Am i being watched on the internet? : examining user perceptions of privacy, stress and self-monitoring under online surveillance

Wai Ho Ip
Hong Kong Baptist University

Follow this and additional works at: https://repository.hkbu.edu.hk/etd_oa

Recommended Citation
https://repository.hkbu.edu.hk/etd_oa/26
Am I Being Watched on the Internet?
Examining User Perceptions of Privacy, Stress and Self-monitoring
under Online Surveillance

IP Wai Ho

A thesis submitted in partial fulfillment of the requirements
for the degree of
Master of Philosophy

Principal Supervisor: Dr. CHANG, Jay H. C.
Hong Kong Baptist University
November 2013
DECLARATION

I hereby declare that this thesis represents my own work which has been done after registration for the degree of MPhil at Hong Kong Baptist University, and has not been previously included in a thesis, dissertation submitted to this or other institution for a degree, diploma or other qualification.

Signature: ________________________

Date: November 2013
ABSTRACT

Modes of communication in modern society have become instant and frequent. Internet users usually post ongoing activities and check their friends’ statuses with texts and photos in social networking sites. During information seeking and sharing processes, they enable peer-to-peer surveillance on the Internet.

The present research adopts Foucault’s (1977) Panopticon as a metaphor to investigate this new advent of online surveillance. Surveillance from unknown people on the Internet may not always exist, but the perception of being surveilled could be embedded in the users’ mind. This kind of suspicion may generate some surveillance effects such as low self-esteem and communication discouragement, namely panoptic effects without the presence of actual surveillance (Botan, 1996). This study focuses on the negative panoptic effects to Internet users, leading to three hypotheses related to privacy infringement, Internet stress and self-monitoring.

An online survey was conducted with 325 respondents aged from 18 to 29. Regression analyses were used to investigate the explanatory power of one’s perception of being surveilled on the outcome variables. The results showed that the respondents with higher level of perceived online surveillance report higher sense of privacy infringement, more situational stress and higher desire of self-monitoring in their online disclosure. With awareness of being surveilled, the respondents realize the information they share online may be exposed to anonymous observers and be prone to storage and dissemination, resulting in privacy infringement. Since online information could be exposed and misused, the respondents feel stressful to share their views and emotions online. They may conduct self-censorship on their online disclosure so as to acquire credits from other Internet users and avoid punishment for improper manner. Implications of these findings are discussed in detail.
ACKNOWLEDGEMENTS

I must offer my heartfelt thanks to my principal supervisor of the thesis, Dr. Jay H. C. CHANG. Without his advice and guidance, I cannot complete this challenging and meaningful task. He walks along with me during the whole process of my thesis preparation, from building theoretical framework, setting hypotheses, designing questionnaire, conducting statistical analysis, finding results to reaching final conclusion with a standard APA style. It is fortunate to work under supervision of Dr. CHANG, who is always helpful, patient and friendly to me.

I am thankful for being taught and taken care by Prof. Ringo Ma, Prof. Chen Ling and Prof. Lynn Webb during my study period of Master of Philosophy in Hong Kong Baptist University. I am enlightened to be a researcher and inspired to design my project from their lectures and sharing. Thanks and applause should also be given to Ms. Eve CHEUNG, Executive Secretary in School of Communication, for her kind assistance whenever I ask for help.

Last but not least, I would express my appreciation and acknowledgment to my parents and friends for their unlimited support and acceptance during my study period.
# TABLE OF CONTENTS

DECLARATION i  
ABSTRACT ii  
ACKNOWLEDGMENTS iii  
TABLE OF CONTENTS iv-v  
LIST OF TABLES vi  
LIST OF FIGURES vii  
LIST OF APPENDICES viii  

CHAPTER I: INTRODUCTION 1  

CHAPTER II: LITERATURE REVIEW 4  
Conceptualization of surveillance 4  
   Definition and development of surveillance 4  
   Levels and Rationale of Surveillance 8  
   Linkage in online network 11  
   Surveillance technologies 13  
Panopticon metaphor for surveillance studies 15  
   Background of Panopticon 15  
   Design and setting of Panopticon 16  
   Traditional vs. Cyber Panopticon 17  
   Applicability of Panopticon to online surveillance 20  
      Internet users with dual roles in online surveillance 20  
      Relatively symmetrical power distribution in online surveillance 21  
      Format change to “The many watch the few” 22  
Panoptic effects 24  
   Self-disciplinary actions in Panopticon 24  
   Awareness of surveillance in Panopticon 26  
   Panoptic effects identified in workplace surveillance 27  
   Perception of surveillance in online context 28  
Three common concerns during online communication 30  
   Invasion of online privacy 31  
      Communication privacy management theory 33  
   Situational stress on the Internet 35  
   Self-monitoring behaviour 38
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Contrasts between traditional and Cyber Panopticon</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Frequencies and descriptive statistics of demographics and computer usage</td>
<td>49</td>
</tr>
<tr>
<td>Table 2</td>
<td>Frequencies of independent and dependent variables</td>
<td>50</td>
</tr>
<tr>
<td>Table 3</td>
<td>Regression analyses of dependent variables affected by online surveillance</td>
<td>53</td>
</tr>
<tr>
<td>Table 4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 1  Aerial view of the Panopticon (Foucault, 1977) 16
# LIST OF APPENDICES

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 1</td>
<td>Screen capture of Internet survey</td>
<td>84</td>
</tr>
<tr>
<td>Appendix 2</td>
<td>Key variables with associated questions and survey results</td>
<td>92</td>
</tr>
</tbody>
</table>
CHAPTER I: INTRODUCTION

Imagine someone is watching you when you are alone with your computer. It is unsure whether the invisible person is present, but the idea that he or she could be with you and at all times lingers. In a surveillance society, you can hardly escape from being “surveilled” with advanced technologies. It seems that nothing is private on the Internet. Secrets are less likely to be kept especially under online surveillance.

Instant and frequent modes of communication in modern society greatly facilitate online surveillance. With the advent of communication technologies in recent years, Internet users are not restricted to connect to the network with fixed personal computers at home or offices. While walking on streets, many people keep updating information with their smart phones and tablets connected to the Internet. They can always interact with their schoolmates, friends and colleagues in social networking sites such as Facebook, Twitter and Weibo, by posting their ongoing activities and checking other users’ statuses with texts and photos. During such information seeking and sharing processes, Internet users enable peer-to-peer surveillance in the connected global network.

Although technologies bring much convenience to Internet users, they induce three common concerns during online communication. Firstly, invasion of privacy is always a potential risk in the open online environment. Some Internet users might be worried about exposing personal information to anonymous observers online with wicked purposes. In fact, raw materials of cyber bullying originate from the information disclosed on victims’ social networking sites, which is stored, forwarded and even tampered. Privacy infringement therefore
becomes a serious issue in the online context. Secondly, online sharing practice might be like a buried bomb to Internet users who are always uncertain or indifferent to its potential risks. Malicious extract and dissemination of personal information by anonymous observers might bring tremendous psychological threats to victims. Uncertain online situations and risks of exposing personal information might cause Internet users psychological discomforts such as depression and stress. These threats might even extend from the online to real-life contexts. Thirdly, Internet users usually perform to be socially desirable in order to protect their social images during online interaction. Some of them are used to conducting self-censorship on their online disclosure so as to acquire credits from other users and avoid potential punishment for improper manner. However, this kind of online self-presentation and selective exposure might sometimes not reflect their real thoughts and emotions to the issues concerned. Therefore, online shared information might be restricted and limited to majority groups with similar social values.

Abovementioned concerns have been examined in the previous communication studies for several decades (Covey, Saladin & Killen, 2001; Folkman, 1984; Thompson, 1981; Wang & Petrison, 1993), but they are still under-explored in the online context. The present research aims to fulfill the academic gap between online communication and respective human responses, by introducing perceived online surveillance as a predictor to explain Internet users’ sense of privacy infringement, perceived situational stress and desire of self-monitoring behaviors. Indeed, online surveillance is a creative and innovative research topic in new media studies (Fuchs, et al., 2012). It is a worthy research topic in modern society with rapid development of technologies, in which Internet users may be subject to coercive monitoring of observers with
anonymous identity and uncertain purposes.

To further explore the influences of online surveillance, this study adopts a quantitative approach to examine its effects on the possible response and behaviour of Internet users during online communication. Specifically, this study investigates whether individual perception of being surveilled online could explain Internet users’ sense of privacy infringement, perceived situational stress and desire of self-monitoring behaviour. Findings of this study should contribute to the existing literature in substantiating the negative effects of surveillance. With knowledge of such possible threats, Internet users could realize the necessity of online privacy protection and ascertain a particular situation changing their emotion and behaviour.
CHAPTER II: LITERATURE REVIEW

To better understand online surveillance and its effects to human daily lives, literature in the scope of surveillance, the Panopticon and online communication is reviewed and analyzed in this chapter. Then, three hypotheses related to human behaviour and responses under online surveillance are posited. To begin with, surveillance, as the most important element in the present study, is introduced and explained in the following paragraphs.

Conceptualization of surveillance

Surveillance is a prepared action of monitoring targets with specific purposes. It might take place in different forms in our society to everyone regardless whether such a phenomenon is being noticed. Its forms keep changing with the technological advancement in recent decades. In the following sections, the idea of “surveillance” is conceptualized in terms of definition, development, level and rationale behind.

Definition and development of surveillance

Surveillance is dynamic in nature and could be interpreted differently from time to time. Definitions of surveillance in the past might not be applicable to the modern society with Internet and computers. Nevertheless, some basic principles and attributes of surveillance remain unchanged and they are commonly used in the previous surveillance studies (Lyon, 2003; Marx, 1988; Rose, 1999; Wood, 2006). Therefore, review of these definitions should lay essential foundation for this study.

Reviewing findings of the surveillance literature, Wood (2006) defined
surveillance as “seeking purposeful, routine, systematic and focused attention paid to personal details for the sake of control, entitlement, management, influence or protection” (p. 3). The attention to people under surveillance is purposeful since the rationale of watching can be justified for the purposes of management, influence and social control (Lyon, 2003). This watching is routine since it happens in daily lives (Rose, 1999). Surveillance is also systematic when it is carried out with a rational schedule. Moreover, it is focused because surveillance mostly targets identifiable persons whose data and particulars are collected, stored, transmitted, retrieved, compared, mined and traded. In modern society, computers greatly convert the nature of surveillance by routinizing, broadening and deepening it as the online network provides a strong linkage among Internet users for communication. Organized memories are therefore assembled and extended without time and space limitations (Marx, 1988).

Mann, Nolan and Wellman (2003) categorized three kinds of surveillance by identifying the relationship between observers and surveilled people. Firstly, top-down surveillance is conducted by governments and organizations on citizens for social control and business purposes. Secondly, surveillance, an inverse form of top-down surveillance, is conducted by individuals to monitor governments and organizations. Thirdly, coveillance refers to peer-to-peer surveillance in which surveilled people are aware of being watched by observers. Andrejevic (2005) regarded this mutual relationship as a lateral surveillance which is mostly managed by individuals, rather than institutions, to keep track of one another within families, friends and acquaintances.

In terms of surveillance nature, physical surveillance played a dominant role in the past such as physical listening and watching the actions of targets (O’Bien, 2008). This kind of traditional surveillance involved close observation of target
individuals or groups such as detective’s supervision on suspected syndicate by
the way of trace (Marx, 1988). The operation of surveillance has developed with
surprising speed for the past decades. Besides physical observation, diversified
forms of surveillance such as psychological surveillance are created via
psychometric testing and data surveillance (Westin, 1971).

With the aid of information technology, data surveillance, named as
dataveillance, monitors the activities and communication of targets in the
systematic and automated ways (Clarke, 1988). A report on the surveillance
society (Wood, 2006) revealed that technologies record movements and activities
of people under surveillance. The ways of surveillance include (i) Closed
Circuit Television (CCTV) in streets and shopping malls, (ii) identity smart cards
revealing personal particulars upon use, (iii) credit cards stating the spending
habits, and (iv) monitor of communication channels such as telephone, email and
the Internet. Activities can be checked and traced when targets go outside or
even stay at home alone. The places targets visit can be located through the
applications (Apps.) installed in smart-phones, records of credit cards and
Octopus cards¹. Friends which targets approach can be identified through the
history of phone calls and emails. Other online activities can easily be traced
through “cookies” and footprints of the Internet. When targets travel abroad,
their whereabouts can be checked through electronic air ticket and immigration
systems.

In the modern surveillance society, technologies are introduced to extract
personal data from the database containing profiles of target individuals or groups
(Marx, 1988). Since the data can be stored in database and easily retrieved for
different purposes to generate new data, the storage system can be largely

¹ Octopus cards are a kind of smart cards for domestic consumption in Hong Kong.
expanded through data accumulation. Surveillance is therefore supported and developed from rich and available data on the Internet. Since technologies have overcome time and space limitations for communication, the Internet becomes a popular tool to share and accumulate data. Searchable databases on the Internet are important to surveillance activities. Since the search engines facilitate the classification of data, Internet users can easily access information by searching categories or specified items. The previous research discovered that Google’s search engine is the most common surveillance methods in the United States to search someone’s interests, friends and acquaintances (Andrejevic, 2005).

Apart from unidirectional search, interpersonal surveillance can be mutual in social media in which Internet users are able to watch and to be watched (Brighenti, 2010; Farinosi, 2011). Trottier (2012) discovered that individuals participate in disclosing information in social networking sites because of peer pressure for sharing common topics. In addition to self-disclosure, personal information may be shown and disseminated in friends’ web pages which contain photos and other content about them. By its nature of sharing, social media greatly facilitate interpersonal surveillance in the ways of creeping and stalking (Shirky, 2008). Both tactics involve perusing and tracing content in social networking sites such as wall posts and photo albums. Creeping and stalking are often perceived negatively when such a surveillance practice is regarded as coercive control rather than sincere caring (Trottier, 2012).

Moreover, collaborative effort on data accumulation by numerous Internet users further encourages surveillance activities such as human flesh search, namely Renrou Sousuo in China (Pan, 2010). Human flesh search usually starts with an open enquiry in the online communities of information about any topics such as private lives of celebrities. Multiple Internet users with active
participation and collaboration make contribution to the search of topics concerned. In China and Hong Kong, collaborative search is often destructive and aggressive to targets who are usually judged as wrongdoers and whose unwelcomed conduct is blamed and criticized. During collaborative search, personal information of targets is extracted and disseminated online to trigger verbal attack and sneer by multiple Internet users. Targets therefore easily suffer from psychological threats such as heavy pressure and depression. Besides taunt and insult, they are forced to undergo a moral judgment and discussion among the online communities.

With the aid of technology and collaborative efforts of Internet users, online surveillance could better be defined as “a purposeful action of providing and searching information of the issues and individuals concerned on the Internet, in order to have control and influence over targets through the global connected network”. In the present study, this definition of online surveillance is widely applied to interpersonal information exchange in social media. Peer-to-peer surveillance indeed always exists while social media users actively share personal information and search particulars of other users in social networking sites and online discussion forums.

**Levels and Rationale of Surveillance**

The concept of surveillance exists for hundreds of years (Bentham, 1996; Foucault, 1977). Its application could be widespread from high to low classes in society when resource and knowledge are exploited. Observers can empower themselves with technology in surveillance actions. Most of them mainly aim to prevent themselves from being ruined by other parties and protect their own benefits or fight for more advantages.
In the beginning, surveillance is widely employed by different countries to reduce social risks and increase national security (Wood, 2006). The governments have the legal power and responsibility to utilize surveillance techniques, for the sake of protecting the legitimate rights and interests of their citizens and fighting against the opposition parties which aim to overthrow the government or carry out the terrorist activities (O’Brien, 2008).

With innovation of technology, surveillance is widespread from governments to organizations and individuals. Workplace surveillance has been prevalent since the 1980s (Aiello, 1993; Botan, 1996). Scientific management encourages surveillance in workplace so as to enhance the productivity of employees and maximize their output (D’Urso, 2005). For instance, computerized measurement of working performance efficiently monitors the productivity of employees. The telephone recordings can be retrieved to improve the quality of customer services and monitor the private calls of employees. Some computer programmes even enable employers to monitor employees’ computer screens in order to prevent any unrelated activities to the work tasks. Apart from surveillance during office hours, employers might monitor the private lives of their employees by visiting their social networking sites in order to understand their personality, conduct and activities while off duty (Fuchs, 2009). In case inappropriate acts and messages are found to contaminate the image and reputation of company, employees may be liable to warning or even dismissal.

Reduction of uncertainty is a common purpose of surveillance in both workplace and marketplace (Campbell & Carlson, 2001). Employers aim to ascertain the productivity and good conduct of employees, whereas capitalists endeavour to predict consumer behavior in the marketplace. Enterprises therefore extensively gather the consumer information such as their preferences.
and habits to plan the marketing strategy in an attempt to enlarge the market share. As Solove (2004) stated, the effectiveness of marketing plan and strategy relies on the amount of data the corporations can obtain. Microsoft and Yahoo are two successful large-scale companies in data collection. These two companies are powerful in selecting advertisements for Internet users and satisfying their consuming desires by tracking their search and web activities to collect their demographic and psychographic data (Turow, 2006).

In regard to the individual level of surveillance, as a frequent mode in online surveillance and the main focus of the present study, Dupont (2008) proposed the term “democratization” on the Internet, meaning the increasing individual accessibility to information through technological tools and services which were previously controlled and afforded by the government and large organizations. With technological advancement and dissemination of knowledge, citizen surveillance on the government not only takes place in a bottom-up form, the information shared in the citizen network can be widespread and then generate new information as well (Cascio, 2005).

In 2008, owing to a large scale of earthquake in Szechwan in China, numbers of infrastructure and buildings collapsed. In view of numbers of deaths and injuries exceeding 460,000, local residents suspected that public constructions with haphazard and unsubstantial fashion were vulnerable to natural hazards. This suspicion triggered the corruption investigation in Szechwan’s construction schemes. Jerry-built projects by the local government were therefore exposed on the Internet. Some officials were found accepting bribes from the builders and failing to play a supervisory role in the construction schemes. Public facilities were mostly built with low quality and loose control, resulting in large collapses in the earthquake. During the investigation process, valuable materials were
shared and widespread among Internet users. The government was less likely to be able to dictatorially control citizens who became more empowered and united while connecting to the online network. They might participate in surveillance “willingly” and “actively”. Cascio (2005) regarded this kind of voluntary monitoring and supervision conducted by citizens in cyberspace as participatory surveillance.

Whitaker (1999) explained that people tend to participate in surveillance voluntarily because they see positive and tangible benefits from participation. Moreover, they are less likely to perceive intangible and indirect disadvantages. Whitaker (1999) cited the use of smart health cards in the western countries as an example. When someone is unconscious and bleeds on the ground in a traffic accident, the first aiders arrive at the scene and locate his smart health card to acquire information such as blood type, medicine allergy and his anamnesis. The first aiders can evaluate the situation properly and provide the appropriate treatment to the casualty. There are few reasons to object using smart health cards. However, smart health cards may not always offer benefits to the users. If the card shows that the casualty lacks credit worthiness on medical insurance, or has anamnesis containing the information of HIV and mental illness, the casualty may be put in different treatments owing to their inferior social or economic status. It is common that individuals tend to focus on benefits and neglect the threats in the participatory surveillance. They might be awake only when crisis happens.

**Linkage in online network**

Surveillance has developed rapidly for decades and is widespread among different social levels. Surveillance technique is also greatly reinforced through
a connected network in the computer-mediated environment (Lyon, 1999). Linkage in the online network is extremely strong when information can easily be stored and distributed among Internet users. Strong linkage not only facilitates online communication, but also reinforces online surveillance in the way of information extraction and instant monitoring.

The idea of “World Wide Web” represents a global network with the electronic interconnected systems and it creates a new kind of communication in cyberspace. Lyon (1999) defined “cyberspace surveillance” as any forms of surveillance occurred in computer-mediated communication in which data collection from the web can be done by typing the keyboard and all information can be seen on screen. Although the term of “cyberspace surveillance” shows the location and specific context of surveillance, it cannot thoroughly describe a unique environment—an unprecedented network connection in the virtual reality. Instead, “online surveillance” should be more appropriate to represent the status quo because “online” can well express the idea of “linkage in the virtual global network”. As Bogard (1996) mentioned, the electronic network is not only a global system, but also an orbital and cellular network linking and gathering macro and micro information. In fact, the online network facilitates information sharing and searching among governments, organizations and individuals. When people get “online” and keep the connection with the Internet network by using computers, they can acquire the most up-to-date information and keep track of any person or event mentioned on the web. Therefore, they can maintain high sensitivity and awareness of their surroundings while getting online.

In the process of establishing the global network in the online context, web-based platforms such as Facebook, Wikipedia, YouTube, Google, Whatsapp strongly support social networking, community building, collaborative
information production and user-generated content diffusion (Fuchs, et al., 2012).
Those social mediums do not represent radical transformation of the Internet, but
the enhancement of social connection and the reproduction of human relationships
instead (Fuchs, 2010). Benkler (2006) supported that the Internet advances the
emergence of peer production systems and platforms in which sharing resources
and outputs are encouraged among widely distributed and loosely connected
people. In view of increasing ability of sharing information and taking
collaborative actions, Internet users can empower themselves by building their
own online network of mass communication (Castells, 2009). Nevertheless, the
Internet enables a global network to facilitate surveillance at the same time
(Fuchs, et al., 2012). When people use social media such as Facebook and
Twitter, the original purpose is to disclose personal data and collect others’
information for social interaction and gratification. However, such common
sharing and searching practice facilitates the prevalence of online surveillance
(Albrechtslund, 2012).

**Surveillance technologies**

Strong linkage among Internet users in the online network provides a
favourable environment to surveillance actions. When they always live with
computers for online communication, observers could closely monitor and obtain
more information about their targets. In addition to advanced technologies used
or specially designed for online surveillance, information and activities can easily
be traced and monitored on the Internet.

All actions and messages on the Internet are traceable since computer
databases store footprints and other information in an automatic and efficient way.
Practically, online surveillance technologies such as cookies, spam spider boots,
spyware and other computer-based profiling softwares facilitate the exploitation
and accumulation of valuable personal information (Wall, 2006). Starke-Meyerring and Gurak (2007) classified those surveillance technologies into three
categories, including capture from general Internet use (e.g. Google and Yahoo
search engines), capture through specialized Internet services (e.g. Cookies and
spam spider boots), and other designed technologies (e.g. Trojan horse and
spyware). Castells (2001) defined the abovementioned items as technologies
which entirely intercept messages, monitor online activities and track information
flow from a specific computer location.

Legitimately, governments, organizations and courts may obtain message
origins identified by surveillance technologies from the Internet service providers.
In 2005, a Hong Kong citizen, Chan Nai Ming, uploaded free seeds of movies
through peer-to-peer technology (i.e. BitTorrent) to the online platforms without
authorization of the copyright owners. Suspecting Chan committed an offence
against the Copyrights Ordinance, Chapter 528 of Laws of Hong Kong, Hong
Kong Customs obtained information of subject seed origins from the Internet
service provider and identified the suspected offender’s location. Having
investigated Modus Operandi of illegal online distribution, Hong Kong Customs
arrested and prosecuted Chan by putting seed origins and distribution flow as
court computer evidence. Chan was eventually sentenced to three-month
imprisonment (Moy, 2005). With the aid of surveillance technologies, illegal
online activities were promptly suspended in a short period of time.

Unlike non-technological surveillance, online surveillance collects data
automatically and is not restricted to co-presence and proximity of observers and
targets. Fuchs, et al. (2012) summarized the attributes and conditions of online
surveillance, including global scale, real-time, high speed, fast data growth, data
multiplicity, hyperlink, “Produsage” (i.e. portmanteau of words “Production” and “Usage”), cooperation, data anonymity, fake data and fake identity. With a similar proposition, Cohen (2008) stated that surveillance with digital technology becomes more ubiquitous, anonymous, automatic and self-reinforcing.

Panopticon metaphor for surveillance studies

Surveillance has developed rapidly over the past decades and its forms have extended from eyeball monitoring to the web tracking. Taking technological advancement into consideration, scholars in disciplinary and surveillance studies are always concerned about power relationships between observers and targets. They have used the Panopticon (Bentham, 1995; Foucault, 1977) as a surveillance metaphor to describe and explain the power distribution of social relationships involving observers and targets (Botan, 1996; Botan & McCreadie, 1990; Campbell, 2005; D’Urso, 2005).

Background of Panopticon

In 1791, a prominent British philosopher and social reformer, Jeremy Bentham, introduced an idea of the “Panopticon” with the detailed plan and calculation to conduct surveillance on inmates in a controlled environment. The Panopticon could be designed as prisons, mad-houses, hospitals or schools (Bentham, 1995) and would be managed with an “apparent omnipresence of the inspector” (p. 45). Bentham (1995) refined his proposal for many years and successfully raised funds from the prime minister of England to erect the Panopticon. However, since the money was inadequate and the landowners greatly opposed his project, no true Panopticon from Bentham's design has ever been built. Although Bentham’s will was not achieved during his time, his
design inspired Michael Foucault to develop a surveillance metaphor in modern disciplinary societies and publish his proposition in 1977. Foucault’s idea follows Bentham’s description of the Panopticon as an unprecedented mode of obtaining power from mind over mind (Foucault, 1977).

**Design and setting of Panopticon**

According to Bentham’s and Foucault’s ideas, the Panopticon is a circular building with an observation tower in the center surrounded by an outer wall (see Figure 1). Cells are built at the outer wall for the incarceration of mental patients and offenders. This kind of design can increase the security through the effectiveness of surveillance. Inmates who are placed in cells separately cannot see each other through the concrete walls. Separated cells imply the lateral invisibility among inmates for the sake of order and control (Foucault, 1977). No plots, collective escapes and new crimes can thus be organized. Since the cells are full of light, all actions of inmates are monitored by the observation tower, which might be managed by guards and accessed by general public and non-institutional members. This policy implies that the prisoners do not know who monitor their activities and when they are monitored. It means the guards can see without being seen (Bentham, 1995). Foucault (1977) argued that this effect can enhance the efficacy of the disciplinary system.
Foucault (1977) contended that the invisibility of guards in the observation tower is a critical and main feature of the Panopticon. “He [The prisoner] is seen, but he does not see; he is the object of information, never a subject in communication” (p. 200). This invisibility facilitates the unverifiable surveillance in the Panopticon. Since the prisoners never know who is watching them and when they are being watched, they might try to self-monitor their own behaviours so as to avoid the disciplinary actions from the guards. Foucault (1977) identified this kind of self-disciplining thoughts and behaviours as self-surveillance.

The invisibility of guards and the visibility of prisoners create an imbalanced power distribution in the Panopticon (Botan, 1996). As Foucault (1977) proposed, “The major effect of the Panopticon was to induce in the inmate a state of conscious and permanent visibility that assured the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects even if it is discontinuous in its action” (p. 201). In a panoptic relationship, prisoners are vulnerable because they are visible to observers, but observers are invisible to them. Prisoners always need to act as if they are being surveilled even sometimes without the real presence of observers. In the practice of self-surveillance, the actual mechanism of coercion can be removed, but the perception of threat of coercion still remains in the mind (Botan, 1996).

**Traditional vs. Cyber Panopticon**

Foucault (1977)’s Panopticon is more like a physical construction in which inmates separately live in the cells under surveillance. However, no building is established to besiege inmates when there is presence of online surveillance. Instead, targeted Internet users are unconsciously monitored by other individuals
and parties while disclosing personal information and showing their activities in the online channels. The environment where online surveillance takes place is regarded as “Cyber Panopticon”.

Bentham (1995) and Foucault (1977) have introduced significant concepts of surveillance which are further developed with a great technological advancement. Since the end of the 1980s, some people started to communicate with others on the Internet by using computers in order to maintain relationships beyond time and space limitations. Moreover, technological development lowers the price of surveillance equipments and creates an easy access to others’ information (Dupont, 2008; Lessig, 2006). As the Internet satisfies the needs of users who want to search and retrieve information online, surveillance becomes a regular and ubiquitous practice among Internet users (Andrejevic, 2005; Lyon, 2001; Pan, 2010). Indeed, information technologies facilitate the development of Cyber Panopticon which could be regarded as an enhanced surveillance metaphor in modern surveillance society. Although Cyber Panopticon is still based on the concepts of Bentham (1995) and Foucault (1977), it has a subtle change in the roles of surveillance practice.

With the aid of the Internet and computers, Cyber Panopticon are different from the traditional one in terms of target, initiative, role and situation, mode of communication and degree of freedom in surveillance (see Table 1). The occupants in Cyber Panopticon might not be disadvantaged groups such as inmates who are forced to reside and be monitored there. They are instead voluntary Internet users who may observe other individuals or may be surveilled at the same time. With the anonymous nature of cyberspace, Internet users are invisible to search the information of those being surveilled and they become observers without being noticed. However, they can simultaneously be
surveilled by other users as well since they are similar to inmates and visible to other observers. In the Panopticon, inmates are low in freedom because they are isolated by the concrete walls and cannot communicate with their neighbours. In Cyber Panopticon, it seems that Internet users, who work on individual tasks, are isolated by the computers which are separately operated in their homes (Vorvoreanu & Botan, 2000). As Webster (2002) argued, computers erect the Panopticon without the physical walls. Nevertheless, they can still have online communication and physical contact with others in the real-life context. The degree of freedom is definitely greater online in comparison to the traditional design.

Table 1. Contrasts between traditional and Cyber Panopticon

<table>
<thead>
<tr>
<th></th>
<th>Traditional Panopticon</th>
<th>Cyber Panopticon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Disadvantaged groups (e.g. prisoner and patient)</td>
<td>Internet users</td>
</tr>
<tr>
<td>Initiative</td>
<td>Compulsory involvement</td>
<td>Voluntary involvement</td>
</tr>
<tr>
<td>Role</td>
<td>Distinct role as observer or surveilled</td>
<td>Dual roles as both observer and / or surveilled</td>
</tr>
<tr>
<td>Situation</td>
<td>Isolated by the concrete wall in a cell</td>
<td>Separated by computers, but inter-connected on the Internet</td>
</tr>
<tr>
<td>Mode of Communication</td>
<td>Invalid communication with others</td>
<td>Valid online communication and physical contact</td>
</tr>
<tr>
<td>Degree of freedom</td>
<td>Lower</td>
<td>Higher</td>
</tr>
</tbody>
</table>

The advent of computers intensifies and extends the panoptic control over the surveilled from real life to the virtual reality. More importantly, information technologies convert social control to be more invasive, mundane and inescapable (Robins & Webster, 1999). In addition, active participation in the online
activities of Internet users contributes to the development of Cyber Panopticon. Since the recent Internet operation is more convenient and relatively less expensive than the past operation, people are more willing to engage in the online activities such as going online shopping, playing online games and disclosing their views and interest in social networking sites (Dupont, 2008). Therefore, the information flow is accelerated and becomes frequent in cyberspace. More and more information is stored in the online databases by numerous information providers, who simultaneously as information seekers search the information they are concerned. As a result, the voluntary participation in surveillance by Internet users establishes the “Participatory Panopticon” (Cascio, 2005) in the online context.

*Applicability of Panopticon to online surveillance*

Due to a great difference between traditional and Cyber Panopticon, some scholars argued that the Panopticon as a surveillance metaphor is no longer adequate enough to represent the current surveillance society (Mathiesen, 1997; Marx, 1985; Poster, 1990; Boyne, 2000; Farinosi, 2011). They strongly argued non-applicability of the Panopticon with three major propositions, including i) no fixed roles in online surveillance, ii) relatively balanced power distribution, and iii) format change to “the many watching the few” (Mathiesen, 1997, p. 219).

*Internet users with dual roles in online surveillance*

Information technologies contribute to a new mode of surveillance in which the online databases are regarded as the Superpanopticon (Poster, 1990), which brings surveillance principles beyond a prison. Electronic communication with enormous databases constitutes the Superpanopticon as a system without concrete
walls, observation tower and guards. Meanwhile, surveillance is reinforced when individuals communicate with each other in the computerized environment (Poster, 1990). Poster (1990) argued that individuals are not passive and under control of observers in the Superpanopticon, but they instead play an active role to conduct their own surveillance by seeking information from and providing information to databases.

A recent research (Farinosi, 2011) found that when young people think about the online environment and their control practices, the surveillance metaphors they employ are very different from what Bentham (1995) proposed. The major metaphor the interviewees used to describe the online environment was “shop-window”. They regarded their online profiles as a tool of self-promotion, instead of disclosed materials to be surveilled. They did not perceive the online environment as the Panopticon because roles of observers and the surveilled are not fixed. In a modern panoptic phase, new opportunities of participation in surveillance are created since Internet users can be both controllers and the controlled (Farinosi, 2011). Individuals could become more powerful in the online context when they get more shared information and materials of other users.

**Relatively symmetrical power distribution in online surveillance**

With regard to the dual roles in online surveillance, power distribution becomes more even and symmetrical because everyone could be observers and the surveilled as well. The original design and setting of the Panopticon (Foucault, 1977) imply an imbalanced power in surveillance and a vertical control from up to down on surveilled people. On the contrary, horizontal control from peer to peer is found in participatory surveillance on the Internet (Albrechtslund,
2008), in which roles of surveillance are not fixed as pure observers and pure surveilled people. Social media with technological enhancement contribute to a relatively symmetrical power structure among Internet users (Farinosi, 2011). Apart from some authorized parties and individuals such as crime investigation units, most Internet users have similar channels to seek information of other users. While engaging in the online activities and disclosing personal information, Internet users should have equal opportunities to be observers and the surveilled. With relatively symmetrical power distribution, the Internet is not only regarded as a medium for powerful groups and individuals to exert social control and domination over others, but also a functional tool for the surveilled to resist against domination (Fuchs, 2011). Bogard (2006) even argued that the system of control in Cyber Panopticon is deterritorializing.

In spite of changes in surveillance roles and power distribution in Cyber Panopticon, Farinosi (2011) argued that the visibility-invisibility contrast as the main feature of the Panopticon still remains in online surveillance. When people use computers at home and disclose themselves on the Internet, they are still visible to observers who could be hidden in the network. This contrast makes people under surveillance insecure when they cannot verify the presence of observers, resulting in designated surveillance roles and imbalanced power distribution in that particular surveillance situation.

Format change to “The many watching the few”

Since there is no fixed role as observers or the surveilled on the Internet, modern surveillance society changes from the situation where the few oversee the many to the situation where the many oversees the few (Mathiesen, 1997). When a user shares his or her personal information in social media, which
connects to friends and colleagues, many potential observers are present and may monitor his or her activities without prior notice. Mathiesen (1997) argued that Foucault’s (1977) Panopticon fails to consider the surveillance societies with technology advancement in which the many might watch the few in the online context. Supporting Mathiesen’s (1997) argument, Ball (2006) stated that people, organizations and technologies become connected to form a “surveillance assemblages” and produce an enormous database on the Internet, contrary to the unidirectional and top-to-down surveillance metaphor (Foucault, 1977).

Nevertheless, Caluya (2008) thought that the idea of the Panopticon (Foucault, 1977) in surveillance is far more than a unidirectional metaphor, which simply describes that observers control over the surveilled. As Foucault (1977) argued “The major effect of the Panopticon was to induce in the inmate a state of conscious and permanent visibility that assured the automatic functioning of power” (p. 201). Foucault’s (1977) Panopticon is indeed an analysis of the functioning of power (Caluya, 2008). Although visibility of the surveilled and the gaze of observers are emphasized in the Panopticon, but it should not be illustrated as an analysis of the gaze, but the functioning of power through the use of the gaze. As Caluya (2008) explained, the main principle of the Panopticon is not the gaze but automatization and disindividualization of power, originated from the omnipresence of observers in the minds of people under surveillance.

The applicability of Foucault’s (1977) Panopticon as a metaphor remains controversial in surveillance studies. Undoubtedly, the Internet is a unique context which allows dual roles in surveillance and provides more symmetrical power to its users. Nevertheless, the enhanced metaphors to describe modern surveillance (Albrechtslund, 2005; Farinosi, 2011; Haggerty & Ericson, 2000; Lyon, 2006; Poster, 1990; Simon, 2005) are all based on the design and principles
of Foucault’s Panopticon (1977). Rather than challenging Foucault’s contributions to disciplinary and surveillance studies, this study is going to incorporate his concepts and propositions into the unique attributes of online surveillance, because the idea of the Panopticon (Foucault, 1977) does provide a solid foundation of visibility-invisibility contrast and automatized functioning of power in the panoptic relationships, resulting in different kinds of panoptic effects on people under surveillance.

**Panoptic effects**

With visibility-invisibility contrast and automatized functioning of power in the panoptic relationships, Foucault (1977) introduced the idea of “perception of surveillance” in the Panopticon in which surveilled people always act as if someone observes their actions, resulting in self-monitoring behaviour as a panoptic effect. Following Botan’s (1996) application of this perception into the examination of workplace surveillance, this study identifies the panoptic effects in the online environment.

**Self-disciplinary actions in Panopticon**

In the panoptic relationships, observers always take an overwhelming and leading position over surveilled people, who acts in a cell as if someone is watching them (Foucault, 1977). It is understood that the Panopticon is not only regarded as a prison to seize freedom of prisoners in a controlled environment, but it also makes the inmates more self-disciplined and self-regulated. Foucault (1977) believed that “Panopticon was also a laboratory; it could be used as a machine to carry out experiments, to alter behavior, to train or correct individuals” (p. 203). He strongly believed that the Panopticon should create positive and
desirable effects such as self-disciplinary actions on inmates, which can be regarded as the panoptic effect at the beginning of Foucault’s (1977) declaration. The present study is going to investigate other potential panoptic effects, particularly from the negative side, such as perceived invasion of privacy, increased stress and discouragement of self-disclosing behaviour, which will be discussed further in other sessions.

Although the previous literature did not explain the panoptic effects in a detailed and thorough way, Botan (1996) contended that such surveillance effects as self-monitoring behaviour are “panoptic” when the key mechanism of generating effects is based on the contrast between the visibility of surveilled people and the invisibility of observers. The panoptic effects can be internalized when the inmates realize their vulnerability in the Panopticon owing to visibility-invisibility contrast. As the inmates never know who is watching them and when they are watched, they may feel insecure and anxious in the cell (Botan and McCreadie, 1990).

In the Panopticon, vulnerability of the inmates could trigger the behavioural panoptic effects. Suspecting that surveillance from the observation tower takes place at any times, the inmates perceive their vulnerability and suffer from the psychological consequences of being surveilled. Therefore, they are more likely to take and avoid certain actions in order to generate favourable situations, resulting in their self-disciplinary actions. For instance, they may comply or pretend to comply with the instructions of observers, reject violence and behave in a cooperative manner in the Panopticon so as to avoid observers’ punishment. These kinds of actions and responses of surveilled people are deemed to be the self-monitoring behaviour.
**Awareness of surveillance in Panopticon**

For the sake of generating power imbalance and panoptic effects, it is necessary for surveilled people to have awareness of surveillance. If surveilled people are not aware of surveillance, no panoptic effects will be created (Botan, 1996; Botan & McCreadie, 1990; Foucault, 1977). It could be common that surveillance occurs without this awareness such as eavesdropping and peering, but it lacks the panoptic effect to surveilled people (D’Urso, 2005).

Botan and McCreadie (1990) argued that the panoptic effects in workplace surveillance vary in different scenarios and work from the interaction of four elements, including i) perception of people under surveillance, ii) surveillance potential of the technology, iii) management policy, and iv) maturation of the situation. The first element abovementioned is the main source of the surveillance effects and other three elements could favour the emergence of surveillance. The first element is especially crucial because perceived surveillance in mind could internalize the relationships between observers and surveilled people with a visibility-invisibility contrast and thus creates the panoptic effects (Botan, 1996). Surveillance potential of the technology leads to the panoptic effects with four main components, including i) to what extent technology makes surveilled people visible, ii) to what degree technology makes observers invisible, iii) how detailed and everlasting the data is recorded, and iv) how technologically driven the data can be. In terms of surveillance technology, management policy determines the implementation of surveillance and its relative levels. Moreover, maturation of situation and environment is significant to the efficiency and success of surveillance. For example, surveillance procedure is well established and the legal issues are resolved.

This conceptual model proposed by Botan and McCreadie (1990) was mainly
applied and cited in surveillance studies (Botan, 1996; D’Urso, 2005) in the workplace context. However, abovementioned elements of the panoptic effects might not be all applicable in the online environment. The applicability of this model into the online context will be discussed further.

**Panoptic effects identified in workplace surveillance**

The Panopticon as a surveillance metaphor offers a useful framework to examine the surveillance effects in the workplace context (Botan, 1996; D’Urso, 2005). With the application of awareness of surveillance in the Panopticon, Botan (1996) adopted the model of Botan and McCreadie (1990) to predict the panoptic effects in workplace surveillance. His study discovered that increases in perception of surveillance, whether it is expected or accepted, can result in greater panoptic effects in the workplace environment (Botan, 1996).

Botan’s (1996) research associates the idea of the Panopticon (Foucault, 1977) with electronic surveillance in the workplace environment. His work made a significant contribution to the identification of panoptic effects, and more importantly, the establishment of panoptic effects as predictable and testable variables based on a survey result. Botan (1996) conducted a mail survey with 453 union members in communication industries. In his study, perceived workplace surveillance is regarded as the independent variable and the panoptic effects are treated as the dependent variables. The results supported that employees with a stronger belief that they were being surveilled reported significantly less workplace privacy, more uncertainty about their job situation, lower levels of self-esteem and workplace communication than employees with less belief that they were being surveilled. Botan’s (1996) study confirmed that changes in perceived surveillance results in detectable changes in the panoptic
In addition to Botan’s (1996) findings, other panoptic effects were observed in the workplace context through studies on electronic surveillance. Apart from a few positive effects such as increased productivity and efficiency (D’Urso, 2005), other responses to surveillance are mainly negative, including distrust between employers and employees, poor working morale (Balitis, 1998; Fitting, 1995), reduced efficiency, decreased job satisfaction, increased number of turnover, absenteeism (Chalykoff & Kochan, 1989; Kidwell & Bennett, 1994; Mishra & Crampton, 1998), decreased sense of fairness and respect for employees (Hartman, 1998; Ottensmeyer & Heroux, 1991), increased stress and other health effects (Posch, 1993).

Perception of surveillance in online context

Botan (1996) used perception of surveillance as the main element to examine panoptic effects in the workplace environment. He discovered that perception of surveillance does exist among the employees who suffer from different kinds of panoptic effects. However, few similar research efforts have been put in the online environment where surveillance always takes place in recent decades. Therefore, this study, which uses perception of surveillance as a single factor to predict online panoptic effects on individuals, intends to fill the academic gap between online communication and corresponding human responses.

Botan and McCreadie’s (1990) model identifies four elements, including i) perception of people under surveillance, ii) surveillance potential of the technology, iii) management policy and iv) maturation of the situation, to predict the panoptic effects in workplace surveillance. However, none of the elements was used to examine panoptic effects in online surveillance in the previous studies.
It is admitted that not all these elements are applicable in the examination of panoptic effects in online surveillance. For example, management policy which is considered more an organizational factor is not a valid factor for interpersonal surveillance. Nevertheless, this study considers perception of surveillance as a significant factor that should not be overlooked in both workplace and online contexts.

As Botan (1996) and Foucault (1977) strongly emphasized, the panoptic effects are present with awareness of surveillance. Perceived online surveillance as a predicting factor is essential in studying the panoptic effects. If perceived surveillance does not exist, there will be no online panoptic effects. As D’Urso (2005) mentioned, perception of surveillance alone might have a powerful function for the management and could have serious potential influence on the individuals. Although the management function is inapplicable in the online context, individual consequences are of great importance and interest to surveillance studies. Therefore, perception of surveillance is the main focus of the present research. Moreover, in an early stage of studying online surveillance, it is not proper and feasible to examine too many elements influencing the panoptic effects in a single study. Consequently, perception of surveillance as the most crucial element extracted from the Botan and McCreadie’s (1990) conceptual model is employed to preliminarily examine online panoptic effects in this study.

As Farinosi (2011) argued, panoptic effects in the traditional Panopticon and in Web 2.0 may be different. Due to different power relations involved, panoptic effects in online surveillance may not be the same with those in workplace surveillance. The roles of observers and surveilled people in workplace surveillance are unequivocally managerial officers and workers respectively.
Power and position of employers are always more overwhelming than employees who are vulnerable under workplace surveillance. But in the online context, Internet users may play dual roles as observers and surveilled people in online surveillance (Farinosi, 2011). No individuals or parties on the Internet have absolute power to control others. Therefore, it is interesting to investigate whether panoptic effects found under workplace surveillance still hold in the online environment. Moreover, the explanatory power of perceived surveillance on panoptic effects can further be illustrated in different contexts as well. With a view to extending the previous findings on electronic surveillance (Botan 1996; Vorvoreanu & Botan, 2000; D’Urso, 2005), this study explores other potential panoptic effects associated with perceived online surveillance, including higher sense of privacy infringement, more Internet stress and higher desire of self-monitoring behaviour.

Three common concerns during online communication

Technologies extend human communication from face-to-face to computer-mediated contexts. During online interaction, Internet users actively participate in surveillance by sharing personal information and seeking materials of others. In line with the frequent online activities, three common concerns related to online communication are raised, including issue of privacy protection, stress management and inclination of self-monitoring (Barnes, 2006; Gangestad & Snyder, 2000; Kraut et al., 1998; Mace & Browder, 1989; Nie et al., 2002; Taddicken, 2012). The present research adopts individual perception of surveillance as an independent factor to predict online responses and behaviour of the respondents. Specifically, it is used to investigate whether the Internet users perceive privacy infringement, feel Internet stress and act in a self-monitoring
Invasion of online privacy

When interpersonal communication becomes active in social networking sites and commercial activities are increasingly prevalent in the online platforms, concerns of surveillance and privacy infringement also increase. Many studies found that the Internet users perceived online privacy as an important issue (Barnes, 2006; Debatin et al., 2009; Taddicken, 2012; Tufekci, 2008). Individual sense of privacy infringement usually rises when the online environment is too open with anonymity, ambiguity and insecurity. While being surveilled online, Internet users might be worried that their personal information shared online is exposed to other users with uncertain purposes and identities, resulting in unexpected crisis, risks and other negative consequences.

Privacy can be illustrated in the way of controlling and regulating accesses to private information (Taddicken, 2012). Westin (1967) defined privacy as the right to prevent the personal information from being disclosed to others. Similarly, Altman (1975) explained that privacy is a kind of selective control of access to someone’s information. Control of privacy depends on different situations (Altman, 1975; Taddicken, 2012) and different individuals (Buchanan et al., 2007). As Botan (1996) stated, invasion of privacy is more likely to result when privacy expectation of individuals is high. Other studies found that privacy might also be influenced by various demographic factors, including age (Bellman et al., 2004), gender (Rodgers & Harris, 2003; Sheehan, 1999), education (Milne & Gordon, 1994; Wang & Petrison, 1993), and such personal and cultural factors as individual experience related to online context (Bellman et al., 2004; Miyazaki & Fernandez, 2001), individual interests and preferences.
Intronà & Pouloudi, 1999), and national and cultural discrepancies (Cho et al., 2009). While the abovementioned factors contribute to the explanation of invasion of privacy, this study focuses on another important predictor – individual perception of surveillance during online communication.

Surveillance and privacy are drastically competitive with each other (Bloss, 2007). Plenty of literature (Alge et al., 2006; D’Urso, 2005; Karat et al., 2005) supported that surveillance is regarded as invasion of privacy and liberty. In the workplace environment, a number of companies are prosecuted for invading employees’ privacy through the use of electronic surveillance measures in their offices (Balitis, 1998), such as electronic performance monitoring and control systems (Alge, 2001). Through these measures, employers could read employees’ email, count their keystrokes, monitor their Internet usage and even peer at their computer screen, so as to assess employees’ working performance and to check whether they do anything unrelated to their job duties during office hours. On the contrary, employees perceived less privacy infringement when their supervisors did not use any form of electronic surveillance on their activities in their offices (Eddy et al., 1999). Empirical evidence showed that workers, who had stronger belief of being surveilled by their supervisors, perceived higher invasion of privacy in their working places than workers who had less belief of being surveilled (Botan, 1996).

In addition to the working environment, Culnan (1993) recommended that privacy be examined in varying contexts, especially for online communication. The advent of social media has changed the individual sense of privacy infringement. Internet users commonly disclose their private information which is exposed in the online communication platforms such as social networking sites and discussion forums. When the shared information of Internet users is
exposed, there is likelihood of monitoring, tampering and forwarding information without owners’ notice and consent, leading to increased sense of privacy infringement. Nevertheless, self-disclosure is regarded as a requirement for communication in the online community (Taddicken, 2011). It seems that protection of own privacy is not a priority in the online interaction, but previous research found that social media users are more concerned about their privacy than expected (Barnes, 2006; Tufekci, 2008, Debatin et al., 2009). They start to consider potential risks of disclosing personal information when growing number of people can access to their information (Trottier, 2012).

Communication privacy management theory

To address privacy protection and management issues, Petronio (2002) introduced communication privacy management (CPM) theory to deal with dualistic contrast between privacy and disclosure by considering whether private information should be concealed or revealed in different contexts, including the Internet. CPM theory is established with benefit-risk calculation in which people aim to strike a balance between needs for privacy and disclosure. Petronio (2002) extend the application of CPM theory to privacy issues raised by new technologies such as the Internet. He stated that the benefits of online disclosure include relationship development with convenience, high efficiency, low cost, and social gratification from self-expression and users’ interaction. However, the corresponding risks to privacy may be increased vulnerability of private information to tampering, theft and electronic surveillance. More risks to Internet users imply higher possibility of privacy infringement and reduced self-disclosure.

Petronio (2007) further proposed five principles of privacy to activate
boundary management of private information. Firstly, people believe they own their private information. Secondly, people think they reserve the right to control the flow of their private information to others. Thirdly, people make their privacy rules to disclose information by opening private boundary or to conceal it by closing private boundary. The decisions are known as boundary management. Fourthly, when people reveal their private information, they assume other shareholders, as co-owners of the information, follow the existing privacy rules or negotiate new ones. The process of negotiation is regarded as boundary coordination. Fifthly, turbulence occurs when the privacy rules are violated by co-owners or boundary coordination is disrupted with different expectations of co-owners. Boundary turbulence often takes place owing to mistrust, anger, suspicion, or uncertainty about sharing private information.

Boundary turbulence is not a necessary process of privacy management when co-owners of private information agree with the negotiated rules. Nevertheless, privacy crises break out due to failure of coordination or deliberate violation. As Petronio (2002) argued, electronic surveillance is a typical situation which controls privacy boundaries and violates private rules of targets. With the establishment of CPM theory, this study goes further and specific to the surveillance effects on privacy infringement in the online context. When Internet users share their information in social media, they grant the rights to their friends to access the web pages. They assume those co-owners follow the implicit privacy rules and protect their information. However, due to inadequate communication or deliberate confrontation, their private information is prone to exposure and dissemination under online surveillance by someone authorized or not restricted to access their web pages. Sense of online privacy infringement is likely to result from boundary turbulence. In addition, Metzger (2007) found
that boundary turbulence experienced in the past online communication would have negative impacts on consumers’ willingness to disclose their information in subsequent online transactions. It is interesting to examine whether vicarious and personal experience during the online interaction, which induce individual perception of surveillance, could also exert an influence on individual sense of privacy infringement.

Online privacy is a serious concern in modern surveillance society with loose legal protection, especially for the private information disclosed in social networking sites (George, 2011). Anonymity, ambiguity and insecurity of the online environment might trigger individual perception of surveillance, which possibly imposes a high risk on sense of online privacy infringement. When Internet users are conscious of being surveilled, they are more likely to contemplate the possibility of exposing personal information to unknown observers. Once the information is disseminated, they are less likely to have control over protecting their own privacy boundary. Therefore, those who perceive online surveillance to be present are likely to be more cautious with the risk on invasion of privacy. Thus, the first hypothesis is posited:

\[
H1: \text{Internet users with higher level of perceived online surveillance will report higher sense of online privacy infringement than those with lower level of perceived online surveillance.}
\]

**Situational stress on the Internet**

Different from online privacy infringement, perceived stress on the Internet concerned in this research is not widely discussed and investigated in the previous literature. Nevertheless, findings in workplace surveillance provide an important
reference to study psychological discomfort under a distinctive online situation. Extending from research on electronic surveillance in workplace, the present study investigates whether perception of surveillance increases stress level of Internet users whose private information may be exposed in the online community.

Stress refers to individual response to threat while lacking in resources to overcome the stressor, irrespective of the presence of actual threat (Greenberg, 1981; Lazarus, 1966). Most kinds of Internet stress studied in the previous literature are related to Internet use and addiction (Akin & Iskender, 2011; Kraut et al., 1998; LaRose, Eastin & Gregg, 2001; Nie et al., 2002) and technical difficulties (Charney & Greenberg, 1999). Taking into account of multiple categorizations of stress, the present study focuses on another specific kind of Internet stress when users encounter an unsafe situation of exposing private information in the online environment.

Such a situational stress means individuals, who are exposed to threat to their security, perceive their incapability and vulnerability in a particular circumstance (Johnson & Medinnus, 1969; Parkes, 1961). Situational stress on the Internet is observable when people reveal their private information in social networking sites which is exposed to their friends, colleagues and relatives. They no longer have full control over their information after sharing to co-owners. Their information may be vulnerable to dissemination, theft, tampering and even online surveillance. As LeCompte (1981) stated, perceived stress is likely to result when the situation involves a high degree of uncertainty of the outcome. With perception of being surveilled online, Internet users may feel stressed, puzzled and worried about the uncertain use and dissemination of their private information.

In the previous surveillance studies, situational stress is often observed in the
working environment (Carayon, 1993, 1994; Kallman, 1993; Levy, 1994). Electronic surveillance in workplace was found to increase the stress level of employees (Aiello et al., 1991; Amick & Smith, 1992; Posch, 1993; Smith et al., 1992). In fact, 23% of employers in Britain use technology to check the quality of employees’ work, resulting in more than 30% of employees being anxious about workplace surveillance (Health, 2008). Similar findings suggested that perceived intensity of monitoring labour in call centers has a strong negative association with their well-being (Holman, Chissick & Totterdell, 2002). For instance, their telephone call records are monitored to evaluate the customer services and also check if any inappropriate private calls hinder their duties. Under such a situation of being monitored in workplace, employees become stressful under constant real and perceived surveillance. Although this kind of job stress and situational stress on the Internet are different in nature, findings of electronic surveillance in workplace have provided an important reference to study psychological discomfort under a distinctive online situation of exposing private information to anonymous observers.

In fact, workplace surveillance is considered more legitimate as it could be designed and intended for assessing employees’ performance and giving feedback for improvement. Identity of observers and purposes of workplace surveillance are usually ascertained. However, it is not likely for Internet users to acknowledge and be compatible with online surveillance because they do not know who watch them, why they are watched and what risks are imposed. Even observers are not always present with their targets, perception of being surveilled online may bring psychological threats to targets. Indeed, online surveillance is associated with high degree of uncertainty, anonymity and insecurity such as i) observers’ quantity and identity and ii) surveillance’s period, content, form and
purpose. As Foucault (1977) suggested, “The more numerous those anonymous and temporary observers are, the greater the risk for the inmate of being surprised and the greater his anxious awareness of being observed” (p. 202). Situational stress of Internet users may be serious given the unknown numbers of invisible observers hidden in the online environment. The circumstance could be even worse when Internet users cannot reject the coercive and permeable surveillance once they connect to the Internet.

As Albrecht (1986) explained, people experience situational stress when they cannot control over the scary circumstance. The difficult situation may involve conflict, a loss of status or acceptance in the eyes of their groups. No wonder online surveillance often becomes overt when targets behave improperly and their actions are criticized in the online communities. Targets may suffer from severe situational stress when their private information disclosed online is prone to exposure, tampering and dissemination. Given observations from workplace surveillance and corresponding situational stress, the second hypothesis is thus formulated as follows.

\[ H2: \text{Internet users with higher level of perceived surveillance will be more stressful online than those with lower level of perceived surveillance.} \]

**Self-monitoring behaviour**

In Foucault’s (1977) Panopticon, inmates in cells become self-monitored because that they suspect someone is watching them. They would perform in a self-disciplinary way, which is regarded as one of the panoptic effects. This kind of behaviour is not rare in the context of online communication. Some Internet users might conduct self-censorship on their disclosure in order to maintain
positive social image and avoid possible punishment from other users. When Internet users perceive online surveillance to be present and are worried about criticism of other users, they are likely to have high desire of self-monitoring of their online disclosure.

As Foucault (1977) indicated, the main purpose of the Panopticon is not only to detain inmates and seize their freedom, but also to make them self-disciplined via self-monitoring. Since the invisibility of observers makes surveillance unverifiable, perception of being surveilled leads inmates to monitor their own behaviour and devote themselves to self-disciplinary actions. It is because inmates are afraid of punishment in case their undesirable behaviours are discovered by the guard hidden in the observation tower (Foucault, 1977). In an experiment of conducting a work task, with the presence of observers, self-monitoring behaviour of an employee was observed. Provided that unproductive performance might be liable to punishment, the employee altered her behaviour to be more productive (Belfiore, Mace & Browder, 1989).

Self-monitoring refers to an expressive control which concerns the antecedents and consequences of variation in the extent to which individuals strategically cultivate public appearances (Gangestad & Snyder, 1985, 1991; Snyder, 1974, 1979, 1987). The gist of self-monitoring is “an acute sensitivity to the cues in a situation which indicate what expression or self-presentation is appropriate and what is not a corollary ability” (Gangestad & Snyder, 2000, p. 527). High self-monitors tend to be highly responsive to social cues of a situation for the sake of governing their appropriate performance; whereas low self-monitors tend to reflect their true attitude and emotion without bind of situations (Daly, 2002). People, who are high in self-monitoring, always show great adaptability to the environment and behave differently for the corresponding
situations. Conversely, people, who are low in self-monitoring, are reluctant and unable to conceal themselves and create an appropriate appearance for the situations (Covey, Saladin & Killen, 2001; Gangestad & Snyder, 2000; Greenberg & Baron, 1990; Robbin, 1993).

Reactive effects of self-monitoring are functionally related to specific environmental events (Mace & West, 1986; Nelson & Hayes, 1981; Spates & Kanfer, 1977). One of the situations or environmental events to result in self-monitoring behaviour would be frequent and immediate monitoring (Mace & Kratochwill, 1988; Nelson, 1977). Surveillance was discovered as an important external variable to self-monitoring actions (Graham, 1998). In an experiment of mock examination, a group of students seating next to each other were closely monitored by a research assistant in a high surveillance setting. Another group was put in a low surveillance condition in which the assistant appeared to be preoccupied and incapable of monitoring the students. The results showed that surveillance determines self-monitoring behaviour and reduces cheating in the examination. As surveillance implies risk of detection, the first group of students tends to avoid dishonesty owing to concerns of punishments and negative evaluation of their characters (Covey, Saladin & Killen, 2001).

Another experiment (Belfiore, Mace & Browder, 1989) on working performance found that surveillance effects on self-monitoring are intrinsic and durable after imposition. In the first stage of the experiment, intrinsic self-monitoring incentive from the employee herself was found to enhance her productivity of photocopying. After imposition of surveillance in the second stage, degree of self-monitoring and productivity of the employee were simultaneously increased. Surveillance was then extracted in the third stage, which induced lowered self-monitoring of the employee. Lowered
self-monitoring led to decreased productivity, but still higher than that in the first stage. Belfiore, Mace & Browder (1989) argued that experience with surveillance in the second stage established the reactive effects of self-monitoring in the third stage. Surveillance would still function even if it might not be present. Since the employee perceived and suspected the existence of surveillance not to be seen, the corresponding effects were still present with reduced magnitude.

Indeed, new technologies increase control over people under surveillance through their self-discipline. Intensive surveillance not only collects information about activities of individuals, but also adjusts their subjectivity in which they evaluate themselves in the way they are defined through surveillance. In workplace surveillance, a good model is designed and shaped as productive workers. Since employees are classified as fit or not fit for work, they tend to perform with higher productivity under surveillance so as to fight for awards and avoid punishments (Graham, 1998). This kind of “good model” can also be presumed on the Internet. As Zhao et al. (2008) stated, individuals are concerned with impression management not only in the face-to-face context, but also in the computer-mediated environment. The good model on the Internet may be related to some social values such as justice, ethics, and political dispositions. Internet users are likely to behave in ways that conform to these values because they aim to manage their impression to other users in the computer-mediated environment (Zhao, Grasmuck & Martin, 2008). With regard to conformity, social media users choose not to upload certain information which is harmful to their reputation. They strive to maintain their virtual images by omitting and removing damaging content. Self-censorship also includes not to behave in an inappropriate manner in the real-life context which could be
documented or photographed in social media (Trottier, 2012).

As Goffman (1959) argued, individuals not only strive to convince others to see them as sincere, respectable, and moral persons, but also have continuous self-representation so as to maintain the established positive images. Provided that social appropriateness is central and crucial to impression management (Dillard, 1990), some people may conduct self-censorship on their disclosed information to comply with the society and avoid undesirable social behaviour during online interaction. Given that self-monitoring behaviours can be best predicted by situational factor (Gangestad & Snyder, 2000) and perception of surveillance can maintain self-monitoring effects (Belfiore, Mace & Browder, 1989), the third hypothesis is generated as follows,

\textit{H3: Internet users with higher level of perceived surveillance will report higher desire of online self-monitoring behaviour than those with lower level of perceived surveillance.}
CHAPTER III: METHODOLOGY

An Internet survey of Hong Kong residents aged from 18 to 29 was conducted between 30 July and 2 September, 2012. The present study aims to investigate whether perception of online surveillance could predict perceived invasion of privacy, Internet stress and self-monitoring behaviour of the respondents to a certain extent.

Sampling

A convenience sample of Internet users with snowballing technique was drawn from the researcher’s acquaintances and some online platform users. For this snowballing sample, the respondents of the present study recruited potential respondents from their social grapevines. This sampling technique is often used in hidden populations such as people under surveillance which are difficult for researchers to access.

Since they are always anonymous and their identities are protected by Internet service providers, it is not feasible to obtain a sampling frame of Internet users for random sampling. Therefore, a convenience sample is commonly used for studying attitude and behaviour of Internet users. Since the targets of this study are Internet users, Internet survey is considered an appropriate channel to reach the target respondents with sufficient experience of using the Internet.

Respondents aged between 18 and 29 were targeted in this study as this age group of young adults were considered to be active in online interaction. In addition, their proficiency of computer skills enabled them to experience online activities and construct personal network on the Internet. With moderate to high levels of education, the potential respondents should have little difficulty in
communicating online and answering the online questionnaire.

Some scholars questioned the generalizability of Internet survey results as the respondents are mainly educated and young Internet users (Batageli & Vehovar, 1998; Zhang, 1999). The results could not be applied to other age and education groups. Nevertheless, such a concern is not applicable to the present research as the target populations of this study are computer-oriented and well-educated youth, who are able to access the Internet and are familiar with information technology.

Data collection

325 respondents participated in this survey. The respondents were invited to participate in this survey from Facebook event page and online discussion forums such as “HKGOLDEN.com” and “Discuss.com.hk”\(^2\). Purpose and source of the survey could be widely and efficiently disseminated over there. With voluntary participation, the respondents can access the questionnaire by clicking “https://qasiatrial.asia.qualtrics.com/SE/?SID=SV_9mlBqUJTRBS7JZO” as a hyperlink in a web page (see Appendix I). While filling out the electronic form, they could submit their answers to a program for tallying scores. This kind of online research could reduce errors in survey completion and data entry. Previous research showed that there were fewer completion mistakes with electronic questionnaire and fewer items were left blank in electronic responding (Kiesler & Sproull, 1986; Stanton, 1998; Truell, 2003). Since the present study is to discover online response and behavioural change of the respondents, Internet survey should be a desirable way and sometimes the only way to reach the target

\(^2\) According to Alexa (2010), the web information company, “HKGOLDEN.com” and “Discuss.com.hk” are two most famous online interaction platforms with high page views in Hong Kong.
populations (Senior & Smith, 1999).

**Survey Instrument**

The respondents normally took 15 to 20 minutes to complete the questionnaire. This questionnaire was pilot tested with fifteen members of the target population on the Internet. These respondents have sufficient experience and knowledge of the information technology and online communication. They could realize the purpose of this study and understand the meaning of most questions. They have given some constructive comments on translation, wording and sequence of the questions. Their feedback was incorporated in the revised questionnaire by making minor modification to the questions’ design, format and wording. Appendix II showed key variables with the associated questions and survey responses. To begin with, two warm-up questions related to daily usage of the Internet and the respondents’ perceived computer competency were firstly asked in the questionnaire (Items 1 & 2). Other items designed to measure the variables under study are elaborated in the following sections.

**Surveillance Index**

To operationalize the independent and the dependant variables, several scales and indices were used in this study. Perceived online surveillance as the only predictor variable in this study was measured by Botan’s (1996) Surveillance Index with modification to fit the online context. The Index is a summative interval scale of three weighted items. As Botan (1996) argued, the respondents’ perception is the most crucial component of the belief of being surveilled and thus constitutes half proportion of this index. To reflect their perception, the
respondents were asked their level of agreement for the statement, “I personally believe I am or have ever been surveilled online” (Item 18). Apart from considering oneself, the respondents’ belief of being surveilled was reinforced when supported by other Internets users. To assess the perceived support of their counterparts, the respondents were asked to what extent that they agree with the statement, “Most of the Internet users believe they are or have ever been surveilled online” (Item 19). This item constitutes one-third weight of the surveillance index because consistent belief from the counterparts could strengthen one’s confidence to his or her stance. In addition, perceived online surveillance was estimated to be high when some parties or individuals acknowledge that some Internet users are under their surveillance. The respondents were asked their level of agreement for the statement, “Some parties or individuals acknowledge that someone on the Internet is or has ever been under their surveillance” (Item 20). This item constitutes to one-sixth weight of the index. Five-point Likert scales ranging from strongly disagree to strongly agree were employed in this index (1=strongly disagree & 5=strongly agree). Score of this Index ranges from one (very low perceived online surveillance) to five (very high perceived online surveillance). Reliability of the Surveillance Index was $\alpha = .812$.

**Invasion of Privacy Score**

To examine three panoptic effects in the online environment, sense of online privacy infringement was assessed with the Invasion of Privacy Score (IPS), proposed by Fusilier and Hoyer (1980). This index was revised to fit the purpose of this study. Four statements assessing respondents’ views on the collection of their information were employed. These items include “It is
acceptable for some parties or individuals to collect my information on the Internet” (Item 3) and “Collecting my information on the Internet is an invasion of my privacy” (Item 6). Five-point Likert scales ranging from strongly disagree to strongly agree were employed in this scale (1=strongly disagree & 5=strongly agree). Items 3 and 4 were reversely coded to observe unidirectionality of the index. Reliability of the IPS was \( \alpha = .741 \) after eliminating item 5. Scores of the IPS range from one (very low privacy invasion) to five (very high privacy invasion) after being divided by the number of items.

**Perceived Stress Scale**

Stress was measured with six items from the Perceived Stress Scale (PSS) (Cohen, Kamarck & Mermelstein, 1983). To fit in with the context of this study, this scale was revised with some online components. Six questions related to the respondents’ thoughts and feelings in their recent online experiences were employed, such as “How often have you felt nervous and stressed on the Internet?” (Item 9) and “How often have you been angered because of online stuff that was outside of your control?” (Item 11). The response options were aligned with five-point Likert scales, including one (never), two (almost never), three (sometimes), four (fairly often) and five (very often). Reliability of the PPS was \( \alpha = .831 \) after eliminating item 10. After being divided with the number of items, scores of the PPS range from five to one with the maximum five points meaning “very often felt stressful” and minimum one point meaning “never felt stressful” in the online environment.

**Revised Self-Monitoring Scale**

Self-monitoring was measured with five items from the Revised
Self-Monitoring Scale (RSMS) (Lennox & Wolfe, 1984). The RSMS used in this survey captures the main self-monitoring style as the ability to modify self-presentation. To fit in with the online context, this scale was imposed with some online components. Five statements from the RSMS related to the respondents’ ability to modify their self-presentation in the online social situations such as “I have the ability to alter my online behaviour if I feel that something else is called for” (Item 13). The statements were assessed with five-point Likert scales ranging from one (strongly disagree) to five (strongly agree). Reliability of the RSMS was $\alpha = .874$ after eliminating item 17. Scores of the RSMS range from one to five (after being divided by the number of items) in this study with lower points indicating relatively low-monitoring and more points indicating high-monitoring dispositions.

**Data Analysis**

In the present study, regression analysis was deemed an appropriate way to examine whether perceived online surveillance could predict privacy infringement, perceived stress and self-monitoring behaviour to a certain extent. It was because regression analysis could provide the explanatory power of the predictor variable on the outcome variables. In gist, three simple linear regressions were used to assess the extent to which change in perceived online surveillance can explain the variances of the perceived invasion of privacy, Internet stress and self-monitoring behaviour respectively.
CHAPTER IV: RESULTS

Demographic data

325 respondents in total completed the questionnaires. They aged from 18 to 29, with a mean of 25.12 (SD = 2.76). 38.5% of them were male (n = 125) and 61.5% were female (n = 200). 79.7% (n = 259) of them completed tertiary education, 14.5% (n = 47) had postgraduate degrees or above and only 5.8% (n = 19) were secondary school graduates. The hours of Internet use every week ranged from 3 to 115 (M = 30.97, SD = 22.90). 27.7% (n = 90) of the respondents perceived their computer competency as strong or very strong, whereas 12.6% (n = 41) acknowledged that they were weak or very weak in using computer. The majority (59.7%, n = 194) thought their computer competency were neutral. As expected, the samples were composed of young adults, with basic computer skills and high education level. Frequencies and descriptive statistics of demographics and computer usage, and frequencies of independent and dependent variables were summarized in Tables 2 and 3 as follows,

Table 2. Frequencies and descriptive statistics of demographics and computer usage

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>25.12</td>
<td>2.76</td>
</tr>
<tr>
<td>Hours of using Internet per week</td>
<td>30.97</td>
<td>22.90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Number</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sex</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>125</td>
<td>38.5</td>
</tr>
<tr>
<td>Female</td>
<td>200</td>
<td>61.5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>325</td>
<td>100</td>
</tr>
</tbody>
</table>
Table 3. Frequencies of independent and dependent variables

<table>
<thead>
<tr>
<th>Education level</th>
<th>Number</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary</strong></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td><strong>Secondary</strong></td>
<td>19</td>
<td></td>
</tr>
<tr>
<td><strong>Tertiary</strong></td>
<td>259</td>
<td></td>
</tr>
<tr>
<td><strong>Postgraduate or above</strong></td>
<td>47</td>
<td></td>
</tr>
<tr>
<td><strong>Total: 325</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perceived computer competency</th>
<th>Number</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Very weak</strong></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>Weak</strong></td>
<td>38</td>
<td></td>
</tr>
<tr>
<td><strong>Neutral</strong></td>
<td>194</td>
<td></td>
</tr>
<tr>
<td><strong>Strong</strong></td>
<td>80</td>
<td></td>
</tr>
<tr>
<td><strong>Very strong</strong></td>
<td>10</td>
<td></td>
</tr>
<tr>
<td><strong>Total: 325</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 3. Frequencies of independent and dependent variables**

<table>
<thead>
<tr>
<th>1. Independent variable</th>
<th>Number</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived online surveillance</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Weak</strong></td>
<td>52</td>
<td>16</td>
</tr>
<tr>
<td><strong>Neutral</strong></td>
<td>114</td>
<td>35.1</td>
</tr>
<tr>
<td><strong>Strong</strong></td>
<td>159</td>
<td>48.9</td>
</tr>
<tr>
<td><strong>Total: 325</strong></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Dependent variables</th>
<th>Number</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sense of online privacy infringement</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Weak</strong></td>
<td>39</td>
<td>12</td>
</tr>
<tr>
<td><strong>Neutral</strong></td>
<td>99</td>
<td>30.5</td>
</tr>
<tr>
<td><strong>Strong</strong></td>
<td>187</td>
<td>57.5</td>
</tr>
<tr>
<td><strong>Total: 325</strong></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>
Remark: Scores of 4 scales measuring independent and dependent variables range from 1 to 5.  
(Weak: below 2.33, Neutral: 2.33-3.66, Strong: above 3.66)

Perceived online surveillance

The mean of the Surveillance Index was 3.49 ($SD = 0.83$) with the score ranging from one (very low perceived online surveillance) to five (very high perceived online surveillance). One sample t-test showed that the sample mean was significantly higher than the mid-point of the Surveillance Index ($t = 10.66$, $df = 324$, $p < .001$).

Three hypotheses

**Sense of privacy infringement and perceived online surveillance**

*H1:* Internet users with higher level of perceived online surveillance will report higher sense of online privacy infringement than those with lower level of perceived online surveillance.
H1 was supported \((r = .361, r^2 = .130, p < .001)\). Perceived online surveillance was found to be a significant factor influencing Internet users’ assessed sense of online invasion of privacy. It explained 13% of the variance of sense of privacy infringement. The respondents perceived a lack of privacy in the online context, with a mean of 3.61 \((SD = 0.83)\). One sample t-test showed that the sample mean was significantly higher than the mid-point of the IPS \((t = 13.27, df = 324, p < .001)\).

**Internet stress and perceived online surveillance**

*H2: Internet users with higher level of perceived surveillance will be more stressful online than those with lower level of perceived surveillance.*

H2 was supported \((r = .332, r^2 = .110, p < .001)\). Perceived online surveillance was found to be a significant factor influencing situational stress on the Internet. It explained 11% of the variance of Internet stress. It was not obvious that the respondents suffered from heavy stress in the online context, with a mean of 2.31 \((SD = 0.64)\). One sample t-test showed that the sample mean was significantly lower than the mid-point of the PSS \((t = -19.47, df = 324, p < .001)\).

**Desire of self-monitoring behaviour and perceived online surveillance**

*H3: Internet users with higher level of perceived surveillance will report higher desire of online self-monitoring behaviour than those with lower level of perceived surveillance.*

H3 was supported \((r = .378, r^2 = .143, p < .001)\). Perceived online surveillance was found to be a significant factor influencing individual desire of
self-monitoring behaviour. The predicting variable explained 14.3% of the variance of this outcome variable. The respondents tended to be high in desire of self-monitoring behaviour in the online context, with a mean of 3.24 (SD = 0.89). One sample t-test showed that the sample mean was significantly higher than the mid-point of the RSMS (t = 4.76, df = 324, p < .001).

The results of all three hypotheses in the present study are summarized in Table 4, which contains three regression analyses of dependent variables affected by online surveillance.

| Table 4. Regression analyses of dependent variables affected by online surveillance |
|---------------------------------|-----------------|-----------------|-----------------|
| Dependent Variables             | Unstandardized Coefficient | R Square | Significant level |
| Invasion of online privacy      | 0.363            | 0.130         | p < .001        |
| Situational stress on the Internet | 0.256           | 0.110         | p < .001        |
| Self-monitoring behaviour      | 0.406            | 0.143         | p < .001        |
CHAPTER IV: DISCUSSION & CONCLUSION

This study examined three possible panoptic effects under online surveillance and found the significant results from the regression analyses. The findings showed that individuals’ perception of online surveillance could predict their sense of online privacy infringement, perceived situational stress and desire of self-monitoring behaviour in the online context to a certain degree.

Perception of online surveillance

Perception of surveillance embedded in the surveilled people was found to have an explanatory power to human response and behavioural change in the online environment. Although the predictor could only explain around ten something percent of variances of the outcomes variables, the present study successfully identified perception of online surveillance as a significant influence on Internet users’ attitudes and behaviors. Its importance to explain the change on human feedback and behaviour while communicating with other Internet users was also observed.

It is essential to identify the perception of online surveillance while examining panoptic effects as such a perception is negligent of actual presence of surveillance, but it still exerts an influence on human attitudes and behaviors. On the contrary, no panoptic effects will be generated if individuals are not aware of surveillance while communicating with others, (Botan, 1996; Botan & McCreadie, 1990; D’Urso, 2005; Foucault, 1977). The respondents in this study perceived relatively strict surveillance in the online context, consistent with Botan’s (1996) study on the employees’ perception of workplace surveillance. These two studies discovered that perception of surveillance and various kinds of
panoptic effects do exist in both the closed setting (workplace) and the open environment (the Internet).

**Three Panoptic effects**

Privacy, stress and self-monitoring have been examined in the face-to-face context for several decades (Belfiore, Mace & Browder, 1989; Covey, Saladin & Killen, 2001; Folkman, 1984; Thompson, 1981; Wang & Petrison, 1993). The present study went further to examine abovementioned variables as panoptic effects in the online context. It discovered that change in perception of online surveillance could explain change in sense of online privacy infringement, perceived situational stress on the Internet and desire of self-monitoring behaviour to a certain extent.

**Higher sense of privacy infringement**

According to the findings of this study, sense of privacy infringement was considered serious on the Internet. Due to easy trace of electronic information and anonymous identity of observers on the Internet, high risk is imposed on online privacy protection. A regression analysis of this research showed that change in perception of online surveillance could explain 13% of the variance of sense of privacy infringement.

The present findings showed that higher sense of online invasion of privacy results when the respondents perceived higher level of online surveillance \( r = .361, r^2 = .130, p = <.001 \). When the respondents are aware of being surveilled on the Internet, they realize the information they share online may be exposed to anonymous observers. For instance, electronic monitoring on consumers’ online behaviour is a common surveillance practice in commercial
industries. When Internet users seek information from Yahoo and Google search engines, their preferences and interests are stored in the database for advertising selection. In order to stimulate consuming desires, commercial advertisements related to their search could be seen in the eye-catching area of the webpage. Internet users may perceive less online privacy as their interests and preferences are captured and stored by the Internet surveillance systems.

Apart from commercial operations, Internet users might be surveilled by other anonymous users with uncertain purposes. With regard to online safety and privacy protection, Internet users might choose to expose the information to any person and exclude someone’s visit by setting the level of privacy security in social networking sites. However, they can still hardly control the flow of their information after posting text, photos and videos in social networking sites. The information could be stored, forwarded or even tampered by someone out of the exclusion. It is not surprising that coercive advertising selection and dissemination of personal information among Internet users are likely to result at the expense of privacy infringement. On the contrary, when Internet users are unaware of online surveillance, they are less likely to worry about whether their online data might be used or misused by others. Some might only regard their online posts as a leisure sharing with their friends to obtain social gratifications. They do not perceive any potential online surveillance conducted in their social networking sites. Therefore, their sense of online privacy infringement was found to be low in this study.

Nevertheless, change in perception of online surveillance only explained 13% of the variance of sense of online privacy infringement. Such a minor influence may be due to the following reasons. Some respondents do not have a profound knowledge of data abuse and sense minimal threats of being exposed to
unknown observers. They may think that surveillance has little harm on them and its effects are exaggerated. Therefore, they might not perceive high invasion of privacy even if they are aware of online surveillance. Moreover, some respondents might think that they do not fear full online disclosure because they have nothing bad to hide. They have little concern on protecting their own privacy even under online surveillance. In addition, privacy paradox (Barnes, 2006; Taddicken, 2012) might affect the respondents’ sense of online privacy infringement in which they perceive benefits from social interaction outweigh its potential risks. When the information Internet users exposed is unimportant and has little impacts on their daily functions of lives, they might assess that social gratifications obtained from online self-disclosure could compensate the cost of information exposed to observers. Therefore, even when they are aware of online surveillance from other Internet users, they may underestimate the prevalence of invasion of privacy online.

Although perception of online surveillance made a little contribution to individual sense of privacy infringement, this study provides a significant new insight into investigating invasion of privacy in the online environment. Apart from demographic and cultural factors stated in the previous studies (Bellman et al., 2004; Cho et al., 2009; Sheehan, 1999; Wang & Petrison, 1993), perception of online surveillance should be put into consideration for a comprehensive analysis of privacy infringement. Such findings contribute significantly to surveillance studies, particularly those in the online context.

**Increased situational stress on the Internet**

Situational stress of the respondents perceived on the Internet was not high in this study, but the finding showed that the respondents felt more stressful when
they perceived higher level of online surveillance ($r = .332$, $r^2 = .110$, $p = <.001$).

Internet users with perception of being surveilled online may feel stressed and worried about the uncertain use and dissemination of their private information exposed to observers. Since perceived online surveillance reduces autonomy and control of Internet users, they are less likely to share their views and emotions without reservation. Instead, they might prevent their disclosure from being tampered, challenged and attacked by observers so as to avoid such a situational stress under online surveillance.

Situational stress is often imposed on some immature or careless Internet users who unintentionally offend others in the online environment and thus suffer from detrimental consequences. According to a recent piece of hot news, a bribe-to-be has encountered a serious criticism in the online platforms after someone forwarded her acid and unkind words to other Internet users. In her Facebook page, she expressed that friends and relatives with only monetary wedding gift of HK$500 were not welcomed in her wedding banquet. Her “grant event” was not designed for charity use. Her expression stimulated harsh feedback from anti-materialists. A large scale of cyber bullying and malicious surveillance was conducted on the bribe-to-be. She finally deleted her Facebook account and tried to escape from the severe moral criticism. In order to ask for release from Internet stress, the groom-to-be posted an apologia on behalf of her fiancé and showed his support to their relationship. However, stress of the bribe-to-be even extended from the Internet to the real-life context as large news coverage stimulated fierce social discussion.

It is convincing that online surveillance reduces control of the Internet users over their environment when information is easily retrieved and disseminated. This piece of news could raise the public concerns of hasty and reckless online
disclosure. Situational stress and tension could be drawn from judgment and criticism of other Internet users under online surveillance. They should take these risks and negative consequences into consideration while disclosing private information in the online context.

In addition to loss of control, uncertainty might trigger Internet stress under online surveillance. The previous studies demonstrated that uncertainty constitutes a powerful stressor (Monat, Averill, & Lazarus, 1972; Zakowski, 1995). Compared with workplace surveillance, online surveillance takes place with more uncertainty. Observers of electronic monitoring in the working environment are usually supervisors or corporation management. Workplace surveillance aims to assess employees’ working performance and regulate their behaviour in office hours through the electronic monitoring systems. However, in the online context, Internet users usually do not realize who act as observers, when, why and how they conduct surveillance. Due to the visibility-invisibility contrast in Cyber Panopticon, targets on the Internet could perceive to be surveilled by someone, but they may not know number and identity of observers, who seem to be omnipresent in the virtual reality. Such a contrast induces anonymity and mystery of observers hidden during online interaction, leading to great sense of targets’ uncertainty of observers and insecurity of the surveillance situation. Suffering from large uncertainty and insecurity, Internet users might estimate potential risks and consequences under online surveillance, resulting in heavy pressure and increased stress.

Nevertheless, similar to the findings of privacy infringement, change in perception of online surveillance only explained 11% of change in perceived situational stress. A possible reason for such a minor influence is that stress, as a complicated psychological response, should be caused by numerous factors in the
online context. Besides perception of online surveillance, below factors are some possible reasons to explain and predict situational stress on the Internet. Firstly, situational stress emerges from daily Internet hassles as a technological source. Frequent job mails and malfunction of computers always trigger disturbance and impatience of employees, followed by high level of stress. When Internet users are unable to seek crucial information from the web, they might feel troubled, helpless and stressful. Sometimes, perceived stress stems from finance pressure such as due electronic bill payment and online stock checking.

In addition to technological causes, personal psychological attributes could explain the emergence of Internet stress. As LaRose, Eastin & Greggi (2001) argued, self-efficacy could reduce the effect of Internet stress. When people perceive high capability of solving problems in the online environment, they are less likely to regard the difficulties as negative scenarios and experience stress. Moreover, some Internet users might suffer from unpleasant and stressful events such as ignorance and isolation in social networking groups, and criticism by their friends and colleagues owing to lacking in prompt response to online invitation. The undesirable personal experience may lead to accumulated situational stress which in turn contributes to greater pressure, depression and stress. In view of many possible causes, perceived online surveillance should not be taken lightly as a minor factor to explain situational stress. It is because individuals increasingly disclose their information in the online environment. They are relatively incapable of protecting disclosed materials, which are vulnerable to misuse and tampering under online surveillance. Therefore, they are hardly to escape from situational stress while threat to their security increases.
**Higher desire of self-monitoring behaviour**

The respondents’ desire of self-monitoring behaviour in the online environment tended to be high as found in this study. The findings showed that individuals reported higher desire of self-monitoring behaviour on the Internet when they perceived higher level of online surveillance ($r = .378$, $r^2 = .143$, $p = <.001$). It is consistent with the previous research on campus and workplace contexts in which cheating behaviour of students in examination was restricted and productivity of the employee was increased under surveillance (Belfiore, Mace & Browder, 1989; Covey, Saladin & Killen, 2001).

Providing additional support to the previous studies on self-monitoring (Graham, 1998; Mace & Kratochwill, 1988; Nelson, 1977), this study discovered online surveillance to be another environmental factor that influences individual perception and explain the corresponding self-monitoring behaviour. While communicating with others online, Internet users are conscious of potential surveillance by someone. They may have a high desire of self-censorship on their online disclosure so as to avoid possible sanctions for improper manners or acquire credits from other Internet users. They might be or pretend to be socially desirable during online interaction. For instance, some Internet users have online connection with their friends in social networking sites. They may hesitate to post their sexy photos and sensitive texts online as they are concerned about perception of their friends, who are not familiar with their personality and may have an undesirable judgment on their private lives based on their disclosure. Even sexy photos and sensitive texts are shared, they may have a stricter privacy setting to avoid criticisms from non-intimate friends.

In addition to relationship with friends, gossip and rumour in offices are seldom shared in public to avoid embarrassment and argument among working
groups. However, those whispers are sometimes disseminated among social networking sites of gossipy employees. Some American companies have dismissed their employees not because of their poor working performance, but their self-disclosure in social networking sites, including their gossips undermining the reputation of colleagues and their grumbles or even complaints to their supervisors (Searcey, 2009). The management may feel uncomfortable when the employees do not behave in both of their working and social lives. Employees should be always reminded that contaminating personal reputation may lead to destructive working relationships and job insecurity. Instead of showing improper conduct and manner, Internet users tend to monitor their self-disclosure and strive to create a positive social image in the online environment.

The present study has provided some empirical evidence to use the Panopticon (Foucault, 1977) as a metaphor in surveillance studies. The findings showed that perception of online surveillance could predict individual desire of self-monitoring behaviour to a certain degree. This result is compatible with Foucault’s (1977) indication that the Panopticon is designed mainly for making the inmates self-disciplined and self-monitored. This original objective still exists and functions in Cyber Panopticon. Although Cyber Panopticon is regarded as a surveillance situation without concrete walls and observation tower, namely Superpanopticon (Poster, 1990), the invisibility-visibility contrast still contributes to automatic functioning of power. The invisibility of observers facilitates the unverifiable surveillance in the Panopticon. Internet users do not know who is watching them and when they are being watched, the perception of being surveilled is already embedded in their minds. Therefore, they may perform as if online surveillance takes place even when there is not any observer.
In this sense, self-monitoring behaviour is likely to result in order to prevent themselves from social isolation and condemnation by other Internet users.

Nevertheless, the findings showed that change in perception of online surveillance only explained 14.3% of change in individual desire of self-monitoring behaviour. As Gangestad and Snyder (2000) stated, self-monitoring behaviour can be best explained by situational factors and personality traits. In addition to online surveillance as a situational cause to form individual perception, personality traits of individuals contribute to different tendency of self-monitoring. Egocentric persons highly consider their own thoughts and neglect the requirement of situation or environment. They are less likely to be affected by online surveillance since they do not pay much attention on others’ criticism and punishment. Moreover, emotional stability could influence self-monitoring of individuals. The bad mood might overwhelm the rationality and trigger abnormal behaviour. In an irritative condition, people tend to release their anger and may perform in an inappropriate manner. Together with personality traits, perceived online surveillance may be a significant factor to explain individual desire of self-monitoring behaviors. In order to establish positive social images, Internet users tend to have a high desire of self-censorship on their online disclosure, especially when they perceive to be surveilled by someone in the online context.

Limitations

Perceived online surveillance was regarded as a single predictor in the present research. With small R square values being obtained from the regression analyses, perceived online surveillance could only contribute to about one-tenth of each outcome variable, including sense of privacy infringement, situational stress
and desire of self-monitoring behaviour. But for a primary study, such results are a satisfactory beginning to investigate online surveillance effects.

Since the present study employed a convenience sample of Hong Kong Internet users, the results may not be representative to the whole population due to the possible self-selection bias. In fact, this sampling method is common for studying Internet phenomenon and online behaviour because it is not feasible to obtain a full list of Internet users globally or locally. Nevertheless, the sample employed in this study is more purposive in nature and restricted to the specific age group from 18 to 29. There should not be a great discrepancy between the sample and population as both parties are young Internet users and experienced in information seeking and sharing in the online environment.

Moreover, Internet survey could assure the computer competency of the respondents, who were required to finish the questionnaires on the web. As the invitation to participate was posted in the two most famous online forums in Hong Kong, the respondents of this study should fall into the target group of active and young Internet users. Furthermore, the present Internet survey was a kind of self-report study. Answers of the respondents might be exaggerated or concealed, resulting in social desirability bias, in which they tended to over-report good behaviours and under-report bad behaviours. However, measures have been taken in the questionnaire design to minimize such a tendency. For instance, questions related to personal attributes are asked in the beginning. Then, questions in the Surveillance Index were put into the almost last part of the questionnaire so as to prevent the respondents from reporting socially desirable answers which might deliberately show that online surveillance exerted an influence on sense of privacy infringement, Internet stress and desire of self-monitoring behaviour.
Recommendations for further studies

Examining outcome variables with multiple predictors should be a proper way to study online surveillance and establish a well-constructed model in further studies. In addition to perceived online surveillance in the present research, locus of control (Kolb & Aiello, 1996) and Internet self-efficacy (Bandura, 1997) may be effective predictors of Internet stress. The interaction among three recommended predictors might constitute a greater explanatory power to Internet stress. While studying effect of online surveillance on self-monitoring behaviour, personality traits, personal experience and psychological state of Internet users should be taken into consideration.

After determining possible predictors, wise methodology could help to detect a significant and satisfactory result of the studies. Apart from quantitative research methods used in the present study, qualitative apparatus such as focus group and in-depth interviews are recommended to obtain valuable information such as views and feelings of coercive surveillance from Internet users. Their actual experience of being surveilled and even cyber bullying should greatly contribute to online surveillance studies in the future.

Peer-to-peer surveillance in the online environment enables active participation of Internet users. Since new surveillance technologies facilitate to a relatively symmetrical structure of visibility of Internet users, they can play a dual role as observers and surveilled people during online interaction (Farinosi, 2011). Therefore, surveillance practice in the online situations should be more complicated. In comparison and contrast between the traditional and Cyber Panopticons (see Table 1), roles of Internet users can be classified as pure observer, pure surveilled, observer-surveilled and non-observer-surveilled. These four surveillance groups may have different attributes, attitudes and
behaviour. Further studies can use this typology for classification of Internet users in order to investigate and compare the difference of their responses towards online surveillance.

**Conclusion**

The present study further explored the effects of online surveillance and discovered that perceived online surveillance of individuals influenced their sense of online privacy infringement, perceived situational stress on the Internet and desire of self-monitoring behaviour. Findings of this research complement to the previous surveillance studies by considering visibility-invisibility contrast on the Internet, and substantiate the negative consequences of online surveillance. After assuring threats derived from online surveillance, public concerns of online privacy protection may be raised and a particular online situation changing their emotion and behaviour can be identified.

For the practical implications of the present study, findings of online surveillance may trigger the Internet users to pay extra attention to their necessity and degree of self-disclosure in the online environment. They should be always alert of being exposed to risk and danger after disclosing private information, provided that individuals are less likely to escape from being monitored with advanced surveillance technologies.

By and large, Internet gradually plays an important and even dominant role in human communication, especially for the young generations and commercial partners. It is admitted that the online network provides both opportunities and threats to the society. Internet users need to strike a balance between perceived benefits from social interaction and potential risk of exposing personal information. Before thorough understanding of human behaviour in the online
context and progress of technological development, Internet users should not
overestimate their ability to oppose against online surveillance and underestimate
its negative impacts to individuals, organizations and governments.
REFERENCES


APPENDICES

Appendix 1. Screen capture of Internet survey

Page 1

As a postgraduate student of School of Communication in Hong Kong Baptist University, I am conducting an Internet survey on “Online Surveillance” to investigate the emotional and behavioral changes of Internet users who communicate with others through social media. I am pleased to invite you to complete this questionnaire. Your responses and personal information will only be used for academic research and kept confidential.
Before answering the questionnaire, please peruse the definition of online surveillance so as to enhance the accuracy of your responses.

Online surveillance is defined as "seeking purposeful, routine, systematic and focused attention paid to personal details on the Internet for the sake of control, entitlement, management, influence or protection."

You perceive your computer competency as

- Very weak
- Weak
- Neutral
- Strong
- Very strong
我可以接受某組織或某人在網上搜集有關我的資料。
It is acceptable for some parties or individuals to collect my information on the Internet.
- 非常不同意 Strongly disagree
- 不同意 Disagree
- 無意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree

我認為某組織或某人有必要在網上搜集有關我的資料。
It is necessary for some parties or individuals to collect my information on the Internet.
- 非常不同意 Strongly disagree
- 不同意 Disagree
- 無意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree

我認為有必要加強限制某組織或某人如何使用在網上搜集得來的資料。
Greater controls are needed to limit how parties or individuals use the information they collect on the Internet.
- 非常不同意 Strongly disagree
- 不同意 Disagree
- 無意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree

我認為在網上搜集有關我的資料是侵犯我的個人私隱。
Collecting my information on the Internet is an invasion of my privacy.
- 非常不同意 Strongly disagree
- 不同意 Disagree
- 無意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree
你有冇覺得因為網絡上的突發事情而感到不爽？
How often have you been upset because of something that happened online unexpectedly?
- 從不 Never
- 甚少 Seldom
- 有時 Sometimes
- 時常 Usually
- 经常 Very Often

你有多常感觉到網絡活動中的事情不受自己控制？
How often have you felt that you were unable to control the important things in your cyber life?
- 從不 Never
- 甚少 Seldom
- 有時 Sometimes
- 時常 Usually
- 经常 Very Often

你在網絡上是否經常感到緊張和壓力？
How often have you felt nervous and "stressed" on the Internet?
- 從不 Never
- 甚少 Seldom
- 有時 Sometimes
- 時常 Usually
- 经常 Very Often

你在網絡上是否經常感到控制自己的真面情緒？
How often have you been able to control irritations in your cyber life?
- 從不 Never
- 甚少 Seldom
- 有時 Sometimes
- 時常 Usually
- 经常 Very Often

你在網絡上有多常因為事情失控而感到憤怒？
How often have you been angered because of online stuff that was outside of your control?
- 從不 Never
- 甚少 Seldom
- 有時 Sometimes
- 時常 Usually
- 经常 Very Often
Page 5 (Continued)

How often have you felt online difficulties were piling up so high that could not be overcome?

- Never
- Seldom
- Sometimes
- Usually
- Very Often

Survey Powered By Qualtrics

Page 6

I have the ability to alter my online behaviour if I feel that something else is called for.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I have the ability to control the way I come across people on the Internet, depending on the impression I wish to give them.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

When I feel that the image I am portraying online is not working, I can readily change it to something that does.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
我可以根據情況調整我的網路行為。
I have found that I can adjust my online behaviour to meet the requirements of any situation I find myself in.

- 非常不同意 Strongly disagree
- 不同意 Disagree
- 持意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree

我在網絡上很難裝扮出正面積極的樣子，即使這樣對我有利。
Even when it might be to my advantage, I have difficulty putting up a good front in online network.

- 非常不同意 Strongly disagree
- 不同意 Disagree
- 持意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree
我相信我曾经或现在在网络上被监视。
I personally believe I am or have ever been surveilled online.

- 非常不同意 Strongly disagree
- 不同意 Disagree
- 網意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree

大部分网络使用者相信他们曾经或现在在网络上被监视。
Most of the Internet users believe they are or have ever been surveilled online.

- 非常不同意 Strongly disagree
- 不同意 Disagree
- 網意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree

我曾听说某些团体或个人在网上监视别人。
I have heard that some parties or individuals performed online surveillance on someone.

- 非常不同意 Strongly disagree
- 不同意 Disagree
- 網意見 Neutral
- 同意 Agree
- 非常同意 Strongly agree
你今年多少歲？
How old are you?

<table>
<thead>
<tr>
<th>&lt;18</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>29</th>
<th>&gt;29</th>
</tr>
</thead>
</table>

性別
Sex
- 男 Male
- 女 Female

工作月薪
Monthly income
- HK$0 - $4,999
- HK$5,000 - $9,999
- HK$10,000 - $14,999
- HK$15,000 - $19,999
- HK$20,000 - $24,999
- HK$25,000 - $29,999
- >HK$29,999

教育程度
Education Level
- 小學或以下 Primary or below
- 中學 Secondary
- 大學及及以上學歷 Tertiary
- 碩士或以上 Postgraduate or above
- 其他 (請註明) Other (Please specify)

Survey Powered By Qualtrics
## Appendix 2. Key variables with associated questions and survey results

<table>
<thead>
<tr>
<th>Variables</th>
<th>Survey Statements and Questions</th>
<th>Results</th>
</tr>
</thead>
</table>
| Perceived online surveillance | • I personally believe I am or have ever been surveilled online.  
• Most of the Internet users believe they are or have ever been surveilled online.  
• I have heard that some parties or individuals performed online surveillance on someone.                                                                                     | Mean = 3.49  
SD = 0.83  
Alpha = .812 |
| Sense of online privacy infringement | • It is acceptable for some parties or individuals to collect my information on the Internet.  
• It is necessary for some parties or individuals to collect my information on the Internet.  
• Collecting information on the Internet is an invasion of my privacy.                                                                                                           | Mean = 3.61  
SD = 0.83  
Alpha = .741 |
| Situational stress on the Internet | • How often have you been upset because of something that happened online unexpectedly?  
• How often have you felt that you were unable to control the important things in your cyber life?  
• How often have you felt nervous and stressed on the Internet?  
• How often have you been angered because of online stuff that was outside of your control?  
• How often have you felt online difficulties were piling up so high that could not be overcome?                                                                                | Mean = 2.31  
SD = 0.64  
Alpha = .831 |
| Desire of online self-monitoring behaviour | I have the ability to alter my online behaviour if I feel that something else is called for. | Mean = 3.24  
SD = 0.89  
Alpha = .874 |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I have the ability to control the way I come across people on the Internet, depending on the impression I wish to give them.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When I feel that the image I am portraying online is not working, I can readily change it to something that does.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I have found that I can adjust my online behaviour to meet the requirements of any situation I find myself in.</td>
<td></td>
</tr>
</tbody>
</table>
CURRICULUM VITAE

Academic qualifications of the thesis author, Mr. IP Wai Ho:

- Received the degree of Bachelor of Social Science (Honours) in Communication (Organizational Communication) from Hong Kong Baptist University, November 2007.

November 2013