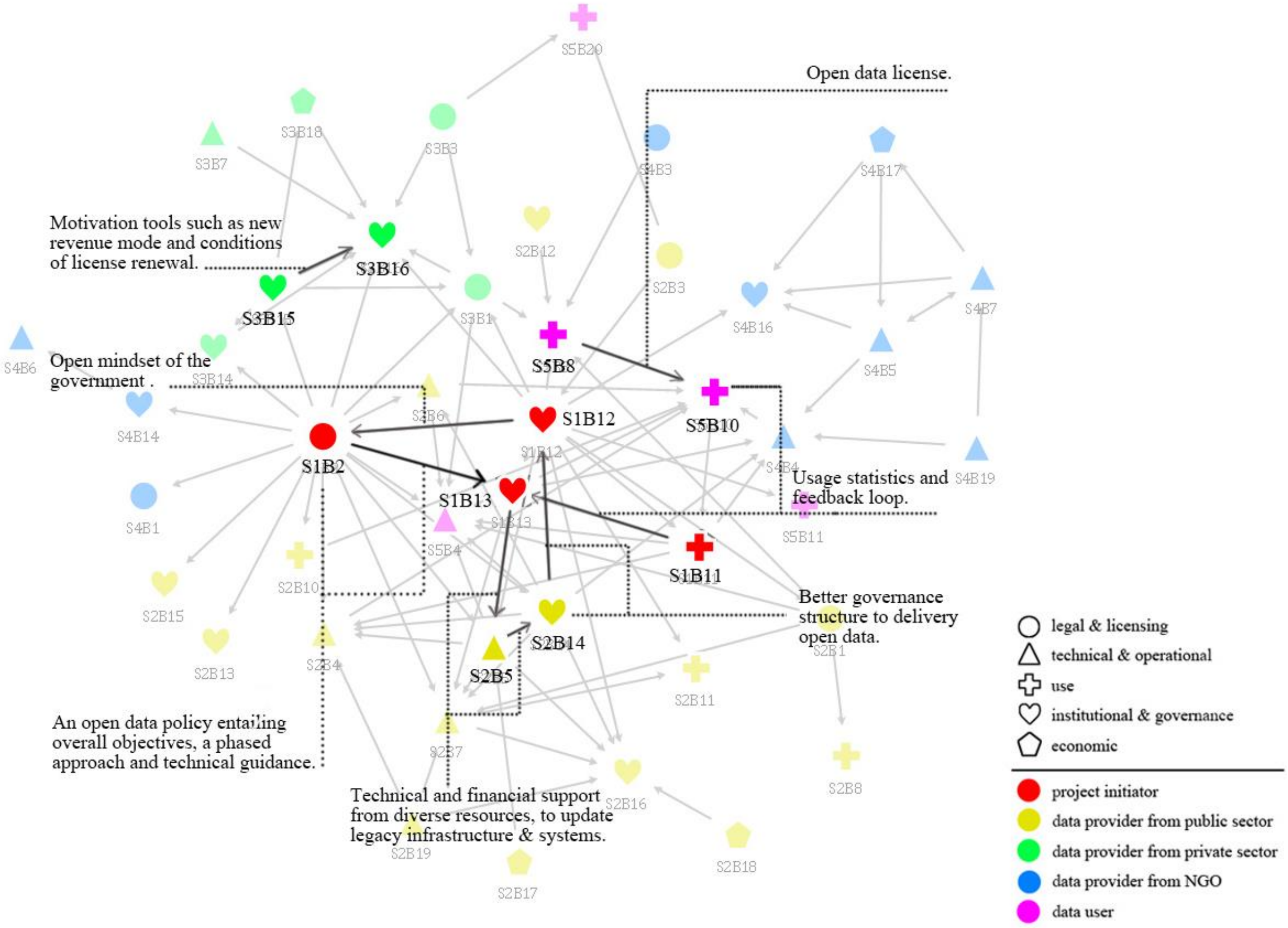
3	S1B11→ S1B13	380.833	The lack of a public participation mechanism leads the initiator to focus only on the trendiness of the open data movement rather than considering the actual needs of users.
4	S1B13→ S2B5	345.5	The initiator only concentrates on the trendiness of open data and therefore fails to guide the upgrading of ICT infrastructure and systems in the public sector.
5	S1B12→ S1B2	270.167	Risk-averse policies used by the initiator slow the publication of the open data policy.
6	S5B8→ S5B10	166.333	Numerous requirements and conditions for reusing reduce users' incentives to use data.
7	S4B4→ S5B10	142.333	Poor quality of data provided by NGOs reduces users' incentives to use data.
8	S2B16→ S2B14	100.833	Unclear incentives for the public sector to provide data cause them to continue managing data in a scattered way across various resources without consistent standards.

Although several links were not highlighted in the betweenness centrality analysis, they were mentioned frequently by different stakeholders during the interviews. The most important link is S3B15→ S3B16 (competing interests and complicated relationships among private entities reduce their incentives to provide data). Parallel service providers compete with each other such that data release causes the risks of leaking commercial information and losing potential opportunities. As stated by a chief IT manager in a private company: "*If we provide all data online, some external app developers will use them, so less users will download our apps which promotes our other services and products.*" Another link is S3B18→ S3B16 (perceived loss of income from releasing licensed data, leads private entities to be unwilling to share their data). Some efforts have been devoted to collecting and processing open data such that some private entities plan to establish/have others establish their own platforms to disseminate data with the possible goal of gaining additional profits. These findings were related to private data providers and echoed the results of a study in Chile (Gonzalez-Zapata & Heeks, 2015), which indicated that the insufficient awareness and visibility of open data's value within the private sector lead them to avoid the open data arena.

The barriers or links related to private data providers did not stand out in the node-level and link-level analyses. This phenomenon is probably because the open data project is government-initiated and mainly involves public data providers (government B/Ds in Hong Kong) at this stage. The economy/expense-related barriers were not highlighted either, which might be explained as: (1) open data is expected to be free for use and (2) the costs of data collection have already been spent when government departments undertook their statutory tasks (Jaatinen, 2016), such as the online monthly digests provided by some government departments in Hong Kong. An economic-related barrier, namely, S4B17 (open data platform is expensive for NGOs to develop and maintain), only occurs in some NGOs, of which the major services provided are not about IT but personal services, such as rehabilitation and care for the disabled.

7.6 Mitigating key barriers and links

As determined from the case study, the main approaches for addressing the barriers identified by SNA include resolving critical barriers, cutting off links, and enhancing stakeholder collaboration. Figure 7-3 shows the recommendations for mitigating key barriers and links.



Open data license.

Motivation tools such as new revenue mode and conditions of license renewal.

Open mindset of the government .

Usage statistics and feedback loop.

Better governance structure to delivery open data.

An open data policy entailing overall objectives, a phased approach and technical guidance.

Technical and financial support from diverse resources, to update legacy infrastructure & systems.

Figure 7-3 Solutions mitigating key barriers and links

The top barrier is the absence of an official open data policy in Hong Kong (S1B2). By contrast, the open data policy in New York was suggested by several interviewees as an example of good practice, especially given that its governance structure consists of: (1) the chief open platform officer (COPO), who oversees the overall open data initiatives and engenders efforts from relevant stakeholders, and (2) open data coordinators (within each public agency), who enable the delivery of datasets, address feedback, and liaise with the COPO (City of New York, 2018). This structure would enforce data release and integration, thereby alleviating scattered data management across different B/Ds without clear responsibility (S2B14). The open data policy in Hong Kong should also properly set a phased approach to fulfill its own objectives. Objectives may vary in different regions, such as obtaining economic benefits through open data in Europe or increasing governance transparency and collaboration in the U.S. This measure of setting appropriate objectives would help avoid focusing on the trendiness of the open data movement (addressing S1B13). Similar to New York, other necessary elements to be addressed in the open data policy besides objectives should include: data format standardization, frequency updates, expected data quality, ownership, deployment of open data license, and public participation.

To ensure the usefulness of open data (addressing S5B10), the initiator or data managers should provide a feedback channel to users on specific datasets that require updating and refining, as well as feedback on the most desirable datasets as practiced by the Canadian government (addressing S1B11→ S1B13). The feedback concept has been regarded as crucial in open systems because it creates a well-defined loop from which the government can learn from the public and fine-tune decision-making (Janssen *et al.*, 2012). Hong Kong may monitor the data usage and directly embed a feedback channel under each datum on the portal to ensure data relevance and usefulness. An open channel should be provided to allow users to suggest specific datasets that require updating.

Numerous requirements and conditions for reusing reduce users' incentives to use data (S5B8→ S5B10). Several databases are covered by copyright; therefore, a specific license for open data for functional use is required to avoid conflicts with creative works, such as drawings and videos. The Open Database License (ODbL) proposed by Open Data Commons (2011) is *"a license agreement intended to allow users to freely share, modify, and use this Database while maintaining this same freedom for others."* Several open data projects worldwide use ODbL to achieve improved legal security, such as OpenStreetMap, OpenCorporates, and Open Food Facts.

While pursuing the trend of open data worldwide, the initiator may fail to ground the support, especially financial support and technical guidance, for the public sector, which is faced with the problem of poor supporting infrastructure and legacy software systems (addressing S1B13→ S2B5). As reflected by other interviewees, this problem is also faced by NGOs, which are now mainly supported by the Labour and Welfare Bureau within the Hong Kong government. This problem should be addressed in the open data policy rather than a hollowed-out description. For example, approaches should be devised on how to replace the currently outdated ICT systems within the public sector through progressive solutions or how to obtain external support, such as through a suitable public–private partnership model or crowd-funding. As for the problem of inconsistent and scattered data management among B/Ds, the initiator needs to provide additional technical guidance to render the data machine-readable and reusable (addressing S2B5→ S2B14). For example, the JSON, XML, and CSV formats are widely used for publishing open data because they are easy for any programming language to read and for computers to process. Additional APIs should be deployed to provide developers with a programmatic access to wide software applications or web services. Besides the phenomenon of scattered data management, an important factor impeding the SC development in Hong Kong is the relative conservative stance of the government, statutory bodies, and private companies toward information sharing (Chan, 2017). The use of a conservative approach in setting objectives and rolling out SC initiatives has been criticized by the IT sector in the Legislative Council and by the society (Yau, 2017). As mentioned by several interviewees, resolving information islands within the public sector would take time due to complex a data governance and conservative environment (S2B14→ S1B12, S1B12→ S1B2). Data publication is simply the beginning along the information value chain, and turning open data into valuable information requires numerous "middles," such as ICT literacy, incentive, and knowledge (Heeks & Kanashiro, 2009).

As for the barrier of risk-averse policy (S1B12), a government may be wary of publishing data that may reveal the shortcomings of the public services. For example, the analysis of data on trash pickups released by the City of Los Angeles in the U.S. indicated that residents living in certain areas received worse services for refuse disposal than those living in other parts of the city (Poston & Jamison, 2015). As a result, this finding aroused wide complaints toward uneven government services and uncovered the insufficiency of funding for street sanitation. Such example is akin to "a bad story" in which open data might reveal the flaws of government work and instill fear of publishing any data. However, the government should bear with such constructive criticisms that would drive the improvement of public services and reinforce democracy in the long term. Moreover, responding to the criticisms derived from data analysis helps establish a solid relationship with the public and leads people to feel comfortable with the idea of sharing information (Miller, 2016).

Incentives would guide stakeholders in engaging with open data development. The barrier S3B16 was described by the convener of an SC union in Hong Kong as: *"Indeed we don't have any incentive for the private sector to share their data."* To address this concern and enhance the engagement from the private sector, a successful case may be viewed as a reference from Barcelona, where the government has proposed a revenue model for encouraging private entities to open up their data. A similar approach has been attempted in the SC pilot area in Hong Kong, i.e., Kowloon East. The development of a new property may be approved under the condition that the future owner regards opening up real-time public parking vacancy information within the property as one of the lease conditions. This approach might be used to encourage bus companies to publish relevant data upon the renewal of their licenses (Ko, 2017), which currently is not a requirement.

Several interviewees mentioned that the increase of open data usability relied on a combination of using heterogeneous data and involving citizens. This observation may be demonstrated by the "596 Acres" Project in New York, which transformed 34 vacant spaces into community gardens from 2011 to 2015. This project, initiated by an NGO, was empowered by the combination of diverse data, including (1) open municipal data about vacant land areas, (2) information obtained via Freedom of Information requests about urban renewal plans, (3) Google Maps, (4) data about existing community gardens published by the organization GrowNYC, and (5) the interactive community maps at OASISNYC.net. The project also highlighted resident engagement by enabling them to organize community projects virtually through signing up on the 596 Acres website and expressing views through online newsletters or face-to-face communication. In this case, public data owned by the government was properly and creatively repurposed while being aggregated with other data sources to suit the needs and interests of different stakeholders/groups (Lämmerhirt, 2017).

7.7 Summary

This chapter presents the last case study that explores the underlying network of stakeholder-associated barriers in open data development. Through SNA, this case study has identified 43 barriers faced by stakeholders in an open data project in Hong Kong and investigated their interdependencies. The major finding is that the lack of open data policy should be tackled with priority. Other important objectives include improving the IT literacy/mindset of the public sectors, upgrading their poor infrastructure and legacy systems, refining the governance structure of delivering open data initiatives, encouraging engagement from private entities, and providing a feedback loop for users. In Hong Kong, with its relatively risk-averse IT policies, bridging up information islands and forming an ecosystem to turn open data into a socially valuable information require further improvements. The next chapter will summarize the key findings of the entire research and refine them on the basis of a validation from experts.

CHAPTER 8 RECOMMENDATIONS TO MITIGATE AGAINST PITFALLS IN SMART CITY DEVELOPMENT

8.1 Introduction

This chapter summarizes the recommendations for mitigating pitfalls in SC development in Hong Kong and other emerging SCs. These recommendations are derived from the studies reported in previous chapters, including: (1) Questionnaire Survey #1 on experts in the SC domain to gain a general understanding of pitfalls in the SC development; (2) the first case study on the public use of mobile applications and the perception on the identified pitfalls; (3) the second case study that investigates the pitfall of system information insecurity through an analysis of the intrinsic reliability of a SPIS; and (4) the third case study on open data development using SNA to investigate the interrelationships of the barriers faced by the different stakeholders involved. The following sections propose and explain these mitigation measures under each pitfall. To show the complete set of recommendations in this chapter after a validation process performed with nine experts (as detailed in Chapter 9). The refinements to the recommendations resulting from the validation interviews are presented within square brackets **[ ]** in this chapter to present the complete picture.

8.2 Mitigation/preventative measures against system information insecurity

The issue of system security attracts considerable attention from citizens as revealed by the first case study on the public use of mobile apps. Experts in the SC domain believe that cyber-attacks, weak security (i.e., security as an after-thought), and interdependency of systems were the riskiest sources of system insecurity instances that would result in serious consequences to society by compromising the confidentiality of user information and leading to a system-wide failure and non-availability of essential services. The reliability analysis of a SPIS indicated that a failure in a central system server may be caused by human error, security violations, and hardware failure (particularly computer breakdown). The following sub-sections propose mitigation/preventative measures based on these findings.

8.2.1 Promote security by design and comply with established international standards

Security by design is a mindset that seeks to make systems as free of vulnerabilities and impervious to attacks as possible throughout the lifecycle of technology systems (Rouse, 2015). This concept should be promoted by the government and realized by ICT system designers/operators through risk assessment and penetration testing to discover vulnerabilities at the design stage, building and configuring ICT systems on the basis of established international standards, and continuing to refine security methodologies to upgrade the system security level. The major challenge of security is often the inability to stay ahead of attackers, who can recognize vulnerabilities and exploit them before the victim organization realizes the issue and places effective counter measures. **[**System designers should exercise due diligence when considering and specifying technology capabilities, vendor history, implementation requirements, and other critical issues at the design stage to minimize any security risk of downstream contractors failing to meet their obligations**]**.

Cybersecurity standards, such as the ISO/IEC 27001 family of standards, can be incorporated into working procedures by system designers. ISO/IEC 27001 is generally recognized as an international yardstick to specify effective information security management that covers an information system's phases of establishment, implementation, maintenance, and subsequent improvement. Moreover, ISO/IEC 27001 is designed to be applicable to all sizes and types of business and organization. ISO/IEC 15408 (known as the Common Criteria) is another standard that should also be deployed in Hong Kong's SC blueprint to evaluate the security properties of IT products. ISO/IEC 15408 has already been adopted in Taiwan since 2009 after the emergence of SC initiatives and IoT technologies. The enforcement of ISO/IEC 15408 can be led by the Innovation and Technology Bureau under the Hong Kong government or a NGO. The Hong Kong Accreditation Service could assess the competency of testing laboratories to conduct IoT security certification. [Evaluation assurance level (EAL) could be used to guide the purchase of IoT-related products following the completion of the Common Criteria security evaluation. EAL comprises seven levels, starting with EAL 1 as the most basic level up to EAL 7, thereby indicating that an IT product has completed the most stringent set of quality assurance requirements].

[Other standards were designed to suit different scopes of work. For example, ISO/IEC 27001 specifies effective information security management that covers an information system's life cycle; IEEE 2700-2014 defines the performance parameters for sensors; and ETSI TS 102 690 describes the end-to-end machine-to-machine functional architecture. The appropriate adoption of standards would facilitate the optimization of system security in smart cities]. Cities and organizations should have their cyber security strategies, the implementation of which should follow a set of objectives and principles. The Hong Kong government does well in this regard with an extensive set of IT security policies and relevant practice guides for use by government B/Ds and agencies when commissioning IT systems. Such security policies may include a baseline IT security policy, practice guide for cloud computing security, and the practice guide for security risk assessment and audit (OGCIO, 2017). A few of these policies are mandatory and represent the minimum security requirements for contractors to protect the government's information systems and data assets. Those requirements are referenced from ISO 27000.

8.2.2 General measures against security violations

Apart from adopting security standards throughout the operation and maintenance stages, system managers should (1) [deploy strong encryption by training staff members and users]; (2) [implement strong access control and change passwords frequently in terms of physical card access, safeguards, and Internet log-ins]; (3) conduct up-to-date anti-virus checking; (4) [frequently back up data through "all-site storage"]; (5) replace legacy equipment, software, and systems; (6) adopt redundancy for servers and power supplies to ensure continual system service under unexpected conditions; (7) have a recovery plan that details immediate responses to confine the damage of an incident if any breach should happen and stipulate clear division of responsibilities (i.e., who takes which role during an incident); (8) [conduct regular drills of critical city functions (e.g., test and prepare the city for normal operation at certain levels without automation by computer systems or networks under the scenario that the transportation systems are being hacked)]; and (9) remain ahead of criminal activities by conducting continuous risk assessment and renewing security methodologies and access rules to firewalls.

8.2.3 Mitigate human errors

Organizations should enforce strict technical monitoring and management regulations to help avoid human errors made by employees. [Logging system is necessary to track and record any action and change made by employees, thereby making human errors traceable in archived database]. Current effective measures that are recommendable for mitigating human errors include the stipulation of a well-defined security policy (e.g., not accessing the external web and attaching personal external drives to workplace computers), and regular training programs for employees. An organization is believed to be capable of strengthening its defenses against cyber-attacks by instilling its people with a security mindset and skills. However, even the best trained people still make procedural/operational errors when they are in a rush or in a mentally exhausted state. Thus, a recovery plan, good operational governance for staff members, and maintenance for each piece of equipment are necessary.

8.3 Mitigation measures against massive personal information leakage

In SCs where citizens' data are collected nearly ubiquitously, the top two risks that cause privacy leakage as identified in the first survey include the absence of strict standards/regulations to protect personal information and users' insufficient awareness and knowledge of data protection. Privacy leakage would result in information exposure, citizen tracking, and even impersonation, thereby risking public trust toward society and posing a threat to democracy. The concept of privacy by design (PbD) is called for in embedding privacy as the default across the entire information life cycle of any information system. Moreover, stringent regulations and education for users are needed.

8.3.1 Incorporate Privacy by Design (PbD)

PbD is an internationally recognized framework that seeks to make privacy integral to organizational priorities, project objectives, and work standards without compromising functionality. PbD was introduced in EU's General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which became enforceable since May 2018. SC promoters should implement PbD as a principle in the ICT domain to avoid possible privacy intrusion. Examples of PbD include restricting the amount of data collected by applications/services and anonymizing the data, setting a definite validity time period (data expiry), and securing user consent to collect their data.

8.3.2 Effects of strict standards/regulations in increasingly data-driven environments

Hong Kong is the first territory in Asia with a set of comprehensive personal data privacy legislation and deploys an independent data privacy regulatory framework (i.e., Personal Data (Privacy) Ordinance (PDPO)) to regulate the private and public sectors that collect, store, process, or use personal data. [However, several important "digital rights" of citizens are missing from PDPO compared with GDPR. For example, the right to erasure (“right to erasure”) allows individuals to have personal data erased from organizations and social media in certain circumstances, especially when the personal data are no longer necessary for the original purpose or if an individual objects to the processing of his/her data for direct marketing purposes (Information Commissioner' s Office, 2018)**]**. Apart from the right to erasure, GDPR stipulates that explicit consent to process personal data should be given by the data subjects before any process happens. By contrast, consent is not a prerequisite for the collection of personal data in PDPO, unless the personal data are used for a new purpose. GDPR imposes considerably stringent requirements on the processing of special categories of personal data (e.g., data on religion and health), whereas PDPO does not provide stringent requirements for any category of personal data that are considered sensitive. Another requirement in GDPR is that the service providers should be transparent with what they are doing with customers’ data through the renewal of the terms of service and privacy policies to be easily understood by anyone (Buckbee, 2018). The first case study on mobile app users determined that people often do not read conditions/terms of privacy when they download apps partly because these items are tedious and complex to read. **[**This issue may be alleviated by the use of clear and concise language (in layman terms) to describe the data collection, use, and other related notices**]**.

8.3.3 Promote awareness of protecting digital privacy

Apart from distributing relevant documents and providing professional workshops, the relevant government organizations and NGOs should instill the idea of protecting digital privacy citywide through considerably diverse and appealing methods, such as inserting an interesting short video on privacy protection at the beginning of popular movies in cinemas or giving a small token to people who correctly complete an online quiz on privacy knowledge. The content of such video and quiz may include (1) the major types of personal data (e.g., name, address, current location, ID number, and bank account); (2) possible methods of leaking personal data when using digital devices (e.g., allowing a third party to access one's data when installing a mobile app, linking to unsecure Wi-Fi in a café with one's smartphone, and clicking on unknown hyperlinks); and (3) examples of methods to protect personal data (e.g., keeping social media profiles barren, bringing one's own device (BYOD principle), constantly reading privacy policies before installing any mobile app, and being cautious about allowing free-of-charge apps to access one's contact list or photo album). In addition, a privacy-aware culture should be promoted among employees who deal with data collection and processing by enabling them to realize the significance of respecting others' privacy rights as a moral obligation and legal requirement.

8.3.4 Promote the use of aggregate information

[The concept of "aggregate information" was introduced to ensure privacy without compromising the benefits provided by big data analysis.**]** A US legislation defines aggregate information as "*collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed*" (Legal Information Institute, 2017). In such places as Japan, organizations are allowed to process or transfer customer information after making data "anonymized, pseudonymized" because their privacy laws were renewed in 2017. This change facilitates data-driven analysis and supports decision-making in urban planning. Hong Kong has yet to pass legislation on open data. Hence, the government may propose an aggregate information law or relevant regulations to ensure privacy while realizing the potential of extensive big data use as well.

8.4 Mitigation measures against public information islands

Open data are the key to bridge information islands in SCs. The main barriers to open data adoption as identified in the current research include the lack of an open data policy, poor infrastructure and legacy systems in the public sector, inefficient management of PSI, lack of public participation mechanism, and insufficient motivation of private data providers. These barriers closely interact with one another and pose immense challenges to the overall open data project. The main mitigation/preventative measures based on these findings are proposed and explained as follows.

8.4.1 Adopt an open data policy

The open data policy should first set a phased approach to gradually fulfill certain objectives (e.g., achieving economic benefits, improving environment quality, or increasing governance transparency) to avoid focusing only on the trendiness of the open data movement. Apart from setting objectives, the open data initiator (e.g., OGCIO in Hong Kong) should provide additional technical guidance to make data substantially machine-readable and reusable at the design stage. An example of technical guidance is about data format. The JSON, XML, and CSV formats are widely used for publishing open data because they are easy for any programming language to read and computers to process. Additional APIs could be deployed to provide developers with programmatic access to enable extensive software applications or web services. [The technical guidance should also include how to make metadata unified and well-documented. The reason is that metadata directly influences the process of searching and discovering relevant data sets for particular consumer needs].

Additional financial support from the government is needed to assist the public sector facing the problem of poor supporting infrastructure and legacy software systems. This strategy should be addressed in the open data policy rather than including it as a hollowed-out description. For example, economical strategies should be devised on how to replace the currently outdated ICT systems within the public sector by progressive solutions or how to obtain external support, such as through a suitable public-private partnership model or crowd-funding. [An improved communication infrastructure, such as the Narrowband IoT network, 5G, and multi-functional smart lampposts (being contemplated in Hong Kong) is also needed to accelerate the collection of citywide open data].

The issuance of a specific license for functional open data would avoid conflicts with creative works, such as drawings and videos. The open database license (ODbL) proposed by the Open Data Commons (2011) is "*a license agreement intended to allow users to freely share, modify, and use this database while maintaining this same freedom for others*." Several open data projects worldwide use the ODbL to have improved legal security, such as OpenStreetMap, OpenCorporates, and Open Food Facts.

8.4.2 Improve data management across organizations and promote public participation

An improved governance structure that enables open data release could enforce data availability and integration, thereby alleviating scattered data management across different B/Ds without clear responsibility. As practiced in New York, such a structure mainly comprises (1) the chief open platform officer (COPO), who oversees the overall open data initiatives and engages effort from the relevant stakeholders; and (2) open data coordinators (within each public agency), who enable the delivery of data sets, address feedback, and liaise with COPO. To improve the usefulness of open data, platform initiator or data managers should enable users to provide feedback on specific data sets that need updating and refining, as well as suggest desirable data sets, as practiced by the Canadian government. Hong Kong may also monitor open data usage to analyze the data relevance and usefulness.

8.4.3 Motivate stakeholder engagement

Incentives would encourage stakeholders to engage with open data development. To enhance the engagement from the private sector, a successful reference case from Barcelona can be considered, in which the government proposed a revenue model for encouraging private entities to open up their data. A similar approach has been tested in the SC pilot area in Hong Kong, Kowloon East. The development of a new property carries the condition that the future owner undertakes to open up real-time public parking vacancy information within the property. This approach may also be used to push bus companies to publish relevant data upon the renewal of their licenses, which is currently not a requirement. [Apart from governance tools, NGOs, and research institutes related to SC development and big data analytics could seek to lobby for the private and public sectors to open up their data sets and even change the conservative culture that obstructs Hong Kong from fulfilling its SC ambition].

8.5 Mitigation measures against digital divide in society

Section 4.4.2.4 (*Causes of digital divide*) in Chapter 4 mentions that the current penetration of smartphones and the Internet among different groups in Hong Kong is high. Certain programs also improve digital accessibilities, such as the “i Learn at home” initiative launched by the government between 2011 and 2018 to support eligible families in procuring affordable Internet access services and personal computers. Hence, owning digital devices is not a major problem in Hong Kong and other developed regions. The top three risks resulting in the digital divide as identified in this research include “personal attitude barriers,” “lack of training programs for unskilled citizens,” and “insufficient special concerns for disadvantaged groups.” Apart from the provision of suitable digital training that caters to the needs of SCs, the narrowing of the digital divide relies on effort from the psychological perspectives by constructing a long-term trustworthy environment and positive mindset among users. Additional measures that narrow the digital divide are proposed in the following subsections based on the findings gained from interviews with disadvantaged groups and the stakeholders helping the disabled in Hong Kong (case Study 1, Chapter 5).

8.5.1 Education and training

8.5.1.1 Identify the digital gap and target groups

The development of an understanding of the ICT usage status in the community lays the foundation for establishing a strategic framework to bridge the digital divide. The Hong Kong thematic household survey report from 2016 to 2017 by the Census and Statistics Department shows the general penetration rate of personal computers, Internet, smartphones, and other information regarding ICT usage, such as time spent in online social activities, major types of products/services purchased online, population familiarity with and usage of Government services (e.g., mobile E-government services and GovHK). The report reveals that the priority groups to receive digital skill training include households in public rental housing and economically active people. Apart from economically deprived people, other potential target groups for combatting the digital divide may include the elderly and disabled.

8.5.1.2 Stakeholder engagement

The process of bridging the digital gap is continuous, in which an array of related organizations may need to be engaged in supporting the general public to become proficient users and leave the status of digital novices (Welsh Government, 2016). First, a coordinator is necessary for communication with strategic partners. In Hong Kong, various not-for-profit organizations have joined the digital inclusion initiative, such as the Cybersenior Network Development Association Limited, Equal Opportunity Commission, and Hong Kong Blind Union. A few private entities also recognize the loss of potential customers who are currently offline or lacking in digital skills. Hence, including digital inclusion activities as part of their services would support community-based programs.

8.5.1.3 Course design

Bridging the digital divide within the SC context requires more than the ability to access the Internet. Given the emergence of SC, previous IT courses (e.g., basic training on the use of Octopus cards, ATM, and web surfing) have become relatively outdated as explained by visually impaired interviewees in the digital divide section (Section 5.5.6, Chapter 5) of this study. For overseas initiatives, an essential digital skills framework was established by the Lloyds Banking Group and Tech Partnership (2018). This framework is intended to be promoted throughout the UK and can be used as reference by other regions. This framework enables adults to participate in and contribute to the current and future digital world by learning the following five skills: (1) digital foundation skills, such as turning on a device, connecting a device to the Internet using Wi-Fi, and logging into a website using their own accounts; (2) communication skills, such as sending e-mail, sharing data, and posting photos on social media platforms; (3) skills in handling information and contents, including using search engines, managing information in local folders, and storing data using cloud services; (4) transaction skills, such as online purchasing, booking travels, and managing bank accounts; and (5) problem solving skills, including accessing support services or using self-help online tutorials.

8.5.2 Removal of attitude/psychological barriers when dealing with ICT

The benefit and ease of using ICT should be understood by conservative people to change their negative attitudes toward advanced technologies. Apart from media education, this knowledge may be instilled via workshops hosted by NGOs (including community centers) and private entities (e.g., banks), which may organize digital inclusion activities as part of their services to attract numerous potential users. An issue that also deserves considerable attention is online security because it has become a concern of “digital laymen.” The Government Digital Service (2014) determined that the lack of trust in cyberspace (concerns with online crime risk) is a major reason for people not going online. Measures that ensure cybersecurity can also be included in digital skill training. Common but effective contents suggested by Go ON UK (2015) include running and updating anti-virus software, distinguishing malicious websites, securing financial transactions, protecting personal data, and respecting the privacy or copyright of others.

8.5.3 Sustainability of improving digital inclusion

The Hong Kong government has devoted resources to develop various mobile apps to assist disadvantaged groups. The government often funds NGOs in one go to develop an app. However, the requisite resources for updating and maintaining the apps after completion are lacking. Moreover, funding NGOs to develop mobile apps on their own is not as effective as outsourcing to IT professional entities. [Therefore, the government may support NGOs to collaborate with private entities to form a sustainable business model to maintain the apps]. Under the current governance structure in Hong Kong, committees (e.g., Rehabilitation Advisory Committee) are assigned to assist disadvantaged groups, particularly to promote a barrier-free environment. However, no committee or entity monitors whether or to what extent accessibility is achieved in the digital world. [Given the increasing digitalization and development of SC, a body is called under the governance structure to maintain continuous focus on digital inclusion].

8.5.4 Provide special concern/care for disadvantaged groups

A certain group of people would consistently be unwilling or unable to use e/mobile services. Therefore, maintaining in-person services is necessary in populous, common and well-publicized places, such as underground stations and banks that also provide electronic services. [Moreover, trained staff members should be stationed at front desks to assist disadvantaged groups to use new digital services. For example, indoor navigation via Beacon and mobile apps is available in a train station in Hong Kong. However, when disadvantaged groups, such as visually impaired people, encountered difficulties in using the mobile app, staff members in the station could not assist substantially because they lack familiarity with the app. Hence, communication should be improved between technology developers and people working in the frontline to form a feedback loop.]

8.6 Summary

This chapter discusses the recommendations ensuing from the previous chapters. It highlights the contribution of this research for mitigating and preventing potential pitfalls in the SC development. Proposed measures are applicable at different implementation stages and levels. Based on findings in this Chapter, Table 8-1 categorizes the measures against identified pitfalls at the stages of design, operation and maintenance/feedback, as well as appropriate action levels of implementation, i.e., individual, corporate and policy. The next chapter validates the findings, in particular the above recommendations.

Table 8-1 Applicability of proposed mitigation measures

Identified pitfall	**Individual level**	**Corporate level**	**Policy level**
System info insecurity	B	A; B; C	A; B
Personal info leakage	B; C	A; B; C	A; B
Info islands	B; C	A; B; C	A; B; C
Digital divide	B	B	A; C

*Stage of implementation:

A-Design stage; B-Operation stage; C-Maintenance/Feedback stage.

CHAPTER 9 VALIDATION OF THE RESEARCH FINDINGS

9.1 Introduction

Following the last chapter, which discusses the recommendations for SC development, this chapter aims to validate (1) the relevance and importance of the identified pitfalls and (2) the practicality, effectiveness, and adequacy of the proposed mitigation/preventative measures. Suggestions to further improve the research findings were obtained by interviewing nine experts/experienced practitioners in the SC development in Hong Kong. Section 9.2 briefly reviews the key findings of this research that will be used as the basis of the validation. Thereafter, Section 9.3 introduces the process and results of the validation and ends with the candidate's responses towards the suggestions collected. A summary is provided at the end of this chapter.

9.2 Summary of the key findings

This section summarizes and categorizes the key recommendations in Tables 9-1 to 9-4. These recommendations were presented to the expert interviewees as the basis for their validation. Subsequent recommendations arising from the validation interviews are shown in brackets **[ ]** in the preceding chapter 8 and herein.

Table 9-1 Mitigation/preventative measures against information system security

Critical issue to be solved	How to mitigate/prevent	Who	When	Derived from
1. Security being an afterthought	(1) Promote security by design; (2) Comply with established international standards and IT security policies;	The government; system designers and	Throughout the system design, operation and	Questionnaire survey#1 on SC experts (Chapter 4).

	(3) [Exercise due diligence when considering and specifying technology capabilities, vendor history, implementation requirements, etc]; (4) [Use Evaluation Assurance Level to guide the purchase of IoT-related products].	operators.	maintenance.	
2. Hardware failure	(5) Back up data [by “all-site storage”]; (6) Have a recovery plan detailing instant responses and clear division of responsibilities; (7) Prepare for redundant servers and extra power suppliers.	System designers, operators, users.	During the operation stage.	Reliability analysis of SPIS (case study 2, Chapter 6).
3. Security violations	(5) to (7) above also apply; (8) Conduct up-to-date anti-virus checking; (9) [Deploy strong encryption by training staff and users]; (10) [Change passwords frequently in terms of physical card access, safeguards, and Internet log-ins]; (11) [Conduct regular drills of critical city functions under the scenario of being hacked]; (12) Renew security methods and access rules of firewall;			
4. Human errors	(13) Have a well-defined security policy; (14) Instill employees with a security mind-set through regular trainings; (15) Impose strict technical monitor and management protocol such as [using logging system to track and record any action and change made].	System operators, users.	During the operation stage.	

Table 9-2 Mitigation/preventative measures against massive personal information leakage

Critical issue to be solved	**How to mitigate/prevent**	**Who**	**When**	**Derived from**
1.Ubiquitous data collection	(1) Incorporate PbD by restricting the amount/type of data collected and anonymize the data, setting a definite validity time period, getting users' consent to collect their data.	The government; system operators; contractors/IT service providers.	Throughout the design, operation, and management stage.	Questionnaire survey#1 on SC experts (Chapter 4).
2. Absence of strict standards or regulations to protect personal data	(2) Move towards strict standards/regulations which impose stringent requirements on the collection and processing of personal data in increasingly data-driven environments; (3) [Clarify and enforce more "digital rights"] (e.g. right to be erasure) for citizens; (4) [Enforce service providers to use clear and concise language (in layman terms) to describe the privacy conditions]; (5) [Promote the use of "aggregate information"].	The government.	During the design and operation stage.	Questionnaire survey#1 on SC experts (Chapter 4).
3. Insufficient awareness and knowledge on privacy protection of users	(5) Instill the general idea of protecting digital privacy through more diverse channels in appealing ways (such as dramatized TV broadcast); (6) Promote a privacy-aware culture for employees who deal with data collection and processing.	The government; NGOs; citizens as users; private entities related to data analytics.	Throughout the SC development.	Questionnaire survey#2 on mobile app users (case study 1, Chapter 5).

Table 9-3 Mitigation/preventative measures against public information islands

Critical issue to be solved	How to mitigate/prevent	Who	When	Derived from
1. Scattered data management across B/Ds	(1) Renew the governance structure to enforce open data development.	The initiator (OGCIO in this research); public departments as data providers.	During the design stage.	SNA of the barriers faced by stakeholders in the open data project (case study 3, Chapter 7).
2. Lack of open data policy	(1) above also applies; (2) Set proper objectives; (3) Provide more technical guidance such as data format, updating frequencies, data ownership, [and how to making metadata well-documented;] (4) Diversify financial resources to improve [citywide communication infrastructure] and systems in the public sector; (5) Issue specific licenses (e.g. Open Database License) for functional open data.			
3. Lack of public participation	(6) Enable users to give feedback on specific datasets that need updating and refining, as well as suggest desirable datasets;	Users, the initiator.	Throughout the operation stage.	
	(7) Monitor open data usage to analyze the data relevance and usefulness.	The initiator.		
4. Insufficient motivation of (potential) data providers	(8) Use new revenue model or contractual measures to encourage private entities to open up data; (9) [Relevant NGOs and research institutes to lobby the private and public sectors to open up their datasets.]	The initiator; private data providers and NGOs.	During the design stage.	

Table 9-4 Mitigation/preventative measures against digital divide

Critical issue to be solved	How to mitigate/prevent	Who	When	Derived from
1. Attitude barriers towards ICT 2. Lack of helpful training programs for unskilled citizens	(1) Identify the digital gap and target groups; (2) Stakeholder engagement: a coordinator and partners including NGOs, and private companies that provide digital services;	The government.	At the design stage.	Questionnaire survey#1 on SC experts (Chapter 4);
	(3) Organize digital inclusion activities as part of the services of private IT companies to attract more potential users;	Private entities.	At the operation stage.	Questionnaire survey#2 on mobile app users (case study 1, Chapter 5).
	(4) Update digital-skill courses in communities, and teach effective measures to ensure cybersecurity and protect privacy;	NGOs; users.		
3. Insufficient special concern/care for disadvantaged groups	(5) Continue requisite resources for updating and maintaining the apps or other development by [promoting the collaboration between NGOs and private entities;]	The government; NGOs; private entities.	At the operation stage.	
	(6) Keep in-person service provisions in some common and well publicized places; (7) [Have trained staff at front desks helping disadvantaged groups to use new digital services;]	Service providers.	At the operation stage.	
	(8) [Build a body under the governance structure to keep continuous focus on digital inclusion.]	The government.	At the design stage.	

9.3 Validation of the proposed recommendations

To validate the relevance and importance of the identified pitfalls, and the effectiveness and practicality of the proposed recommendations, nine experts/experienced practitioners in the domain of SC development were invited for face-to-face interviews from July to August in 2018. Each interview lasted approximately one hour. During each interview, the author explained the entire research and the expert gave their general comments and specific views on the proposed recommendations. At the end of the interview, each expert ranked the research findings in terms of their relevance and importance, practicality, effectiveness, and adequacy using a Five-point Likert scale (1 represents "Not agree at all," while 5 represents "Totally agree").

A pilot test was conducted with three fellow research staff members individually before the formal interviews to evaluate the clarity of items in Tables 9-1 to 9-4. To ensure that the interviewees completely understand the findings, a template of questions and issues to be discussed during the interviews was prepared (see Appendix 4: *Validation Questionnaire Sample*). The questionnaire includes three sections: (1) a brief introduction of the entire research and the four pitfalls, (2) Tables 9-1 to 9-4 listing the recommendations proposed (except those presented in brackets), and (3) the criteria to evaluate these recommendations. The validation deploys similar criteria used in the approved theses of Cheung (2009), Javed (2013), and Lee (2016) with suitable modifications to fit the context of the current research. The validation criteria comprise eight attributes. To evaluate the relevance and importance of identified pitfalls, the three criteria involve whether the pitfalls (1) exist in reality, (2) are comprehensive, and (3) bring significant adverse effects to society. To evaluate the practicality of the proposed measures, the criteria include whether they are (1) clear and understandable and (2) implementable in the majority of circumstances. To analyze the effectiveness and adequacy of the proposed recommendations, the criteria include whether (1) the proposed measures would be effective to avoid pitfalls in SC, (2) this study would guide the improved implementation of SCs, and (3) the parties recommended for taking the stated actions are appropriate. Table 9-6 summarizes the evaluation results using these criteria.

9.3.1 Profile of the experts

The experts were selected because of their knowledge, working experience, and positions. They were from organizations that have engaged in the SC development in Hong Kong. They were approached during prior conferences and events closely related to SCs. Table 9-5 shows that the interviewees were from the public sector, private sector, and NGOs and represent diverse occupational backgrounds. All interviewees have extensive working experience (ranging from 9 to 30 years) and hold important positions in their organizations.

Table 9-5 Interviewees' profile (expert interviews for validation)

No.	Organization type	Nature of work	Years of work experience	Position in organization
1	Public sector	Academic	≥30 years	Senior researcher
2	Public sector	Project management	≥17 years	Assistant manager
3	Private sector	Project management, consultancy/advisory	≥15 years	Senior project manager
4	Private sector	Customer service	≥18 years	Senior director
5	Private sector	Data analytics, product	≥19 years	Chief data officer

		development		
6	Private sector	Marketing/Sale	≥15 years	Cyber security expert
7	Private sector	Consultancy/advisory	≥21 years	Director
8	NGO	Technology development, strategy planning	≥28 years	Chairman
9	NGO	Customer service	≥9 years	Founder

9.3.2 Validation results

Table 9-6 shows the results of the validation questionnaire returned from the experts after the face-to-face interviews.

Table 9-6 Results of the validation questionnaire for experts

Criterion	Not agree at all ◄──► Totally agree					Mean	SD
	1	2	3	4	5		
A. Relevance & Importance							
(1) The pitfalls identified in this study exist in reality.	0.0% (0)	0.0% (0)	0.0% (0)	33.3% (3)	66.7% (6)	4.67	0.50
(2) The pitfalls identified in this study are comprehensive.	0.0% (0)	0.0% (0)	0.0% (0)	88.9% (8)	11.1% (1)	4.11	0.33
(3) The pitfalls identified may bring significant adverse effects to the society.	0.0% (0)	11.1% (1)	11.1% (1)	44.4% (4)	33.3% (3)	4.00	1.00
B. Practicality							
(4) The proposed preventative and mitigation measures are clear and understandable.	0.0% (0)	0.0% (0)	22.2% (2)	44.4% (4)	33.4% (3)	4.00	0.78
(5) The proposed preventative and mitigation measures are implementable in most circumstances.	0.0% (0)	0.0% (0)	33.4% (3)	33.3% (3)	33.3% (3)	3.89	0.87
C. Effectiveness & Adequacy							
(6) The proposed preventative and measures would be effective to solve pitfalls in smart cities.	0.0% (0)	0.0% (0)	22.2% (2)	66.7% (6)	11.1% (1)	4.11	0.60
(7) This study would help guide better implementation of smart cities.	0.0% (0)	0.0% (0)	11.1% (1)	33.3% (3)	55.6% (5)	4.67	0.73
(8) The parties recommended for taking the stated actions are appropriate	0.0% (0)	0.0% (0)	11.1% (1)	66.7% (6)	22.2% (2)	4.11	0.60

The mean score of all items were above 3.5, which means that the findings of this research were generally agreed upon by the experts. Note that the evaluation criteria “the pitfalls identified in this study exist in reality” and “this study would help guide better implementation of smart cities” received the highest scores (mean score = 4.67). Although one of the criteria under practicality (i.e., the proposed preventative/mitigation measures are implementable in most circumstances) was given a relatively low score (mean score = 3.89), the experts provided suggestions to improve these measures as discussed in the next section.

9.3.3 Suggestions from validation and Candidate’s responses

Table 9-7 summarizes the comments collected from the nine experts. The responses are made to improve the entire research, particularly the proposed mitigation/preventative measures. Additional effective solutions commonly used in related industries were suggested by the validation experts to enhance the practicality of the recommendations. These solutions are also incorporated in the thesis and presented in brackets **[   ]** in Chapter 8.

Table 9-7 Experts’ comments on the research findings and responses from the candidate

Suggestions from Interviewee 1
(1) It is good to mention ISO standards, which are professional and interoperable in quality. An additional common measure to ensure information security is to change passwords frequently in terms of physical card access, safeguarding, and internet log-ins. Strong encryption can be realized by training staff members and users. Specify the

measure of backing up data by adding an “all-site storage,” which includes onsite storage (e.g., storing important data on local hard drives) and offsite storage (e.g., storing important data on a remote server).

(2) It is necessary to substantially elaborate why Hong Kong needs GDPR or strict rules.

Responses from the Candidate

(1) Comments were incorporated into the following sections of this thesis: 8.2.2 (*General measures against security violations*) in Chapter 8.

(2) The candidate suggested moving toward considerably strict regulations, such as GDPR, which imposes stringent requirements on the processing of special categories of personal data. This recommendation is made because of several important issues to ensure privacy protection, which is lacking in the current principle-based Personal Data (Privacy) Ordinance (PDPO) in Hong Kong. Unlike the traditional digital world, SCs pose considerable challenges to privacy protection. With extensive data being collected ubiquitously in SCs, including the right to erasure (“right to erasure ”), distinguishing sensitive personal data from non-sensitive one, regulating data processors directly, and requiring consent as a pre-requisite for the collection of personal data are necessary (consent is now a pre-requisite in HK’s PDPO only when the personal data is used for a new purpose). The preceding discussions were emphasized in Section 4.4.4.2 (*Measures against personal information leakage*) in Chapter 4, and Section 8.3.2 (*Effects of strict standards/regulations in increasingly data-driven environments*) in Chapter 8.

Suggestions from Interviewee 2

(1) The identified pitfalls are important. You may depict the four pitfalls within the SC context to assist readers understand them easily.

(2) Elaborate more on the selection of security standards because of the availability of various types to choose from, which focus on different aspects.

(3) Metadata is important. We need a coordinator to absorb raw data, and then mask them, instead of collecting masked data together.

Responses from the Candidate

(1) At the beginning of this thesis, a prelude/story depicts these pitfalls as a fairly common scenario in a SC. It helps readers understand these pitfalls easily and realize their real significance.

(2) A spectrum of standards were introduced with their foci and where they are applicable in Section 4.4.4.1 (*Measures against system information insecurity*) in Chapter 4 and Section 8.2.1. (*Promote security by design and comply with established international standards*) in Chapter 8.

(3) In the third case study on SNA of the open data project in Hong Kong (Chapter 7), a barrier related to metadata exists: *B6. Poorly documented metadata.* However, this barrier was not highlighted in the analysis result. Given its importance as suggested by the expert, it has been highlighted in Section 8.4.1 (*Adopt an open data policy*) in Chapter 8.

Suggestions from Interviewee 3

(1) What is the definition/scope of SC in this research?

(2) The government also spends money to develop apps that will assist disadvantaged groups, although the effects are uncertain.

(3) Whether collecting more urban data or narrowing [the] digital divide, an improved communication infrastructure is needed for SC development in Hong Kong, such as (the)

Narrowband IoT network and 5G.

Responses from the Candidate

(1) To fit the scope of this research, a definition of SC has been provided after the discussion of current definitions in Section 1.1.1 in Chapter 1. “Based on the review of the existing definitions of SC, this study proposes its own concept of SC, which emphasizes technology and social integration and suits the scope of this research. The concept is that a SC improves citizens’ quality of life and social integration through the application of advanced information technologies, effective governance, and proactive solutions, which mitigate potential pitfalls.”

(2) This issue has been discussed in Section 5.5.6 in Chapter 5. Only a few respondents know about any group being assisted by the government in the use of information technology. This finding was recorded through interviews with organizations helping disadvantaged groups: “... although the government had developed several platforms or apps to help the disadvantaged, it was important to maintain and update those facilities further, and to involve more efforts from the private sector.”

(3) Improved communication infrastructure, such as the arrow-band IoT network, 5G mobile communication, and the multi-functional smart lampposts collecting citywide real-time data were discussed in Section 7.5 in Chapter 5 and Section 8.4.1 in Chapter 8.

Suggestions from Interviewee 4

(1) To mitigate human error, a logging-in system is necessary to track and record any action and change made (trackable achieve database).

(2) Another measure that should be emphasized in privacy protection is to use aggregated data.

Responses from the Candidate

(1) Comments were incorporated in Section 8.2.3 (*Mitigate human errors*) in Chapter 8.

(2) The use of aggregate data fulfills the potential of big data without compromising citizens' privacy. The issue is included in Section 8.3.4 (*Promote the use of aggregate information*) in Chapter 8.

Suggestions from Interviewee 5

The research is timely and can be an important contribution to the body of knowledge. Digital information and its management within SCs is critical to the operation of an economy that is increasingly interdependent and connected in (i) stakeholders, processes and (ii) outcomes. Taking this perspective, the PhD research should seek to understand not only how pitfalls should be mitigated, but also identify sustainable digital strategies to develop smart cities.

Responses from the Candidate

This research aims to promote an improved SC development by mitigating/preventing potential pitfalls. Stakeholder-related issues in the open data project and digital inclusion activities, which may generate social and economic benefits, were discussed in Chapter 7 Sustainable strategies to develop smart cities were incorporated in the conclusion part (Section 10.4.2 in Chapter 10: *A holistic approach and sustainable strategies to develop SCs*).

Suggestions from Interviewee 6

The biggest challenge of security is often the inability to get ahead of attackers who will be able to find the vulnerability and exploit it before the organization realizes the issue and put the effective counter-measure in place. Due diligence design of smart city is crucial. The city must be able to remain operational at a certain level even without automation by computer systems or networks in case of disaster or when unexpected.

Responses from the Candidate

Following the introduction of the security-by-design concept, the need to conduct thorough due diligence of deployed technologies at the design stage has been added in Section 8.2.1 (*Promote security by design and comply with established international standards*) in Chapter 8.

Suggestions from Interviewee 7

(1) The security solutions should be more specific for smart cities, for example, add drilling of critical city functions in case of unexpected happening.

(2) It is worth considering the need to deploy stricter regulation to protect privacy in Hong Kong at this stage because of cultural and other regional differences. Users balance the efficiency, price, and privacy and make a trade-off.

(3) The privacy conditions of using digital services or installing mobile apps need to be more user-friendly and readable. Make laymen easily understand the conditions.

Responses from the Candidate

(1) Recommendations to improve information security are derived from the expert questionnaire survey and reliability analysis of a SPIS. They are generalized to fit the majority of systems in SCs from the perspective of technology and management. The need of conducting regular drill of critical city functions such as transportation were added in Section 8.2.2 (*Defense security violations by common measures*) in Chapter 8.

(2) Section 8.3.2 (*Effects of strict standards/regulations in increasingly data-driven environments*) in Chapter 8 shows the important issues missing from Hong Kong's privacy regulatory framework PDPO compared with EU's GDPR, including the right to be forgotten/right to erasure and consent as a prerequisite to collect personal data. Although cultural and other regional differences exist between HK and the EU, it would be better if HK can move toward the more stringent requirements to better adapt to increasing digitalization and ubiquitous data collection needs.

(3) The use of plain language in terms of services and privacy policy is a new requirement in GDPR. This concept was added in Section 8.3.2 (*Effects of strict standards/regulations in increasingly data-driven environments*) in Chapter 8.

Suggestions from Interviewee 8

(1) It is better to mention a numerical grade (Evaluation Assurance Level or EAL) to test an ICT product after the completion of the Common Criteria security evaluation. The enterprises could use EAL as a guide when purchasing IoT-related products. IoT device makers whose products conform to EAL may enjoy higher adoption by customers.

(2) Emphasize the role of NGO in pushing open data development in the long run, such as lobbying the private and public sector to open their mindset, particularly the quasi-public sector, such as train companies and transportation card companies. To change the conservative culture, NGOs play an important role in encouraging open-mindedness that is imperative in moving forward Hong Kong's smart city ambition.

(3) The effectiveness of mitigation measures should be substantially measurable.

Responses from the Candidate

(1) Comments were incorporated into Section 8.2.1 (Promote security by design and

comply with established international standards) in Chapter 8.

(2) The long-term role of NGOs was emphasized in Section 8.4.3 (Motivate stakeholder engagement).

(3) The effectiveness of several measures was measured and proved to be significant by other studies. For example, an empirical study by Wamuyu (2017) used community technology centers to offer digital literacy skills training as an interventional approach to successfully narrow the digital divide. Providing digital-skill education and training at the community level, which is similar to the said measure, was included in Section 8.5.1 in Chapter 8. An employee awareness training program in Missouri in the U.S. was acknowledged for its effectiveness in raising security awareness, reducing human errors, and keeping the security culture alive (Newcombe, 2016). Similarly, Section 8.2.3 in Chapter 8 includes the suggestion that an organization can strengthen its defenses against cyber-attacks by instilling a security mindset among its people and providing skills through regular training programs for employees.

Suggestions from Interviewee 9

Disadvantaged groups should be carefully considered in SCs.

(1) Although in-person services are available, staff working in the front line cannot well help disadvantaged groups to use newly-developed services as they are not familiar with the technologies (e.g., indoor navigation via Beacon and mobile app in a metro station). Hence, communication should be improved between technology developers and people working in the frontline.

(2) The government has endeavored to develop various apps to assist disadvantaged groups. Moreover, the requisite resources are lacking for the long-term updating and

maintenance of the app after completion.

(3) Under the current committee structure, committees are assigned to assist disadvantaged groups and promote a barrier-free environment. However, there is a lack of a committee or entity to monitor whether accessibility is achieved in the digital world.

Responses from the Candidate

(1) The need to train people working in the front line was added in Section 8.5.4 (*provide special concern/care for disadvantaged groups*) in Chapter 8.

(2) The need to develop a business model to sustainably maintain the mobile apps launched by the government was discussed in Section 8.5.3 (*Sustainability of improving digital inclusion*) in Chapter 8.

(3) To maintain continuous effort in digital inclusion, the need for a committee or entity monitoring whether accessibility is achieved in the digital world was added in Section 8.5.3 (*Sustainability of improving digital inclusion*) in Chapter 8.

9.4 Summary

This chapter summarizes the key mitigation/preventative measures derived from the expert questionnaire survey and three case studies. They were validated as being mostly important and useful by nine experts in the domain of SCs and refined (where shortfalls existed) according to the suggestions obtained through the validation interviews. These measures are expected to facilitate an improved development of SCs. The next chapter concludes this research and discusses the benefits of SCs upon resolution of the potential pitfalls.

CHAPTER 10 CONCLUSIONS

10.1 Introduction

This chapter concludes this research. The research objectives are reviewed together with their fulfillments. The conclusions summarize the main findings, highlighting the significance of this study from theoretical and practical perspectives. Moreover, this chapter presents the research limitations and suggestions for future research works.

10.2 Review of the research objectives

This study aims at identifying potential pitfalls with possible causes and adverse effects, and recommending proactive measures to help guide the implementation of SC progressively. The research objectives are summarized as follows:

(1) To identify potential pitfalls in the development of SCs;

(2) To identify possible causes and adverse effects of such pitfalls; and

(3) To provide recommendations to mitigate/prevent the associated problems.

10.3 Fulfillment of the research objectives

This research is divided into three stages, namely, (1) the identification of pitfalls based on a comprehensive literature review; (2) the analysis of possible causes and adverse effects through a questionnaire survey on SC experts and three case studies; and (3) the development of recommendations for a better SC development. Table 10-1 summarizes how the research objectives were realized and the outcomes.

Table 10-1 Research objectives and their fulfillment

Research objectives	**Method Used**	**Outcomes**
1. Identify potential pitfalls in the development of SCs.	Literature review (Chapter 2).	Common pitfalls were identified as: System information insecurity; Privacy leakage; Information islands; Digital divide.
2. Identify the possible causes and adverse effects of such pitfalls; 3. Provide recommendations to mitigate/prevent the associated problems.	A questionnaire survey (#1) on SC experts (Chapter 4).	Initial findings on the key issues to tackle (i.e. important causes of each pitfall) and effective measures were obtained.
	Case study 1(Chapter 5): (1) A questionnaire survey (#2) on mobile app users; (2) Interviews with stakeholders participating in the smart parking projects; (3) Interviews with disadvantaged groups as well as stakeholders helping the disabled.	(1) How users perceived these pitfalls within the context of mobile apps providing real-time parking information; (2) Why many carpark operators were not willing to share their real-time vacancy information; (3) What support is needed most by the disadvantaged groups.
	Case study 2 (Chapter 6): Reliability analysis of a SPIS using FFTA.	Possible mechanisms of service non-availability and the relative importance of events triggering it.
	Case study 3 (Chapter 7): SNA of barriers faced by stakeholders in the open data project to examine the rationale of the problem of information islands.	The interrelationships of barriers faced by different stakeholders involved in the open data project, and critical barriers to tackle.

On the basis of an extensive literature review, four pitfalls in the development of SCs have been identified. These pitfalls are as follows: (1) system information insecurity, (2) privacy leakage, (3) information islands, and (4) digital divide. Questionnaire survey # 1 for SC experts was then conducted for them to rate the relative importance of possible causes, adverse effects of each pitfall in terms of its likelihood, severity, and the effectiveness of mitigation measures. Initial findings on the key issues to tackle and effective measures to mitigate them were obtained at this stage. It was also affirmed that the problem about information islands calls for a different method to examine the stakeholder-related rationale instead of just letting the experts rank the relative importance of possible causes. Another finding was that interviews with some disadvantaged groups and stakeholders helping them were necessary to obtain more in-depth understanding and explanations on what support is needed most by disadvantaged groups.

Three case studies were conducted to investigate the four common pitfalls in the context of several SC projects in Hong Kong to empirically fulfill the second and third objectives (i.e., to identify the key factors leading to the pitfalls and mitigation measures against them). Data needed for the first case study were collected through questionnaire survey # 2 to investigate how users perceived these pitfalls in the context of mobile apps that provide real-time parking information. Following the questionnaire survey, several interviews were conducted with the following: (1) stakeholders participating in the smart parking app projects that were initiated in Hong Kong by the public and private sectors to identify the reasons why many carpark operators were unwilling to share their real-time vacancy information and (2) disadvantaged groups and organizations helping the disabled in Hong Kong to understand the causes of digital divide and find out possible solutions. The second case study investigated the pitfall of system information insecurity by analyzing the reliability of a SPIS. Through the use FFTA, the possible mechanisms of service non-availability were examined, and the relative importance of events causing service non-availability was evaluated. The third case study used SNA to investigate the interrelationships of barriers faced by different stakeholders involved in the project of open data, which is key to bridging information islands in emerging SCs. The key barriers with strategic positions in the network were identified, and the solutions that mitigate them were proposed accordingly.

10.4 Research conclusions

10.4.1 Preventative/mitigation measures against pitfalls

The development of SCs might cause damage to the society by risking the security of critical city systems, intruding citizens' privacy, forming information islands, and widening the digital gap. These pitfalls call for a holistic approach to mitigation or prevention.

System insecurity in SCs can be mitigated by technological and managerial measures to ensure the availability of critical city functions. Technological measures include deploying security by design, conducting due diligence to minimize any security risk of downstream contractors failing to meet their obligations, and complying with cybersecurity standards and other common and yet effective measures in daily operations.

These operations typically include deploying strong encryption, strengthening access control, backing up data by “all-site storage,” and renewing security methodologies and access rules of firewall. Management measures include preparing a recovery plan and conducting the drills of critical city functions and the stipulation of well-defined security policy to minimize human errors and providing regular training programs and good operational governance for employees.

Individual privacy must be safeguarded in SCs where citizens’ data are collected ubiquitously. The concept of Privacy by Design (PbD) is to be enforced in any SC initiative by embedding privacy as the default across the entire information life cycle of any information system. Stringent regulations supporting improved digital rights for citizens are needed. Meanwhile, aggregate information processing law or relevant regulations are expected to ensure privacy while realizing the potential of using more big data. Educating users is also necessary to instill awareness and the basic knowledge of proactively protecting digital privacy.

Bridging information islands in SCs relies on the development of open data policies that need efforts from different stakeholders. An open data policy should first set a phased approach to fulfill clear objectives and disseminate operational technical guidance. A better governance structure within the public sector is also needed to enforce data availability and integration. For the improvement of the usefulness of open data, the platform initiator or data managers should monitor data usage and enable users to give feedback. Moreover, for the enhancement of engagement from the private sector, motivation tools, such as a revenue model and conditions upon license renewal, can be used. NGOs and research institutes could contribute to forming an open data ecosystem by lobbying the private and public sectors to open their datasets for public access.

Narrowing the digital divide in developed cities (where owning a computer and accessing to the Internet is not a problem) mainly relies on the provision of suitable digital training that caters to the needs of SCs, and constructing a trustworthy environment, and positive mindset among users in the long run. Furthermore, keeping in-person services and improving the training of front-line staff that assist people with digital illiteracy are necessary. Digital inclusion is not only NGOs' task. Related organizations may need to be engaged in supporting the public to become proficient users and leave the status of digital novices. Continuous efforts for maintaining the current outcomes can be derived from sustained cooperation among different entities.

10.4.2 A holistic approach and sustainable strategies to develop SCs

Despite an increasing number of cities jumping on the SC bandwagon, SCs are still a territory in want of research. Intended outcomes are compromised by poor design and inefficient policies. Four pitfalls identified in this study indicate the need for a comprehensive vision of SC dimensions. Upon the improvement of reliability in performance of smart systems, privacy must be protected as a basic human right when a huge volume of data is being collected. The interoperability of data reinforces value-adding development and economic sustainability. Making the value or outcome of SC equally enjoyed by all groups helps ensure social justice and equity along with social sustainability. With the accumulation of research and practical experience in different domains, the concept and practice of SCs will mature over time.

In addition to the holistic approach to avoid pitfalls in developing SCs, sustainable strategies connecting stakeholders and different processes are also necessary. The government, as the initiator, sets policies based on the actual needs of the city. Following the policies, private service providers may develop commercially viable technologies and services for citizens, as well as the government. NGOs seek to change the conservative culture that obstructs Hong Kong to fulfill its SC ambition by lobbying the private and public sectors to open their datasets. NGOs also contribute to narrowing the digital divide by helping disadvantaged groups adjust to the SC environment. Well-balanced governance mechanisms with appropriate policies and novel business models might be used to further engage private entities. Meanwhile, the outcome of SC initiative must be clearly shown, and a feedback loop must be closed to refine the entire process.

10.5 Contributions of this study

10.5.1 Theoretical significance

On a theoretical basis, this study contributes to the conceptualization and implementation aspects of SCs. While most existing studies on SCs focus on the beneficial aspects, this study examined the possible downsides. Referring to existing definitions, this study has proposed its own concept of a SC, which emphasizes technology and social integration and suits the scope of this research. Under this concept, a SC is one that improves citizens' quality of life and social integration through the application of advanced information technologies, effective governance, and proactive solutions, which mitigate the potential pitfalls.

From the perspective of methodology, two quantitative methods have been used in this research besides non-parametric statistics using SPSS. The application of SNA identified the key barriers of open data development and enabled their dependencies to be visualized. Compared with the traditional factor ranking method, this network approach provides a better understanding on the chain effects between barriers faced by stakeholders. FFTA identified basic events causing a failure in the central server of a SPIS and determined their probabilities of occurrence when statistics were insufficient. FFTA coped with uncertainty by expressing failure probabilities in the form of linguistic judgments. This method also translated the physical system configuration into a logic structure, which shows scenarios in a system that would result in a failure.

10.5.2 Practical implications

This empirical research on the potential pitfalls of SC development covers technological and non-technological aspects, revealing challenges and suggesting proactive solutions. The proposed mitigation or preventative measures may be used as a reference by planners and managers of emerging SCs to avoid the possible downsides. It also contributes to the improvement of current SC performance assessment and development frameworks that used to focus only on the positive and functional aspects of SCs but sparingly evaluate the possible downsides. This study also investigated the roles of different stakeholders and the importance of their cooperation with one another. This research helps improve the governance and sustainable development of SCs.

10.6 Limitations of this research

(1) In the Case Study on mobile app users, 67.1% respondents had an education level of university and above. Although interviews have been carried out with poorly-educated elderly and other disadvantage groups to alleviate such “bias”, more diversified pools of respondents could be included in the survey to obtain a more comprehensive view.

(2) In Case Study 2, the top event of the fault tree was set as complete service non-availability caused by the central server failure. However, in reality, a common situation could be information inaccuracy caused by faults committed by a portion of the participating carpark operators at any one time. Given that reliability is a basic characteristic of information security, and it is impractical to assess the failure probability of hundreds of carparks operating various hardware and software, this research only focuses on the failure of the central server. The obtained failure rate might be a little bit higher than actual cases, as back-up servers are installed to provide redundancy in industries (hence increasing reliability).

(3) The effectiveness of several proposed measures is acknowledged to be limited under certain situations.

This research recommends the provision of suitable digital training as the main mitigation measure to narrow digital divide. However, based on findings from the expert questionnaire survey (Section 4.4.2.4), it is understood that personal attitude barrier is the predominant factor causing digital divide in Hong Kong or other emerging SCs. There are always people reluctant to attend digital training no matter how these training courses evolve. In addition to that situation, constructing a trustworthy environment and positive mindset among users is not easy, and it is inevitably a long-term effort. Therefore, the effectiveness of providing digital training is somewhat limited.

Another limitation lies in one of the measures protecting personal information. In Section 8.3.2, it was suggested that mobile app developers should use clear and concise language (in layman terms) to describe the privacy conditions so that users could understand how their data would be used and then make their own decisions of installing the app or not. However, in many mobile apps, services will not be provided if users do not agree with some terms such as accessing photos and contact lists, giving third parties their email addresses and numbers, etc. Users may trade off their personal information for convenience. In this case, the management of mobile app development or even the whole digital services industry needs a more thorough study beyond the scope of this research.

10.7 Suggestions for future research

(1) This research mainly draws upon the experience of emerging SCs, such as Hong Kong, where the bulk of data were collected. For mature SCs, such as Barcelona and London, the pitfalls and mitigation measures may be different. Therefore, future research may investigate SCs at different stages and compare the similarities and differences on a like-with-like basis.

(2) For Case Study 2, FFTA based on expert perceptions only was used to study the occurrence probability of basic events that might cause failure in the central server. Future

studies may evaluate the severity of basic events when they occur. Such studies may use empirical research methods, employing statistical data that may be accumulated over time by suppliers of IT systems.

(3) For Case Study 3, this research focuses on barriers pertaining to the launch of an open data project and its initial operation stage. Future studies may investigate whether the importance of the barriers and links in the network would change over time as a follow-up study to investigate the dynamic nature of the network. More stakeholders may be included in the study after some operational stages have been gone through, as Hong Kong continues to develop as a SC.

APPENDICES

Appendix 1. Survey Questionnaire #1: *a study of the potential pitfalls in the development of smart cities*

The approach of Smart City does benefit both urban living and management by enabling people to understand, monitor, and manage cities more efficiently and sustainably. However, some potential pitfalls (including **System Insecurity, Personal Privacy Leakage, Information Islands, and Digital Divide**) cannot be underestimated. This study aims at identifying potential pitfalls in the development of smart cities, investigating possible causes and providing mitigation measures. The questionnaire consists of Part A, B, C and D. It will take about 20 minutes to complete.

Part A- Background of Respondent

1. Region where you work.

   A. Hong Kong SAR　　B. Mainland China

   C. Other (please specify): __________________

2. What is your highest education level?

   A. Primary education　　B. Secondary education　　C. College or diploma

   D. University and above　　E. Other (please specify): __________________

3. Type of organization in which you are working:

   A. Public sector or related organization　　B. Private sector

   C. Non-Government Organization (NGO)　　D. Other (please specify): ____________

4. Nature of your work:

   A. Technology development/engineering　B. Project management　C. Marketing/Sale

   D. Customer service　　E. Academic　　F. Consultancy/Advisory

   G. Other (please specify): __________________

5. Position in your organization (optional): __________________

6. Years of working experience:

   A. Less than 2 years　　B. 2-4 years　　C. 5-10 years　　D. Over 10 years

7. How much do you know about Smart City?

   A. I have no idea about it.　　B. I know very little about it.

   C. I have some knowledge about it.　D. I know it very well.

8. Please name a Smart-City project in the world which you know about (if any):

____

Note: In the following parts (Part B, C and D), you are invited to rate: 1) the likelihood and severity of possible causes of each pitfall; 2) the severity of their adverse effects; and 3) effectiveness of mitigation measures against them. Four pitfalls have been identified based on literature review. Brief descriptions of them are for your reference only.

(1) System Information Insecurity: The correct performance and trustworthiness of a system for the desired purposes are unavailable.
(2) Personal Information Leakage: Data are accessed or used to extract users' sensitive information without permission, destroying the anonymity of information origin and disclosing the personal identities.
(3) Information Islands: Information systems that are isolated and incompatible mutually.
(4) Digital Divide: Unequal accessibility and capability to use information technologies among various groups.

Part B- Likelihood and Severity of Possible Causes

Please rate the Occurrence Likelihood and Severity (if it occurs) of causes of each pitfall by ticking a number from 1 to 5.

Pitfall	**Possible Causes of the Pitfall**	**Occurrence Likelihood**							**Severity (if it occurs)**					
		Very Low ↔ Very High					Don't know		Not severe at all ↔ Very severe					Don't know
		1	**2**	**3**	**4**	**5**			**1**	**2**	**3**	**4**	**5**	
System Information Insecurity	Weak security and encryption, security being an after-thought.													
	Cyber-attacks.													
	Large and interdependent systems with many stakeholders involved, making it difficult to ensure end-to-end security.													
	Errors in design.													
	Poor management and operation models of outsourcing products and services.													
	Limited security sponsorship and management support in the development of smart systems.													
	Using insecure legacy systems and poor maintenance.													
	Human errors and negligent staff.													

	Other(s), pls. specify:												
Personal Information Leakage	Heterogeneity and ubiquity of IoT-enabled system without providing notice and seeking consents of targets.												
	Unauthorized access to systems.												
	Insufficient awareness and knowledge on data protection of users.												
	Absence of strict standards/regulations to protect personal information.												
	Other(s), pls. specify:												
Information Islands	Incompatible data standards and formats.												
	Difficulty of engaging with a broad spectrum of stakeholders.												
	Insufficient cooperation and communications among stakeholders.												
	Independent development and non-integrated panning of IT application systems.												
	Closed government culture and risk-averse policy.												
	Other(s), pls. specify:												
Digital Divide	Insufficient provisions of physical access to Internet and digital services.												
	Computer ill-literacy and lack of skills.												
	Poor quality of services.												
	Personal attitude barriers and weak information awareness of citizens.												
	Lack of special care for disadvantaged groups.												
	Lack of training programs for unskilled citizens.												
	Insufficient engagement initiatives from the society.												
	Other(s), pls. specify:												

Part C- Adverse Effects of Pitfalls

Please rate the Severity (if it occurs) of each pitfall by ticking a number from 1 to 5.

Pitfall	Adverse Effects of the Pitfall (if it occurs)		Severity (if it occurs)					
			Not severe at all ↔ Very severe					Don’t know
			1	2	3	4	5	
System Information Insecurity	A system-wide failure and non-availability of essential services.							
	Breaching the confidentiality of users’ information.							
	Economic loss.							
	Other(s), pls. specify:							
Personal Information Leakage	Information exposure, citizen tracking and even impersonation.							
	Risking public trust towards the society and posing threat to democracy.							
	Economic loss.							
	Other(s), pls. specify:							
Information Islands	Replicated facilities, resources wasting and overlapping.							
	Reducing the efficiency of smart cities.							
	Causing inconvenience in residents’ life.							
	Other(s), pls. specify:							
Digital Divide	Widening social and economic inequality.							
	Reducing the effectiveness of smart cities.							
	Other(s), pls. specify:							

Part D- Effectiveness of Mitigation Measures against Pitfalls

Please rate the effectiveness of the following mitigation measures for Smart City Development, and indicate which stakeholder may implement it best referring to the stakeholders list below.

Pitfall	**Mitigation measures against Pitfall**		**Effectiveness**					
			Not effective at all ←→ Very effective					Don't know
			1	**2**	**3**	**4**	**5**	
System Information Insecurity	Management controls over operation and design.							
	General technical countermeasures such as frequent backup, anti-virus programs, software updates, firewalls against intruders.							
	Employing/developing well-defined standards for developing and managing ICT services.							
	Improving security awareness and availability safeguards, conducting continuous vulnerability assessment.							
	Developing a cyber-security strategy and recovery plan.							
	Other(s), pls. specify:							
Personal information leakage	Establishing standards on how public data could be collected and used.							
	Utilizing education and training to help improve users' knowledge and awareness of information privacy; and informing developers their responsibilities and best exercises.							
	Legislation to allow users to control their own data and create a regulatory environment.							
	Employing Privacy by Design (PbD).							
	Conducting Privacy Impact Assessments (PIA).							
	Other(s), pls. specify:							
Information Islands	Sharing interoperable protocols among tech suppliers.							
	Formulating open standards and improving data quality.							
	Promoting cross-sectional collaboration among different interfacing organizations.							
	Planning the process of systems and data integration at the design stage.							
	Other(s), pls. specify:							

Digital Divide	Increasing network coverage and the penetration of digital devices.							
	Providing financial support for computer acquisition or Internet access and decreasing telecommunications charges.							
	Providing education and training, facilitate social learning to the public.							
	Improving public services for disadvantaged groups and enhancing their information literacy.							
	Motivating digital inclusion initiatives of both citizens and private sectors.							
	Other(s), pls. specify:							

Further comments on the Smart City Development in your region (optional):

Name and contact Email for receiving summary statistics (optional):_______________________

-The End-

Thank you very much!

Appendix 2. Survey Questionnaire #2: mobile applications (Apps) for finding a parking vacancy

Smart cities provide time-saving facilities to their residents. For example, the “Energizing Kowloon East Office” of the Hong Kong Government has developed a smart carparking system via an APP called “MyKE” for installation on smart phones. This APP provides real-time (instantly updated) parking space information in the area of Kowloon East, with anticipation to be extended to cover the whole Hong Kong in future. This survey is to understand your expectations and perceptions on the smart apps for finding real-time parking vacancies, as well as your understanding of smart city issues in Hong Kong. There are **16** questions in this survey. It takes about **10 minutes** to complete this survey questionnaire that includes **Parts A and B.**

Part A. Respondent background

1. What is your gender?

   A. Female B. Male

2. What is your age range?

   A.18~30 B. 31~45 C. 46~60 D. Above 60

3. What is your highest education level?

   A. Primary education B. Secondary education C. College or diploma

   D. University and above E. Other (please specify): ________________________

4. Driving experience:

   A. Not at all B. Less than 1 year C. 1~3 years

   D. 4~10 years E. More than 10 years

Part B. Expectations on parking apps and understanding about smart cities

5. Do you know about any system or application for finding a parking vacancy? (you may choose multiple answers)

   A. My Kowloon East – MyKE B. Hong Kong eRouting

   C. Sino Parking D. Wilson Parking (HK)

   E. You know about none of them.

   F. Other system or application you know, please specify: __________________________

6. Which of the following functions would you like to have in the mobile app for finding a parking vacancy? (you may choose multiple answers)

   A. Real-time parking vacancy B. Real time Traffic condition

   C. Route guidance/direction D. Advance booking parking lots

E. Parking charge information

F. Extra functions apart from the above description, please specify: ____________________

7. Please rate the relative importance of the following factors when you decide whether to use a parking APP.

1= Not important at all ↔ 5=Very important

A. My phone is able to run it (__)　　B. It is free of charge or low-cost (__)

C. It is stable/reliable (__)　　D. It covers the information of a wide area (__)

E. It is easy to use (__)　　F. Its information is accurate/up to date (__)

G. It doesn't seem to leak my personal information (__)

Any extra factor for you to decide whether to use a parking app (apart from those in Q.7 above): ____________________________

8. Do you read the disclaimers/conditions when you download and install mobile applications?

A. Never (Pls. go to Q.10 below).　B. Yes, but just sometimes.

C. Yes, I read it carefully every time I download and install my applications.

9. Will you give up downloading and installing a mobile app just because you don't accept the disclaimers/conditions?

A. Never. B. Yes, but just sometimes.　C. Yes, always.

10. Which personal information you do not want to give away when you download/use mobile apps? (you may choose multiple answers. **Not** every existing system collects such information.)

A. Location (tracking)　B. Email address　C. Phone no.

D. Account of social media such as Facebook and WeChat

E. Other(s): _____________________

11. How often do you use e-services or mobile services in your daily life, such as online shopping, mobile map, etc.? **1= Never ↔ 5=Always**

A. 1 (Pls. go to Q13 below)　B. 2　C. 3　D. 4　E. 5

12. How do you usually feel about using current e-services or mobile services, such as online booking, mobile navigation, etc.? **1= Very easy ↔ 5= Very difficult**

A. 1　B. 2　C. 3　D. 4　E. 5

13. Would you mind if you have to use different Apps for finding parking vacancies when you go to different districts in Hong Kong?

1= Do not mind at all ⟷ 5= Very much

A. 1 B. 2 C. 3 D. 4 E. 5

14. Which one of the following groups do you know best as being helped by the HK government in promoting their use of information technology?

A. None B. Elderly C. Visually impaired

D. Physically disabled E. Hard of hearing

F. Other groups, please specify: ____________________________

15. How do you feel about your involvement and participation in the HK's Smart City initiative?

A. I know nothing about it

B. I heard about it but have no interest

C. I am very interested in it but not involved

D. I participate in public forums to voice out my views.

E. I am involved in other ways (please specify: ______________________________)

16. Smart City aims at improving people's life quality using information technologies. Do you have the following concerns about the Smart City trend? (you may choose multiple answers)

A. Information insecurity (e.g. cyber-attacks, system break-down)

B. Personal data leakage

C. Lacking ability to use advanced information technology

D. Information non-integration (e.g., too many platforms, each providing incomprehensive information)

E. No, I don't worry any of them, since benefits outweigh such worries.

F. Other concerns about smart cities, if any, please specify: ____________________________

-END-

Survey Questionnaire #2: mobile applications (Apps) for finding a parking vacancy (Chinese Version for Locals)

調查問卷：關於智慧停車系統的應用程式（APP）

智慧城市致力於為居民生活提供高科技設施，以達至便利和節省時間。例如，“起動九龍東辦事處”研發了一款關於智慧停車場系統的應用程式 （APP），通過 “MyKE”APP 安裝在手機上，提供九龍東區域的停車場即時車位資訊，並期待將來能夠覆蓋全港。此部分研究目的是搜集您對實時（及時更新）泊車資訊之意見，以及對智慧城市之理解。調查問卷包括 A 及 B 部分，總共 16 個問題，完成大約需要 10 分鐘。

A 部分：受訪者簡介

1. 性 別：

   A. 女 B. 男

2. 年齡：

   A. 18~30 歲 B. 31~45 歲 C. 46~60 歲 D. 60 歲 以上

3. 教育程度：

   A. 小學教育 B. 中學教育 C. 專上 D. 大學及以上

   E. 其他（請註明）：________________

4. 駕車年数：

   A. 無 B. 少於 1 年 C. 1~3 年 D. 4~10 年 E. 超過 10 年

B 部分：對實時泊車資訊之意見，以及對智慧城市之理解。

5. 您知道以下用來尋找泊車位的信息系統或者 APP 嗎？（您可以選擇一個或以上答案）

   A. My Kowloon East – MyKE B. Hong Kong eRouting（香港行車易）

   C. Sino Parking（信和停车场） D. Wilson Parking (HK)（威信停車場）

   E. 以上都不知道

   F. 其它系統或者軟件，請註明：________________

6. 您希望泊車 APP 具備以下哪些功能？（您可以選擇一個或以上答案）

   A. 提供實時泊車空位數目 B. 提供實時交通狀況 C. 路線導航

   D. 提前預定泊車空位 E. 提供泊車費用資訊

   F. 其餘功能，請註明：________________

7. 請評價以下因素對於您決定是否使用某一泊車 APP 之重要性。

   1=一點都不重要 ↔ 5=非常重要

   A. 手機可以運行該 APP( ) B. 該 APP 可以免費使用或者收費較低( )

   C. 該 APP 穩定可靠( ) D. 該 APP 包含了較大區域範圍內的泊車資訊( )

   E. 該 APP 很容易使用( ) F. 該 APP 的信息準確，更新快( )

   G. 該 APP 不會泄露我的個人資訊( )

   其餘重要因素（除了以上 Q7 列舉的因素）， 請註明：________________

8. 下載以及安裝移動 APP 時，您是否會閱讀免責聲明/條款？

A. 從不（請跳去以下 Q10）　　B. 有時候會

C. 是的，每一次下載以及安裝時我都認真閱讀

9. 您會由於不接受免責聲明/條款而放棄下載以及安裝移動 APP 嗎？

A. 從不　B. 有時候會　C. 是的，總是

10. 當下載或使用移動 APP 時，您不願意洩露下列哪項個人資訊？（您可以選擇一個或以上答案， 現有的泊位系統並不是必須收集這些信息）

A. 地理位置（追蹤） B. 電郵地址　C. 電話號碼

D. 社交媒體賬號，例如 Facebook，微信

E. 其他個人信息，請註明：___________

11. 日常生活中，您會使用信息服務或者移動 APP 嗎？(例如網上購物，手機地圖等)

1=從不 ←→ 5=總是

A. 1（請跳去以下 Q13）　B. 2　C. 3　D. 4　E. 5

12. 使用現時的信息服務或者移動 APP 時（例如網上購物，手機導航等），您的感受是？

1=非常容易 ←→ 5=非常困難

A. 1　B. 2　C. 3　D. 4　E. 5

13. 當您駕車去本港**不同**的地方時，您介意使用**不同**的移動 APP 尋找泊車空位嗎？

1=一點都不介意 ←→ 5=非常介意

A. 1　B. 2　C. 3　D. 4　E. 5

14. 您最瞭解香港政府在以下 哪個群體中 協助推行資訊科技項目的使用？

A. 沒有 B. 長者 C. 視障人士 D. 行動不便人士 E. 聽障人士

F. 其他群體，請註明：__________________________

15. 關于香港建設智慧城市之倡議，您感覺自己對此的參與程度如何？

A. 我完全不了解香港智慧城市之建設。

B. 我聽說過香港智慧城市之建設，但是沒有興趣。

C. 我對香港的智慧城市建設很興趣，但是沒有參與其中。

D. 我通過公衆討論會來表達自己的觀點。

E. 我通過其它方式來參與其中，請註明是何種方式：______________________

16. 智慧城市致力於通過信息科技來提升人們的生活質量。您對於智慧城市有以下的擔憂嗎？（您可以選擇一個或以上答案）

A. 系統信息不安全 （例如網絡攻擊，系統崩潰）。 B. 個人资訊泄露。

C. 市民缺乏使用先進信息科技的能力。

D. 信息過于分散 （例如存在許多平台和 App，每一個提供不完整的信息）。

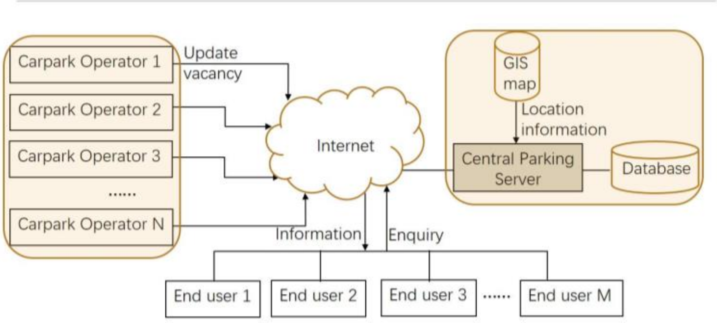
E. 我不擔心這些問題，因為智慧城市帶來的好處超過了這些顧慮。

F. 您的其他擔憂，請註明：__________________________

———— **問卷完，謝謝您的配合！** ————

Appendix 3. Questionnaire Survey#3: *reliability analysis of a smart parking information system*

Smart Parking Information System is designed to facilitate drivers to find parking vacancies. In most smart parking information systems (as shown in the Fig below), two sides are included: 1) **central parking server** which stores, manages and disseminates the parking information like real-time vacancy, location, opening hours; and 2) **individual carpark operators** which upload real-time vacancy number to the central system. End-users obtain the parking information via internet-connected devices.



This questionnaire aims at collecting your opinion about the **occurrence probability** of each **event** that may lead to the service non-availability of central parking server. It includes part A and B, and will take about 10 minutes to complete.

Part A- Background of Respondent

1. Region where you work:

   A. Hong Kong SAR B. Mainland China C. Other (pls. specify): ________________

2. What is your highest education level?

   A. Primary education B. Secondary education C. College or diploma

   D. University and above E. Other (please specify): __________________

3. Type of organization in which you are working:

   A. Public sector or related organization B. Private sector

   C. Non-Government Organization (NGO) D. Other (pls. specify): __________________

4. Nature of your work:

   A. Technology development/engineering B. Project management

   C. Marketing/sale D. Customer service E. Academic

   F. Consultancy/advisory G. Other (pls. specify): ______________________

5. Years of working experience in Information Technology and Electronic Engineering:

   A. Less than 2 years B. 2-4 years C. 5-10 years D. Over 10 years

6. How much do you know about smart parking information system?

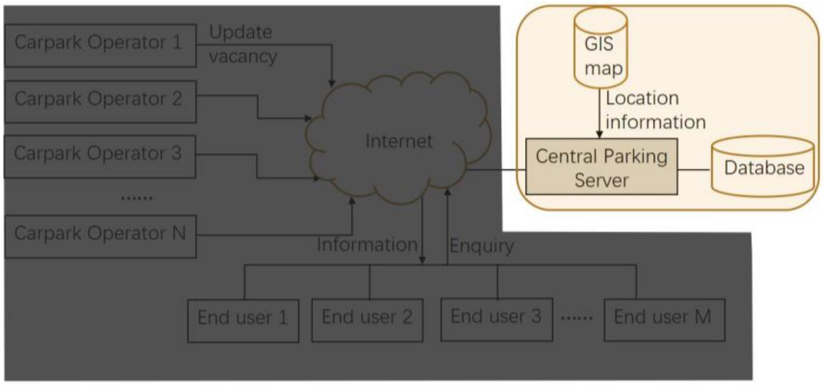
   A. I have no idea about it. B. I know very little about it.

   C. I have some knowledge about it. D. I know it very well.

7. Please name a smart parking information system/platform/App which you know about and where it is applicable (if any): ______________________________________

Part B. Failure Assessment in the Central System Server

Please rate the **Occurrence Probability** of each basic event that may lead to the non-availability in the ***central parking server*** (as highlighted in below Fig) by ticking a number from 1 to 5.



(Focus of Part B)

Category	**Basic Event Leading to the Service Non-availability**	**Occurrence Probability**					
		Very Low ←→ Very High					Don't know
		1	2	3	4	5	
Malicious Attacks	Security Violations (e.g. Dos, DDoS, Ransomware)						
	Firewall Failures						
	Recovery Delays						
Human Errors	Malicious Behaviors of Employees (insider attack)						
	Procedural/operation Errors (e.g. deleting files by mistake, incorrect input)						
Hardware Failures (non-malicious)	Computer Down						
	Communication Device Down (e.g. router down, link broken)						
Software Failures (non-malicious)	Data Corruption (e.g. errors in Database tables)						
	Application Software Failures (e.g. web server failure, Database engine failure)						
	Operating System Failures (e.g. Bugs)						

-The End. Thank you very much! -

Appendix 4: Validation Questionnaire Sample

PhD Research: A Study of Potential Pitfalls in the Development of Smart Cities and Mitigation Measures

This study aims at investigating potential pitfalls in the development of smart cities and recommending mitigation measures accordingly. The 4 identified pitfalls include system insecurity, personal privacy leakage, information islands and digital-divide. Brief descriptions of them are for your reference only.

System information insecurity	The correct performance of a system for its desired purposes are unavailable.
Personal information leakage	Data is accessed or used to obtain users' sensitive information/identities without permission.
Information islands	Information systems that are isolated and incompatible mutually.
Digital divide	Unequal accessibility and capability to use information technologies among various groups.

Through questionnaire surveys, interviews with relevant experts and stakeholders and contextual case studies, corresponding mitigation measures are proposed as follows:

1. Mitigation measures against city-wide information system security

Critical issue to be solved	**How to mitigate/prevent**	**Who**	**When**	**Derived from**
1. Security being an afterthought	(1) Promote security by design; (2) Comply with established international standards and IT security policies;	The government; system designers and operators.	Throughout the system design, operation and maintenance.	Questionnaire survey#1 on SC experts (Chapter 4).
2. Hardware failure	(3) Back up data regularly; (4) Have a recovery plan detailing instant responses and clear division of responsibilities; (5) Prepare for redundant servers and extra power suppliers.	System designers, operators, users.	During the operation stage.	Reliability analysis of SPIS (case study 2, Chapter 6).

3. Security violations	(3) to (5) above also apply;
	(6) Conduct up-to-date anti-virus checking;
	(7) Renew security methods and access rules of firewall;			

4. Human errors	(8) Have a well-defined security policy; (9) Instill employees with a security mind-set through regular training programs; (10) Impose strict technical monitor and management protocol.	System operators, users.	During the operation stage.	

2. Mitigation measures against massive personal information leakage

Critical issue to be solved	How to mitigate/prevent	Who	When	Derived from
1.Ubiquitous data collection;	(1) Incorporate PbD by restricting the amount/type of data collected and anonymize the data; setting a definite validity time period; getting users' consent to collect their data.	The government; system operators; contractors/IT service providers.	Throughout the design, operation, and management stage.	Questionnaire survey#1 on SC experts (Chapter 4).
2. Absence of strict standards/regulations to protect personal data	(2) Move towards strict standards/regulations which impose stringent requirements on the collection and processing of personal data in increasingly data-driven environments; (3) Clarify and enforce more "digital rights" for citizens.	The government.	During the design and operation stage.	Questionnaire survey#1 on SC experts (Chapter 4).
3. Insufficient awareness and knowledge on privacy protection of users	(4) Instill the general idea of protecting digital privacy through more diverse channels in appealing ways (such as dramatized TV broadcast); (5) Promote a privacy-aware culture for employees who deal with data collection and processing.	The government; NGOs; citizens as users; private entities related to data analytics.	Throughout the SC development.	Questionnaire survey#2 on mobile app users (case study 1, Chapter 5).

3. Mitigation measures against public information islands

Critical issue to be solved	How to mitigate/prevent	Who	When	Derived from
1. Scattered data management across B/Ds	(1) Renew the governance structure to enforce open data development.	The initiator (OGCIO in this research); public departments as data providers.	During the design stage.	SNA of the barriers faced by stakeholders in the open data project (case study 3, Chapter 7).
2. Lack of open data policy	(1) above also applies; (2) Set proper objectives; (3) Provide more technical guidance such as data format, updating frequencies, data ownership; (4) Diversify financial resources to improve systems in the public sector; (5) Issue specific licenses (e.g. Open Database License) for functional open data.			
3. Lack of public participation	(6) Enable users to give feedback on specific datasets that need updating and refining, as well as suggest desirable datasets for specified purposes;	Users, the initiator.	Throughout the operation stage.	
	(7) Monitor open data usage to analyze the data relevance and usefulness.	The initiator.		
4. Insufficient motivation of (potential) data providers	(8) Use new revenue model or contractual measures to encourage private entities to open up data.	The initiator; private data providers and NGOs.	During the design stage.	

4. Mitigation measures against digital divide in the society

Critical issue to be solved	How to mitigate/prevent	Who	When	Derived from
1. Attitude barriers towards ICT; 2. Lack of helpful training programs for unskilled citizens	(1) Identify the digital gap and target groups; (2) Stakeholder engagement: a coordinator (e.g. OGCIO) and strategic partners including NGOs and private companies that provide digital services;	The government.	At the design stage.	Questionnaire survey#1 on SC experts (Chapter 4); Questionnaire survey#2 on mobile app users (case study 1, Chapter 5).
	(3) Organize digital inclusion activities as part of the services of private IT companies to attract more potential users;	Private entities.	At the operation stage.	
	(4) Update digital-skill courses in communities, and teach effective measures to ensure cybersecurity and protect privacy;	NGOs; users.		
3. Insufficient special concern/care for disadvantaged groups	(5) Continue requisite resources for updating and maintaining the apps or other development;	The government; NGOs; private entities.	At the operation stage.	
	(6) Keep in-person service provisions in some common and well publicized places;	Service providers.	At the operation stage.	

After reading Page 1 to 3, please help to complete the following in the next page:

1. Type of organization in which you are working:

A. Public sector or related organization B. Private sector

C. Non-government organization

2. Nature of your work:

A. Project management B. Marketing/Sale

C. Customer service D. Academic

E. Consultancy/advisory F. Other (please specify): ________________

3. Years of work experience: __________________

4. Position in your organization (optional): __________________

5. Your evaluation of the recommendations arising from this research:

Validation criteria	Not agree at all ↔ Totally agree				
	1	2	3	4	5
A. Relevance & Importance					
The pitfalls identified in this study exist in reality.					
The pitfalls identified in this study are comprehensive.					
The pitfalls identified may bring significant adverse effects to the society.					
B. Practicality					
The proposed mitigation measures are clear and understandable.					
The proposed mitigation measures are implementable in most circumstances.					
C. Effectiveness & Adequacy					
The proposed measures would be effective to mitigate pitfalls in smart cities.					
This study would help guide healthier implementation of smart cities.					
The parties recommended for taking the stated actions are appropriate					

5. Your comments regarding this research (or the mitigation measures):

-The End-

REFERENCES

Abella, A., Ortiz-De-Urbina-Criado, M., and De-Pablos-Heredero, C. (2017). A model for the analysis of data-driven innovation and value generation in smart cities' ecosystems. *Cities, 64*, 47-53.

Agudelo, J. P., and Barrera, H. E. C. (2014, June 4-6). *Approach for a Congestion Charges System Supported on Internet of Things.* Paper presented at the IEEE Colombian Conference on Communications and Computing (COLCOM), Bogota, Colombia.

Ahvenniemi, H., Huovila, A., Pinto-Seppä, I., and Airaksinen, M. (2017). What are the differences between sustainable and smart cities? *Cities, 60*, 234-245.

Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-García, J., Leung, S., Mellouli, S., Nam, T., Pardo, T., Scholl, H., and Walker, S. (2012, September 3). *Building understanding of smart city initiatives.* Paper presented at the International conference on electronic government, Berlin, Heidelberg.

Albino, V., Berardi, U., and Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology, 22*(1), 3-21.

Allwinkle, S., and Cruickshank, P. (2011). Creating smart-er cities: An overview. *Journal of Urban Technology, 18*(2), 1-16.

Ameyaw, E. E., and Chan, A. P. (2015). Risk ranking and analysis in PPP water supply infrastructure projects: an international survey of industry experts. *Facilities, 33*(7/8), 428-453.

Andreasson, K., and Jian, Y. (2015). China's Digital Divides and Their Countermeasures *Digital Divides: The New Challenges and Opportunities of e-Inclusion* (pp. 65-78): CRC Press.

Angelidou, M. (2014). Smart city policies: A spatial approach. *Cities, 41*, S3-S11.

Anthopoulos, L. (2017). Smart utopia VS smart reality: Learning by experience from 10 smart city cases. *Cities, 63*, 128-148.

ARUP and RIBA. (2013). Designing with data: Shaping our future cities. Retrieved from https://www.architecture.com/Files/RIBAHoldings/PolicyAndInternationalRelations/Policy/Designingwithdata/Designingwithdatashapingourfuturecities.pdf [Accessed: 19 Jan 2016].

Arzberger, P., Schroeder, P., Beaulieu, A., Bowker, G., Casey, K., Laaksonen, L., Moorman, D., Uhlir, P., and Wouters, P. (2004). An international framework to promote access to data. *Science, 303*(5665), 1777-1778.

Ashibani, Y., and Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, 68*, 81-97.

Attard, J., Orlandi, F., Scerri, S., and Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly, 32*(4), 399-418.

Bélanger, F., and Carter, L. (2009). The impact of the digital divide on e-government use. *Communications of the ACM, 52*(4), 132-135.

Barry, E., and Bannister, F. (2014). Barriers to open data release: A view from the top. *Information Polity, 19*(1, 2), 129-152.

Batty, M. (2013). Big data, smart cities and city planning. *Dialogues in Human Geography, 3*(3), 274-279.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G., and Portugali, Y. (2012). Smart cities of the future. *The European Physical Journal Special Topics, 214*(1), 481-518.

Berghmans, P., and Van Roy, K. (2011). Information Security Risks in Enabling e-Government: The Impact of IT Vendors. *Information Systems Management, 28*(4), 284-293.

Bigelow, S. J. (2011). The causes and costs of data center system downtime: Advisory Board Q&A. Retrieved from http://searchdatacenter.techtarget.com/feature/The-causes-and-costs-of-data-center-system-downtime-Advisory-Board-QA [Accessed: 28 Mar 2018].

Bigelow, S. J. (2013). Hardware and software approaches to improve virtual server reliability. Retrieved from http://searchservervirtualization.techtarget.com/answer/Hardware-and-software-approaches-to-improve-virtual-server-reliability [Accessed: 28 Mar 2018].

Blakemore, M., and Craglia, M. (2006). Access to public-sector information in Europe: Policy, rights, and obligations. *The Information Society, 22*(1), 13-24.

Boorsma, B. (2016). Digitization: Challenges & Opportunities. Retrieved from https://blogs.cisco.com/government/digitization-challenges-opportunities [Accessed: Jan 29 2018].

Boorsma, B. (2017). The 12 Pitfalls of Smart City Efforts of the Past - and what we can learn from them. Retrieved from https://anewdigitaldeal.com/158/the-12-pitfalls-of-smart-city-efforts-of-the-past-and-what-we-can-learn-from-them [Accessed: Jan 23 2018].

Bosch, P., Jongeneel, S., AIT, H.-M. N., and Airaksinen, M. (2016). CITYkeys indicators for smart city projects and smart cities. Retrieved from http://nws.eurocities.eu/MediaShell/media/CITYkeysD14Indicatorsforsmartcityprojectsandsmartcities.pdf [Accessed: Oct 30 2018].

Botha, N., Small, B., Crutchley, P., and Wilson, J. (2001). Addressing the rural digital divide in New Zealand. *Social Systems Research Unit, AgResearch Ltd.*

Braun, T., Fung, B. C., Iqbal, F., and Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable cities and society, 39*, 499-507.

Buckbee, M. (2018). GDPR Requirements in Plain English. Retrieved from https://blog.varonis.com/gdpr-requirements-list-in-plain-english/ [Accessed: 29 Sep 2018].

Cairney, T., and Speak, G. (2000). *Developing a Smart City: Understanding Information Technology Capacity and Establishing an Agenda for Change*: Centre for Regional Research and Innovation, University of Western Sydney.

Calzada, I., and Cobo, C. (2015). Unplugging: Deconstructing the smart city. *Journal of urban technology, 22*(1), 23-43.

Caragliu, A., Del Bo, C., and Nijkamp, P. (2011). Smart cities in Europe. *Journal of urban technology, 18*(2), 65-82.

Cardon, A. H. (1996). *Durability Analysis of Structural Composite Systems: Reliability, risk analysis and prediction of safe residual structural integrity-Lectures of the Special Chair AIB-Vincotte 1995*: CRC Press.

Cassandras, C. G. (2016). Smart cities as cyber-physical social systems. *Engineering, 2*(2), 156-158.

Cavoukian, A., Polonetsky, J., and Wolf, C. (2010). SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society, 3*(2), 275-294.

Centre for Economics and Business Research. (2015). The economic impact of Basic Digital Skills and inclusion in the UK. Retrieved from https://goon-uk-prod.s3-eu-west-1.amazonaws.com/uploads/The%20economic%20impact%20of%20digital%20skills%20and%20inclusion%20in%20the%20UK_Final_23_11_15.pdf [Accessed: 18 July 2017].

Cerrudo, C. (2015). An emerging US (and world) threat: Cities wide open to cyber attacks.

Securing Smart Cities. Retrieved from https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_cyber-security_CesarCerrudo.pdf [Accessed: 29 Oct 2018].

Chan, A. P., Chan, D. W., and Ho, K. S. (2003). Partnering in construction: critical study of problems for implementation. *Journal of Management in Engineering, 19*(3), 126-135.

Chan, H., and Perrig, A. (2003). Security and privacy in sensor networks. *Computer, 36*(10), 103-105.

Chan, W. K. O. (2017). Living up to the smart city dream. Retrieved from http://www.chinadaily.com.cn/hkedition/2017-08/18/content_30763049.htm [Accessed: 13 Sep 2018].

Chang, H. S., and Yang, H. M. (2010). Public acceptance of the Cyber Taipei initiative and cyber-government services. *Habitat International, 34*(2), 210-218.

Chatzigiannakis, I., Vitaletti, A., and Pyrgelis, A. (2016). A privacy-preserving smart parking system using an IoT elliptic curve based security platform. *Computer Communications, 89*, 165-177.

Cheang, L. S., and Lei, G. (2015). Digital inclusion: the Singapore Perspective. *Digital Divides: The New Challenges and Opportunities of e-Inclusion, 195*, 149.

Cheliyan, A., and Bhattacharyya, S. (2017). Fuzzy fault tree analysis of oil and gas leakage in subsea production systems. *Journal of Ocean Engineering and Science, 3*(1), 38-48.

Chen, S., and Hwang, C. (1992). Fuzzy multiple attribute decision making methods *Fuzzy multiple attribute decision making* (pp. 289-486). Berlin, Heidelberg: Springer.

Cheung, E. (2009). *Developing a best practice framework for implementing public private partnerships (PPP) in Hong Kong (Unpublished doctoral dissertation).*

Queensland University of Technology, Queensland, Australia.

Chinnaiyan, R., and Somasundaram, S. (2010). Evaluating the reliability of component-based software systems. *International Journal of Quality & Reliability Management, 27*(1), 78-88.

Chouffani, R. (2016). Common failures of responding to security breaches in healthcare. Retrieved from http://searchhealthit.techtarget.com/tip/Common-failures-of-responding-to-data-breaches-in-healthcare [Accessed: 27 Mar 2018].

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., and Scholl, H. J. (2012). *Understanding smart cities: An integrative framework.* Paper presented at the 45th Hawaii International Conference on System Science (HICSS).

Cisco. (2015). The Internet of Things, Infographic. Retrieved from http://blogs.cisco.com/diversity/the-internet-of-things-infographic [Accessed: 23 Sep 2016].

City of New York. (2018). Open Data Policy and Technical Standards Manual. Retrieved from https://opendata.cityofnewyork.us/wp-content/uploads/2018/04/Open-Data-Policy_TSM_v1.4_FINAL_04.02.18-1.pdf [Accessed: 13 Sep 2018].

Clapp, R. (2010). What does availability/uptime mean in the real world? Retrieved from https://interworks.com/blog/rclapp/2010/05/06/what-does-availabilityuptime-mean-real-world/ [Accessed: May 9 2018].

Clifford, S., and Hardy, Q. (2013). Attention, Shoppers: Store Is Tracking Your Cell. Retrieved from http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=1 [Accessed: 23 May 2016].

Cloud Security Alliance. (2016). Future-proofing the Connected World: 13 Steps to

Developing Secure IoT Products. Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf [Accessed: 26 Nov 2016].

Cocchia, A. (2014). Smart and digital city: a systematic literature review *Smart City: How to Create Public and Economic Value with High Technology in Urban Space* (pp. 13-43). Cham: Springer International Publishing.

Colding, J., and Barthel, S. (2017). An urban ecology critique on the "Smart City" model. *Journal of Cleaner Production, 164*, 95-101.

Colmenar, E., Muslim, A., and Dara, R. (2014, June 1-4). *Open data offers open opportunities: A case study on improving aid management.* Paper presented at the 2014 IEEE Canada International Humanitarian Technology Conference - (IHTC), Montreal, QC.

Commerce and Economic Development Bureau. (2013). 2014 Digital 21 Strategy: Smarter Hong Kong, Smarter Living. Retrieved from http://www.digital21.gov.hk/eng/ [Accessed: 16 Oct 2017].

Conradie, P., and Choenni, S. (2012, October 22 - 25). *Exploring process barriers to release public sector information in local government.* Paper presented at the Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance, New York, USA.

Conradie, P., and Choenni, S. (2014). On the barriers for local government releasing open data. *Government Information Quarterly, 31*, S10-S17.

Cooley, D. (2014). London tests pedestrian sensors to make crossing streets safer. Retrieved from https://smartcitiescouncil.com/article/london-tests-pedestrian-sensors-make-crossing-streets-safer [Accessed: 25 June 2018].

Cordella, A., and Willcocks, L. (2010). Outsourcing, bureaucracy and public value:

Reappraising the notion of the “contract state”. *Government Information Quarterly, 27*(1), 82-88.

Cuervo, M. R. V., and Menéndez, A. J. L. (2006). A multivariate framework for the analysis of the digital divide: Evidence for the European Union-15. *Information & Management, 43*(6), 756-766.

Cullen, R. (2001). Addressing the digital divide. *Online information review, 25*(5), 311-320.

Daniel, W. W. (1978). *Applied nonparametric statistics*. Boston: Houghton Mifflin.

Development Bureau. (2015). *Developing Kowloon East into a Smart City District – Feasibility Study (Agreement No. CE 56/2015)*. Hong Kong SAR: Development Bureau.

Dirks, S., Keeling, M., and Dencik, J. (2009). How smart is your city?: Helping cities measure progress. *IBM Institute for Business Value, IBM Global Business Services, New York*.

Doyle, L. (2017). Software-based networking brings new automation perks, challenges. Retrieved from http://searchdatacenter.techtarget.com/feature/Software-based-networking-brings-new-automation-perks-challenges [Accessed: 27 Mar 2018].

Dutton, W. H., and Blank, G. (2015). Cultural stratification on the Internet: Five clusters of values and beliefs among users in Britain *Communication and Information Technologies Annual* (pp. 3-28): Emerald Group Publishing Limited.

Dutton, W. H., and Reisdorf, B. C. (2017). Cultural divides and digital inequalities: attitudes shaping Internet and social media divides. *Information, Communication & Society*, 1-21.

Edmunds, S. (2015). Comment on the revamped Data.Gov.HK site. Retrieved from https://opendatahk.com/2015/03/data-gov-hk-site/ [Accessed: 19 May 2018].

Edmunds, S. (2018). Hong Kong's parking data failure. Retrieved from https://opendatahk.com/2018/01/parking-data/ [Accessed: 28 Aug 2018].

Edwards, L. (2016). Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. *European Data Protection Law Review, 2*(1), 28-58.

Elmaghraby, A. S., and Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research, 5*(4), 491-497.

Energzing Kowloon East Office. (2017). Smart City @Kowloon East. Retrieved from http://www.ekeo.gov.hk/en/smart_city/index.html [Accessed: 5 Dec 2017].

European Commission. (2011). Open data: an engine for innovation, growth and transparent governance. Retrieved from https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/viv8th9rn0zy [Accessed: Oct 30 2018].

European Union Agency for Network and Information Security (ENISA). (2014). Privacy and Data Protection by Design - from policy to engineering. Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design [Accessed: 6 Nov 2016].

Expósito-Izquierdo, C., Expósito-Márquez, A., and Brito-Santana, J. (2017). Mobility as a Service. *Smart Cities: Foundations, Principles, and Applications* (pp. 409-415). Hoboken, USA: John Wiley & Sons, Inc.

Ferraz, F. S., and Ferraz, C. A. G. (2014, December 8-11). *Smart city security issues: depicting information security issues in the role of an urban environment.* Paper presented at the IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC), London.

Finney, N. K. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. *Parameters, 44*(3), 149-151.

FireMon, L. (2016). Whitepaper: Firewall cleanup recommendations Retrieved from https://www.firemon.com/resources/collateral/firewall-cleanup/ [Accessed: 27 Mar 2018].

Fuchs, C. (2009). The role of income inequality in a multivariate cross-national analysis of the digital divide. *Social Science Computer Review, 27*(1), 41-58.

Fylan, F. (2005). Semi-structured interviewing. *A handbook of research methods for clinical and health psychology*, 65-78.

Galdon-Clavell, G. (2013). (Not so) smart cities?: The drivers, impact and risks of surveillance-enabled smart environments. *Science and Public Policy, 40*(6), 717-723.

Gascó-Hernández, M., Martin, E. G., Reggi, L., Pyo, S., and Luna-Reyes, L. F. (2018). Promoting the use of open government data: Cases of training and engagement. *Government Information Quarterly*.

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., and Halderman, J. A. (2014, August 19). *Green lights forever: analyzing the security of traffic infrastructure.* Paper presented at the 8th USENIX Workshop on Offensive Technologies (WOOT 14), San Diego.

Giffinger, R., and Pichler-Milanović, N. (2007). Smart cities: Ranking of European medium-sized cities. Retrieved from http://www.smartcity-ranking.eu/download/city_ranking_final.pdf [Accessed: 31 Oct 2018].

Go ON UK. (2015). Appendix 7: Go ON UK's definition of basic digital skills. Retrieved from https://publications.parliament.uk/pa/ld201415/ldselect/lddigital/111/11115.html [Accessed: 28 May 2018].

Gonzalez-Zapata, F., and Heeks, R. (2015). The multiple meanings of open government data: Understanding different stakeholders and their perspectives. *Government Information Quarterly, 32*(4), 441-452.

Gould, R. V., and Fernandez, R. M. (1989). Structures of mediation: A formal approach to brokerage in transaction networks. *Sociological methodology, 19*, 89-126.

Government Digital Service. (2014). Government Digital Inclusion Strategy. Retrieved from https://www.gov.uk/government/publications/government-digital-inclusion-strategy/government-digital-inclusion-strategy [Accessed: 7 June 2018].

Graham, S., and Marvin, S. (2001). *Splintering urbanism: networked infrastructures, technological mobilities and the urban condition*. London: Routledge.

Greenfield, A. (2010). *Everyware: The dawning age of ubiquitous computing*. Berkeley, CA: New Riders.

Gunes, M., and Deveci, I. (2002). Reliability of service systems and an application in student office. *International Journal of Quality & Reliability Management, 19*(2), 206-211.

Gungor, V. C., Lu, B., and Hancke, G. P. (2010). Opportunities and challenges of wireless sensor networks in smart grid. *IEEE transactions on industrial electronics, 57*(10), 3557-3564.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., and Hancke, G. P. (2011). Smart grid technologies: communication technologies and standards. *IEEE transactions on Industrial informatics, 7*(4), 529-539.

Gunkel, D. J. (2003). Second Thoughts: Toward a Critique of the Digital Divide. *New Media & Society, 5*(4), 499-522.

Hall, R. E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., and Von Wimmersperg, U. (2000, September 28). *The vision of a smart city.* Paper presented at the 2nd International Life Extension Technology Workshop, Paris.

Hargittai, E. (2001). Second-level digital divide: Mapping differences in people's online skills. *First Monday, 7*(4).

Harris, R., and Baumann, I. (2015). Open data policies and satellite Earth observation. *Space policy, 32*, 44-53.

Harrison, T. M., Pardo, T. A., and Cook, M. (2012). Creating open government ecosystems: A research and development agenda. *Future Internet, 4*(4), 900-928.

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., and Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management, 36*(5), 748-758.

Haughn, M., and Gibilisco, S. (2014). confidentiality, integrity, and availability (CIA triad). *Security management.* Retrieved from http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA [Accessed: 14 March 2016].

Heeks, R., and Kanashiro, L. L. (2009). Remoteness, Exclusion and Telecentres in Mountain Regions: Analysing ICT-Based "Information Chains" in Pazos, Peru. *Development Informatics working paper*(38).

HKCERT. (2017). Hong Kong Security Watch Report (Q4 2016). Retrieved from https://www.hkcert.org/my_url/en/blog/17012702 [Accessed: 6 Mar 2018].

Ho, N. (2017). IoT devices pose security threat in HK. Retrieved from https://www.cw.com.hk/it-infrastructure/iot-devices-pose-security-threat-hk [Accessed: 6 Mar 2018].

Holbrook, A., Krosnick, J. A., and Pfent, A. (2005). The causes and consequences of response rates in surveys by the news media and government contractor survey research firms *Advances in telephone survey methodology* (pp. 499-528). New Jersey, USA: John Wiley & Sons, Inc.

Hollands, R. G. (2008). Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City, 12*(3), 303-320.

Hong Kong Innovation and Technology Bureau. (2017). Hong Kong Smart City Blueprint. Retrieved from https://www.smartcity.gov.hk/ [Accessed: 8 Mar 2018].

Hong Kong Legislative Council Panel on Transport. (2017). Parking Policy. Retrieved from https://www.legco.gov.hk/yr16-17/english/panels/tp/papers/tp20170519cb4-1021-9-e.pdf [Accessed: Mar 3 2018].

Hong Kong Transport Advisory Committee. (2014). Report on study of road traffic congestion in Hong Kong Retrieved from http://www.thb.gov.hk/eng/boards/transport/land/Full_Eng_C_cover.pdf [Accessed: 12 Oct 2017].

Hossain, M. A., Dwivedi, Y. K., and Rana, N. P. (2016). State-of-the-art in open data research: Insights from existing literature and a research agenda. *Journal of organizational computing and electronic commerce, 26*(1-2), 14-40.

House of Commons. (2016). Digital skills crisis: Second Report of Session 2016 -17. Retrieved from https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf [Accessed: 19 July 2017].

HP Inc. (2014). HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Retrieved from http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WBwwOfp96Uk [Accessed: 4 Nov 2016].

Huang, W., Fan, H., Qiu, Y., Cheng, Z., and Qian, Y. (2016). Application of fault tree approach for the causation mechanism of urban haze in Beijing—Considering the risk events related with exhausts of coal combustion. *Science of the Total*

Environment, 544, 1128-1135.

Huijboom, N., and Van den Broek, T. (2011). Open data: an international comparison of strategies. *European journal of ePractice, 12*(1), 4-16.

IBM. (2010). Smarter Planet. Retrieved from http://www.ibm.com/smarterplanet/us/en/ [Accessed: 20 OCT 2016].

IBM and Ponemon Institute. (2017). 2017 Cost of Data Breach Study: Global Overview. Retrieved from https://www.ibm.com/security/data-breach [Accessed: Apri 9 2018].

Information Commissioner' s Office. (2018). Right to erasure Retrieved from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ [Accessed: 29 Sep 2018].

Institute of Electrical and Electronics Engineers (IEEE). (2015). About - IEEE Smart Cities. Retrieved from http://smartcities.ieee.org/about [Accessed: 19 OCT 2016].

International Organization for Standardization (ISO). (2015). ISO/TS 37151:2015 Preview Smart community infrastructures -- Principles and requirements for performance metrics. Retrieved from https://www.iso.org/standard/61057.html [Accessed: Jan 28 2018].

International Telecommunication Union. (2011). Measuring the information society. Retrieved from http://www.oecd.org/sti/ieconomy/oecdguidetomeasuringtheinformationsociety2011.htm [Accessed: 15 April 2016].

Ipsos MORI. (2015). Basic Digital Skills UK Report 2015 Retrieved from https://s3-eu-west-1.amazonaws.com/digitalbirmingham/resources/Basic-Digital-Skills_UK-Report-2015_131015_FINAL.pdf [Accessed: 18 July 2017].

Jaatinen, T. (2016). The relationship between open data initiatives, privacy, and government transparency: a love triangle? *International Data Privacy Law, 6*(1), 28.

Janssen, K. (2011). The influence of the PSI directive on open government data: An overview of recent developments. *Government Information Quarterly, 28*(4), 446-456.

Janssen, M., Charalabidis, Y., and Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information systems management, 29*(4), 258-268.

Javed, A. A. (2013). *A model of output specifications for public-private partnership projects (Unpublished doctoral dissertation).* The Hong Kong Polytechnic University, Hong Kong.

Johnston, E. W., and Hansen, D. L. (2011). Design lessons for smart governance infrastructures. *Transforming American governance: Rebooting the public square*, 197-212.

Kalampokis, E., Tambouris, E., and Tarabanis, K. (2011). A classification scheme for open government data: towards linking decentralised data. *International Journal of Web Engineering and Technology, 6*(3), 266-285.

Kao, E. (2018). Hong Kong government needs to improve access to public sector data to realise smart city ambition, academics say. Retrieved from https://www.scmp.com/news/hong-kong/health-environment/article/2144201/hong-kong-government-needs-improve-access-public [Accessed: 13 Sep 2018].

Katz, L. (1953). A new status index derived from sociometric analysis. *Psychometrika, 18*(1), 39-43.

Khan, Z., Pervez, Z., and Ghafoor, A. (2014, December 8-11). *Towards cloud based smart cities data security and privacy management.* Paper presented at the IEEE/ACM 7th international conference on Utility and cloud computing (UCC), London, UK.

Khatoun, R., and Zeadally, S. (2017). Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Communications Magazine, 55*(3), 51-59.

Kim, Y., Choi, T. Y., Yan, T., and Dooley, K. (2011). Structural investigation of supply networks: A social network analysis approach. *Journal of Operations Management, 29*(3), 194-211.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79*(1), 1-14.

Kitchin, R. (2016). *Getting smarter about smart cities: Improving data privacy and data security*. Retrieved from Data Protection Unit, Department of the Taoiseach, Dublin, Ireland:

Kitchin, R., and Dodge, M. (2017). The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 1-19.

Kline, R. R. (2015). Technological Determinism. In J. D. Wright (Ed.), *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)* (pp. 109-112). Oxford: Elsevier.

Knoke, D., and Yang, S. (2008). *Social network analysis* (2nd ed. Vol. 154). Los Angeles: Sage Publications.

Ko, C. (2017). Serving up smart city in Hong Kong by 2020. Retrieved from https://www.cw.com.hk/it-hk/serving-up-smart-city-hong-kong-by-2020 [Accessed: 18 May 2018].

Koss, V., Azad, S., Gurm, A., and Rosenthal, E. (2012). This is for everyone: The case for universal digitisation. Retrieved from https://www.strategyand.pwc.com/reports/this-everyone-case-universal-digitisation [Accessed: 29 Oct 2018].

Kourtit, K., Nijkamp, P., and Arribas, D. (2012). Smart cities in perspective–a comparative European study by means of self-organizing maps. *Innovation: The European journal of social science research, 25*(2), 229-246.

Kozlov, D., Veijalainen, J., and Ali, Y. (2012, February 24 - 26). Sec*urity and privacy threats in IoT architectures.* Paper presented at the Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway.

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing, 13*(6), 391-399.

Kučera, J., Chlapek, D., and Nečaský, M. (2013, August 26). *Open government data catalogs: Current approaches and quality perspective.* Paper presented at the International conference on electronic government and the information systems perspective, Berlin, Heidelberg.

Kulk, S., and van Loenen, B. (2012). Brave new open data world? *International Journal Of Spatial Data Infrastructures Research, 7*, 196-206.

Lämmerhirt, D. (2017). Data And The City: How Can Public Data Infrastructures Change Lives in Urban Regions?   Retrieved from https://blog.okfn.org/2017/02/09/data-and-the-city-new-report-on-how-public-data-is-fostering-civic-engagement-in-urban-regions/ [Accessed: 13 May 2018].

Lavasani, S. M., Ramzali, N., Sabzalipour, F., and Akyuz, E. (2015). Utilisation of fuzzy fault tree analysis (FFTA) for quantified risk analysis of leakage in abandoned oil and natural-gas wells. *Ocean Engineering, 108*, 729-737.

Lavrakas, P. J. (2008). *Encyclopedia of survey research methods* (Vol. 2). Los Angeles: Sage Publications.

Lee, G., and Kwak, Y. H. (2012). An open government maturity model for social media-based public engagement. *Government Information Quarterly, 29*(4), 492-503.

Lee, J. H., Hancock, M. G., and Hu, M.-C. (2014). Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco. *Technological Forecasting and Social Change, 89*, 80-99.

Lee, P. (2016). *A model for energy performance contracting (EPC) in Hong Kong (Unpublished doctoral dissertation).* The Hong Kong Polytechnic University, Hong Kong.

Lee, W.-S., Grosh, D. L., Tillman, F. A., and Lie, C. H. (1985). Fault Tree Analysis, Methods, and Applications: A Review. *IEEE transactions on reliability, 34*(3), 194-203.

Legal Information Institute. (2017). 47 CFR 64.1600 - Definitions. Retrieved from https://www.law.cornell.edu/cfr/text/47/64.1600 [Accessed: 29 Sep 2018].

Leon, R. D., Rodríguez-Rodríguez, R., Gómez-Gasquet, P., and Mula, J. (2017). Social network analysis: A tool for evaluating and predicting future knowledge flows from an insurance organization. *Technological Forecasting and Social Change, 114*, 103-118.

Leung, K. (2018). Official Hong Kong transport info app HKeMobility rolled out, but key data from MTR and other major operators not included. Retrieved from https://www.scmp.com/news/hong-kong/hong-kong-economy/article/2156689/official-hong-kong-transport-info-app-hkemobility [Accessed: 28 Aug 2018].

Lewis, N. (2015). What's the difference between extortionware and ransomware? *Malware.* Retrieved from http://searchsecurity.techtarget.com/answer/Whats-the-difference-between-extortionware-and-ransomware [Accessed: 19 March 2016].

Li, J. (2017). Hong Kong women taxi drivers on why they love the job and how they deal with sexist colleagues and passengers. Retrieved from https://www.scmp.com/lifestyle/article/2108234/hong-kong-women-taxi-drivers-why-they-love-job-and-how-they-deal-sexist [Accessed: 12 Oct 2018].

Li, L. (2010). *A Guide to e-City Construction (in Chinese)* (Vol. 1, pp. 2-3). Nanjing: Northeast University Press.

Li, Y., Dai, W., Ming, Z., and Qiu, M. (2016). Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers, 65*(5), 1339-1350.

Lin, C.-T., and Wang, M.-J. J. (1997). Hybrid fault tree analysis using fuzzy sets. *Reliability Engineering & System Safety, 58*(3), 205-213.

Lin, X., Ho, C. M. F., and Shen, G. Q. P. (2017). Who should take the responsibility? Stakeholders' power over social responsibility issues in construction projects. *Journal of Cleaner Production, 154*, 318-329.

Linders, D. (2013). Towards open development: Leveraging open data to improve the planning and coordination of international aid. *Government Information Quarterly, 30*(4), 426-434.

Lindlof, T. R., and Taylor, B. C. (2010). *Qualitative communication research methods*: Sage.

Lloyds Banking Group, and Tech Partnership. (2018). Essential Digital Skills Framework. Retrieved from https://www.thetechpartnership.com/basic-digital-skills/basic-digital-skills-framework/ [Accessed: 7 June 2018].

Lo, C. (2018). After Singapore medical data hack, Hong Kong's Department of Health becomes latest cyberattack victim. Retrieved from https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2158023/after-singapore-medical-data-hack-hong-kongs [Accessed:

23 Aug 2018].

Lyytinen, K., and King, J. L. (2006). Standard making: a critical research frontier for information systems research. *Mis Quarterly, 30*, 405-411.

Mah, P. (2015). Lessons from the Singapore Exchange failure. Retrieved from http://www.datacenterdynamics.com/power-cooling/lessons-from-the-singapore-exchange-failure/94438.fullarticle [Accessed: 16 March 2016].

Mahmood, Y. A., Ahmadi, A., Verma, A. K., Srividya, A., and Kumar, U. (2013). Fuzzy fault tree analysis: A review of concept and application. *International Journal of System Assurance Engineering and Management, 4*(1), 19-32.

Mahmoud, A. L. H., and Ahmad, R. (2009). THE SMART CITY INFRASTRUCTURE DEVELOPMENT & MONITORING. *Theoretical and Empirical Researches in Urban Management, 4*(2(11)), 87-94.

Markey, E. J., and Waxman, H. A. (2013). Electric Grid Vulnerability: Industry Response Reveal Security Gaps. Retrieved from http://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf [Accessed: 17 March 2016].

Martínez-Ballesté, A., Pérez-Martínez, P. A., and Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine, 51*(6), 136-141.

Masip-Bruin, X., Ren, G. J., Serral-Graci, R., and Yannuzzi, M. (2013, July 15-18). *Unlocking the Value of Open Data with a Process-Based Information Platform.* Paper presented at the 2013 IEEE 15th Conference on Business Informatics (CBI), Vienna.

Maxwell, L. (2018). How to ensure that your smart city strategy is inclusive. Retrieved from https://hub.beesmart.city/strategy/how-to-ensure-that-your-smart-city-strategy-is-inclusive [Accessed: 27 Aug 2018].

McAfee Inc. (2014). Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. Retrieved from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [Accessed: 26 Nov 2016].

McClure, S., Scambray, J., and Kurtz, G. (2001). *Hacking exposed : network security secrets and solutions* (3rd ed.). Berkeley, Calif: Osborne/McGraw-Hill.

McLaren, R., and Waters, R. (2011). Governing location information in the UK. *The Cartographic Journal, 48*(3), 172-178.

Meijer, A., and Thaens, M. (2009). Public information strategies: Making government information available to citizens. *Information Polity, 14*(1, 2), 31-45.

Meola, A. (2016). A major red flag about security could threaten the entire IoT. Retrieved from http://www.businessinsider.com/iot-cyber-security-hacking-problems-internet-of-things-2016-3 [Accessed: 23 Sep 2016].

Miller, B. (2016). How to Overcome the 'Bad Story' Fear and Open Up Your Data. Retrieved from http://www.govtech.com/civic/How-to-Overcome-the-Bad-Story-Fear-and-Open-Up-Your-Data.html [Accessed: 31 May 2018].

Mok, D. (2014). Cyberattack hits 10,000 patients' health data: Ransom demanded from CUHK medical faculty as other victims come forward. Hong Kong. Retrieved from http://www.scmp.com/news/hong-kong/article/1567284/cyberattack-hits-10000-patients-health-data [Accessed: 19 March 2016].

Mok, K. Y., Shen, G. Q., Yang, R. J., and Li, C. Z. (2017). Investigating key challenges in major public engineering projects by a network-theory based analysis of stakeholder concerns: A case study. *International Journal of Project Management, 35*(1), 78-94.

Molloy, J. C. (2011). The open knowledge foundation: open data means better science. *PLoS Biol, 9*(12), e1001195.

Monette, D. R. (2014). *Applied social research : a tool for the human services* (9 th ed.). Belmont, CA: Belmont, CA : Brooks/Cole, Cengage Learning.

Moskvitch, K. (2016). Privacy and snooping in Smart cities: utopia or reality? Retrieved from http://eandt.theiet.org/magazine/2016/01/privacy-and-smart-cities.cfm [Accessed: 19 July 2016].

Murphie, A., and Potts, J. (2003). Culture and technology. New York: Palgrave Macmillan.

Nam, T., and Pardo, T. A. (2011, June 12 - 15). *Conceptualizing smart city with dimensions of technology, people, and institutions.* Paper presented at the Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, Maryland, USA.

Navigant Research. (2016). Gulf States Smart Cities Index: Assessment of Strategy and Execution for 10 Cities. Retrieved from https://www.navigantresearch.com/research/gulf-states-smart-cities-index [Accessed: Jan 28 2018].

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., and Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. *Cities, 38*, 25-36.

Newcombe, T. (2016). Can Security Awareness Training Change Behavior and Reduce Risk? Retrieved from http://www.govtech.com/security/Can-Security-Awareness-Training-Change-Behavior-and-Reduce-Risk.html [Accessed: 29 Sep 2018].

Nunnally, J. (1978). Psychometric theory: New York: McGraw-Hill.

Octopus Cards Limited. (2016). Company Profile. Retrieved from https://www.octopus.com.hk/en/document/company_profile.pdf [Accessed: Mar 5 2018].

Odendaal, N. (2003). Information and communication technology and local governance: understanding the difference between cities in developed and emerging economies. *Computers, Environment and Urban Systems, 27*(6), 585-607.

Office of the Government Chief Information Officer. (2017). Report of Consultancy Study on Smart City Blueprint for Hong Kong. Retrieved from https://www.smartcity.gov.hk/report/ [Accessed: 16 Oct 2017].

OGCIO. (2017). Information and Cyber Security Within the Government. Retrieved from https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/ [Accessed: 10 Oct 2018].

Okoli, C., and Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & management, 42*(1), 15-29.

Okuhara, M., Shiozaki, T., and Suzuki, T. (2010). Security architecture for cloud computing. *Fujitsu Sci. Tech. J, 46*(4), 397-402.

Onisawa, T. (1988). An approach to human reliability in man-machine systems using error possibility. *Fuzzy sets and systems, 27*(2), 87-103.

Onisawa, T. (1990). An application of fuzzy concepts to modelling of reliability analysis. *Fuzzy sets and Systems, 37*(3), 267-286.

Open Data Commons. (2011). Open Database License (ODbL) v1.0. Retrieved from https://opendatacommons.org/licenses/odbl/1-0/ [Accessed: 19 May 2018].

Open Knowledge International. (2015). What is Open Data? Retrieved from http://opendatahandbook.org/guide/en/what-is-open-data/ [Accessed: 13 May 2018].

Open Knowledge International. (2016). Global Open Data Index. Retrieved from https://index.okfn.org/place/hk/ [Accessed: 19 May 2018].

Orlikowski, W. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Organization Science, 11*(4), 404-428.

Paganini, P. (2013). Israeli road control system hacked, causes traffic jam on Haifa highway. *The Hacker News.* Retrieved from http://thehackernews.com/2013/10/israeli-road-control-system-hacked.html [Accessed: 17 March 2016].

Pan, N.-F., and Wang, H. (2007, August 24-27). *Assessing failure of bridge construction using fuzzy fault tree analysis.* Paper presented at the Fourth International Conference on Fuzzy Systems and Knowledge Discovery, Hainan, China.

Parise, S. (2007). Knowledge management and human resource development: An application in social network analysis methods. *Advances in Developing Human Resources, 9*(3), 359-383.

Patrizio, A. (2017). British Airways's outage, like most data center outages, was caused by humans. Retrieved from https://www.networkworld.com/article/3200105/data-center/british-airways-outage-like-most-data-center-outages-was-caused-by-humans.html [Accessed: Apri 9 2018].

Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go? *MIS quarterly, 35*(4), 977-988.

PCPD. (2012). Report on Privacy Awareness Survey on Smartphones and Smartphone Apps. Retrieved from https://www.pcpd.org.hk/english/resources_centre/publications/surveys/files/smartphone_survey_e.pdf [Accessed: 27 Aug 2018].

Pertet, S., and Narasimhan, P. (2005). Causes of failure in web applications *Technical Report CMU-PDL-05-109* (Vol. 92). Pennsylvania, USA: Parallel Data Laboratory, Carnegie Mellon University.

Poole, S. (2014). The truth about smart cities: 'In the end, they will destroy democracy'. Retrieved from https://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase [Accessed: 16 May 2017].

Porta, L. L. (2018). Open Wi-Fi risks: Is it safe to connect to open and free networks? Retrieved from https://www.wandera.com/open-wi-fi-risks/ [Accessed: 3 Aug 2018].

Poston, B., and Jamison, P. (2015). Many poorer areas of L.A. get less trash service, analysis shows. Retrieved from http://www.latimes.com/local/cityhall/la-me-illegal-dumping-20150815-story.html [Accessed: 31 May 2018].

Prell, C., Hubacek, K., and Reed, M. (2009). Stakeholder analysis and social network analysis in natural resource management. *Society and Natural Resources, 22*(6), 501-518.

Price, B. A., Adam, K., and Nuseibeh, B. (2005). Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *International Journal of Human-Computer Studies, 63*(1), 228-253.

PwC. (2017). Report of Consultancy Study on Smart City Blueprint for Hong Kong. Retrieved from https://www.smartcity.gov.hk/report/ [Accessed: 13 May 2018].

Rahman, S. M. M., Hossain, M. A., Hassan, M. M., Alamri, A., Alghamdi, A., and Pathan, M. (2016). Secure privacy vault design for distributed multimedia surveillance system. *Future Generation Computer Systems, 55*, 344-352.

Rebollo-Monedero, D., Bartoli, A., Hernández-Serrano, J., Forné, J., and Soriano, M. (2014). Reconciling privacy and efficient utility management in smart cities.

Transactions on Emerging Telecommunications Technologies, 25(1), 94-108.

Reffat, R. (2003). Developing a successful e-government. *Proc. Sympos. e-Government: Opportunities and Challenge, Muscat Municipality, Oman, IV1–IV13*.

Riggins, F. J., and Dewan, S. (2005). The digital divide: Current and future research directions. *Journal of the Association for information systems, 6*(12), 4.

Robin, C. Y., and Poon, C. (2009). Cultural shift towards sustainability in the construction industry of Hong Kong. *Journal of environmental management, 90*(11), 3616-3628.

Rodosek, G. D., and Golling, M. (2013). Cyber Security: Challenges and Application Areas *Supply Chain Safety Management* (pp. 179-197). Munich: Springer Berlin Heidelberg.

Rouse, M. (2015). security by design. Retrieved from https://whatis.techtarget.com/definition/security-by-design [Accessed: 15 Oct 2018].

Rowley, J., and Slack, F. (2004). Conducting a literature review. *Management Research News, 27*(6), 31-39.

Santos, J. R. A. (1999). Cronbach's alpha: A tool for assessing the reliability of scales. *Journal of extension, 37*(2), 1-5.

Scarfone, K. (2009). *Guide to general server security: Recommendations of the national institute of standards and technology*: Diane Publishing.

Scheerder, A., van Deursen, A., and van Dijk, J. (2017). Determinants of Internet skills, uses and outcomes. A systematic review of the second-and third-level digital divide. *Telematics and informatics, 34*(8), 1607-1624.

Schmidt, R., Lyytinen, K., and Mark Keil, P. C. (2001). Identifying software project risks: An international Delphi study. *Journal of management information systems, 17*(4), 5-36.

Sen, M., Dutt, A., Agarwal, S., and Nath, A. (2013, April 6-8). *Issues of privacy and security in the role of software in smart cities.* Paper presented at the 2013 International Conference on Communication Systems and Network Technologies (CSNT), Gwalior India.

Senol, Y. E., Aydogdu, Y. V., Sahin, B., and Kilic, I. (2015). Fault tree analysis of chemical cargo contamination by using fuzzy approach. *Expert Systems with Applications, 42*(12), 5232-5244.

Shadbolt, N., O'Hara, K., Berners-Lee, T., Gibbins, N., Glaser, H., and Hall, W. (2012). Linked open government data: Lessons from data. gov. uk. *IEEE Intelligent Systems, 27*(3), 16-24.

Shen, A. (2018). Cyberattacks could cost Hong Kong massive US$32 billion annually, according to study. Retrieved from https://www.scmp.com/news/hong-kong/hong-kong-economy/article/2150875/cyberattacks-could-cost-hong-kong-massive-us32 [Accessed: 16 Aug 2018].

Shi, L., Shuai, J., and Xu, K. (2014). Fuzzy fault tree assessment based on improved AHP for fire and explosion accidents for steel oil storage tanks. *Journal of hazardous materials, 278*, 529-538.

Shin, J.-H., and Jun, H.-B. (2014). A study on smart parking guidance algorithm. *Transportation Research Part C: Emerging Technologies, 44*, 299-317.

Siegel, S., and Castellan, N. (1956). *Nonparametric statistics for the behavioral sciences*. New York: McGraw-hill.

Smart Cities Council. (2014). Definitions and overviews. Retrieved from http://smartcitiescouncil.com/smart-cities-information-center/definitions-and-overviews [Accessed: 19 OCT 2016].

Solis, F., Sinfield, J. V., and Abraham, D. M. (2012). Hybrid approach to the study of inter-organization high performance teams. *Journal of construction engineering and management, 139*(4), 379-392.

South China Morning Post. (2010). Octopus escapes penalty for selling data. Retrieved from http://www.scmp.com/article/727912/octopus-escapes-penalty-selling-data [Accessed: 5 Mar 2018].

Sparapani, J. (2016). Fight threats to information security: Inform your people. Retrieved from http://searchcio.techtarget.com/blog/TotalCIO/Fight-threats-to-information-security-Inform-your-people [Accessed: 27 Mar 2018].

Steward, D. V. (1981). The design structure system: A method for managing the design of complex systems. *IEEE transactions on Engineering Management*(3), 71-74.

Stone, M. (1961). The opinion pool. *The Annals of Mathematical Statistics, 32*(4), 1339-1342.

Symantec. (2016). Internet Security Threat Report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_14869594&om_ext_cid=biz_email_elq_&elqTrackId=3f9e79f4cbf14b9a9d39e52f9e438f5f&elqaid=2902&elqat=2 [Accessed: 26 Nov 2016].

Symantec. (2018). 2018 Internet Security Threat Report. Retrieved from https://www.symantec.com/security-center/threat-report [Accessed: 25 Mar 2018].

Tang, W. (2017). Hong Kong's smart city dreams can move faster on big data. Retrieved from http://www.scmp.com/comment/insight-opinion/article/2126132/hong-kongs-smart-city-dreams-can-move-faster-big-data [Accessed: 13 May 2018].

Tasseron, G., and Martens, K. (2017). Urban parking space reservation through bottom-up information provision: An agent-based analysis. *Computers, Environment and Urban Systems, 64*, 30-41.

Thomas, A., Kalidindi, S. N., and Ganesh, L. (2006). Modelling and assessment of critical risks in BOT road projects. *Construction Management and Economics, 24*(4), 407-424.

Thomas, G. (2011). A typology for the case study in social science following a review of definition, discourse, and structure. *Qualitative inquiry, 17*(6), 511-521.

Thomas, J. C., and Streib, G. (2003). The new face of government: citizen-initiated contacts in the era of E-Government. *Journal of public administration research and theory, 13*(1), 83-102.

Toppeta, D. (2010). The smart city vision: how innovation and ICT can build smart,"livable", sustainable cities. *The Innovation Knowledge Foundation, 5*, 1-9.

Townsend, A. M. (2013). *Smart cities: Big data, civic hackers, and the quest for a new utopia* (1 st ed.). New York: WW Norton & Company.

Transport Advisory Committee. (2014). Report on Study of Road Traffic Congestion in Hong Kong. Retrieved from http://www.thb.gov.hk/eng/boards/transport/land/Full_Eng_C_cover.pdf [Accessed: 15 Jan 2017].

Transport Department. (2017). Section 5 : Driving Licences, Offence and Prosecution Statistics. Retrieved from http://www.td.gov.hk/filemanager/en/content_4860/table51.pdf [Accessed: 5 Dec 2017].

Tuckman, B. W., and Harper, B. E. (2012). *Conducting educational research* (6 th ed.). Maryland, United States: Rowman & Littlefield Publishers.

Unal, P., Temizel, T. T., and Eren, P. E. (2017). What installed mobile applications tell about their owners and how they affect users' download behavior. *Telematics and Informatics, 34*(7), 1153-1165.

United Nations. (2014). United Nations E-Government Survey 2014: E-Government for the future we want. *United Nations Department of economic and social affairs*.

Van Deursen, A. J., Helsper, E. J., and Eynon, R. (2016). Development and validation of the Internet Skills Scale (ISS). *Information, Communication & Society, 19*(6), 804-823.

Van Deursen, A. J., and Van Dijk, J. A. (2009). Improving digital skills for the use of online public information and services. *Government Information Quarterly, 26*(2), 333-340.

Van Deursen, A. J., and Van Dijk, J. A. (2014). The digital divide shifts to differences in usage. *New media & society, 16*(3), 507-526.

Van Dijk, J. (2005). *The Deepening Divide: Inequality in the Information Society*. Thousand Oaks: United States, California, Thousand Oaks: SAGE Publications, Inc.

Van Dijk, J. (2006). Digital divide research, achievements and shortcomings. *Poetics, 34*(4), 221-235.

Van Dijk, J. (2012). The evolution of the digital divide: The digital divide turns to inequality of skills and usage. *J. Bus, M. Crompton, M. Hildebrandt, & G. Metakides (Eds.), Digital enlightenment yearbook, 2012*, 57-75.

Van Dijk, J., and Hacker, K. (2003). The Digital Divide as a Complex and Dynamic Phenomenon. *An International Journal, 19*(4), 315-326.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly, 33*(3), 472-480.

Vanolo, A. (2016). Is there anybody out there? The place and role of citizens in tomorrow's smart cities. *Futures, 82*, 26-36.

Vickery, G., and Wunsch-Vincent, S. (2006). Digital broadband content: public sector information and content. *Organization for Economic Cooperation and Development.* Retrieved from http://www.oecd.org/internet/ieconomy/36481524.pdf [Accessed: 20 MAY 2017].

Viitanen, J., and Kingston, R. (2014). Smart cities and green growth: outsourcing democratic and environmental resilience to the global technology sector. *Environment and Planning A, 46*(4), 803-819.

Walravens, N. (2015). Mobile city applications for Brussels citizens: Smart City trends, challenges and a reality check. *Telematics and Informatics, 32*(2), 282-299.

Wamuyu, P. K. (2017). Bridging the digital divide among low income urban communities. Leveraging use of Community Technology Centers. *Telematics and informatics, 34*(8), 1709-1720.

Wasserman, S., and Faust, K. (1994). *Social network analysis: Methods and applications* (Vol. 8). Cambridge, UK: Cambridge University Press.

Weerakkody, V., Irani, Z., Kapoor, K., Sivarajah, U., and Dwivedi, Y. K. (2017). Open data and its usability: an empirical view from the Citizen's perspective. *Information Systems Frontiers, 19*(2), 285-300.

Welsh Government. (2016). Delivering Digital Inclusion: A Strategic Framework for Wales. Retrieved from https://gov.wales/docs/dsjlg/publications/comm/160316-digital-inclusion-strategic-framework-en.pdf [Accessed: 28 May 2018].

Welsh Government Social Research. (2011). Digital Inclusion: Analysis Package. Retrieved from http://gov.wales/docs/caecd/research/110823-digital-inclusion-analysis-package-en.pdf [Accessed: 14 Nov 2017].

WHO. (2016). Global Health Observatory (GHO) data. Retrieved from http://www.who.int/gho/urban_health/en/ [Accessed: 8 Jan 2018].

Witte, J. C., and Mannon, S. E. (2010). *The Internet and social inequalities*. New York, USA: Routledge.

Wright, D., and De Hert, P. (2012). Introduction to privacy impact assessment *Privacy Impact Assessment* (pp. 3-32). Dordrecht: Springer.

Yadron, D. (2016). Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers. *Technology.* Retrieved from http://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center [Accessed: 19 March 2016].

Yang, R. J., and Zou, P. X. (2014). Stakeholder-associated risks and their interactions in complex green building projects: A social network model. *Building and environment, 73*, 208-222.

Yanrong, K., and Whyte, J. (2014). Comparative Study of Smart Cities in Europe and China. *EU-China Policy Dialogues Support Facility II2014, Ministry of Industry and Information Technology (MIIT) and China Academy of Telecommunications Research (CATR).*

Yau, C. (2017). Hong Kong smart city blueprint rolled out amid scepticism over pace and scope. Retrieved from https://www.scmp.com/news/hong-kong/economy/article/2124543/hong-kong-smart-city-blueprint-rolled-out-amid-scepticism [Accessed: 13 Sep 2018].

Yigitcanlar, T., and Lee, S. H. (2014). Korean ubiquitous-eco-city: A smart-sustainable urban form or a branding hoax? *Technological Forecasting and Social Change, 89*, 100-114.

Yin, R. K. (2009). Case study research: Design and methods (applied social research methods). *London and Singapore: Sage*.

Yu, T., Shen, G. Q., Shi, Q., Lai, X., Li, C. Z., and Xu, K. (2017). Managing social risks at the housing demolition stage of urban redevelopment projects: A stakeholder-oriented study using social network analysis. *International Journal of Project Management, 35*(6), 925-941.

Zadeh, L. A. (1999). Fuzzy sets as a basis for a theory of possibility. *Fuzzy sets and Systems, 100*, 9-34.

Zhang, B., Zou, Z., and Liu, M. (2011, May 6-8). *Evaluation on security system of internet of things based on fuzzy-AHP method.* Paper presented at the 2011 International Conference on E-Business and E-Government (ICEE), Shanghai, China.

Zhao, F., Collier, A., and Deng, H. (2014). A multidimensional and integrative approach to study global digital divide and e-government development. *Information Technology & People, 27*(1), 38-62.

Zou, Y., and Wang, C. (2008). The Analysis of China's E-government "information island" phenomenon. *Journal of Library and Information Sciences in Agriculture, 20*(3), 17-21.

Zuiderwijk, A., Jeffery, K., and Janssen, M. (2012). The potential of metadata for linked open data and its value for users and publishers. *JeDEM-e-Journal of e-Democracy and Open Government, 4 (2) 2012*.