Cultural Studies@Lingnan 文化研究@嶺南

Volume 36 *第三十六期 (2013) : 教育疑難何其多*

Article 8

9-2013

Right to privacy and surveillance in a technology-mediated society

Hoi Yu Polly POON

Follow this and additional works at: http://commons.ln.edu.hk/mcsln

 Part of the Critical and Cultural Studies Commons

Recommended Citation

POON, Hoi-yu Polly (2013). Right to privacy and surveillance in a technology-mediated society. Cultural Studies@Lingnan, 36.
Retrieved from http://commons.ln.edu.hk/mcsln/vol36/iss1/8/

This 文化評論 Criticism is brought to you for free and open access by the Department of Cultural Studies at Digital Commons @ Lingnan University. It has been accepted for inclusion in Cultural Studies@Lingnan 文化研究@嶺南 by an authorized editor of Digital Commons @ Lingnan University.

Right to Privacy and Surveillance in a Technology-mediated Society

Poon Hoi-yu Polly

Introduction

Under the rapid growth and fast penetration of technological innovations such as internet and e-mail communication under a neo-liberal economic order since the 80s, people in Hong Kong become highly technology-mediated nowadays in their daily lives across different disciplines including political, economic and cultural activities. One side of the arguments suggested that legal protection of privacy in Hong Kong developed in the pre-digital era is not applicable to the digital world. This has posed unprecedented challenges to privacy protection in recent years. However, another side raised that personal privacy is no longer important to the individuals in the digital world nowadays. Facebook founder, Mark Zuckerberg, argued "privacy is dead"[1] by elaborating that privacy is only an obsolete social norm. He believed people enjoy sharing their personal information publicly online nowadays. In response to Mark's claim, this paper will review the importance of privacy by re-examining the concepts of privacy as suggested by Jurgen Habermas and Beate Roessler, who related privacy with individual autonomy and construction of personal identity.

A case study approach was chosen to review and discuss the effectiveness of the privacy laws in Hong Kong in the first part of the study. Yahoo! Shitao case in 2005 was selected to be scrutinized in this paper as this case touches on a number of controversial privacy issues uniquely to this digital era such as definition of "personal data" in digital realm and cross-border data transfer etc. The paper is to unfold the unprecedented challenges posed to privacy protection and the ambiguity of the local legal legislations under the development information and communication technologies in an information society. This is also to point out that the vagueness is

actually authorizing and legalising privacy intrusion and surveillance practices in the society.

Furthermore, this study also aims to examine privacy intrusion and surveillance by introducing a cultural studies perspective. Michel Foucault's concept of governmentality is employed as a framework to understand the development of technologies and surveillance from the 18th century to the information age nowadays. It is to provide an alternative account on technologies, surveillance and the normalisation of ubiquitous surveillance nowadays under a neo-liberal framework.

Privacy in Informational Age

Importance of Privacy

The paper begins by examining the history of the notion of privacy. The following 2 key conceptual building blocks will be covered to reveal how they shaped our expectation and laws afterwards.

Public-private divide concept introduced by Jurgen Habermas[2] explained the co-extensive relationship of public and private domain and the importance of protection of private right to public good. Jurgen Habermas's Structural Transformation of the Public Sphere published in 1962 provided a good account of the emergence of the public and private sphere in the modern form. The public space is the space in which private persons gather to discuss public matters and compete with a view to arriving at consensus to provide the basis and authority of public policy. However, in Habermas's view, the source of control and criticisms are found in the private sphere instead. Privacy emerges at this time as a key principle of central importance to the public sphere. According to this, privacy concept of the public sphere was woven into the legal structure of the state in Europe and the private person acquired constitutional protections.

Moreover, a recent study by Beate Roessler in 2005 related privacy with autonomy. In her view, autonomy is about the subjective capacity to take a decision plus follow it through; and the external (social, political or technological) conditions that make such action possible[3]. She suggested that privacy; which is associated with control over access to various aspects of the self; is in three different dimensions namely decisional, informational and local privacy. It is essential to have the state's protection of the private sphere to provide an external condition that promotes autonomy in decision making, access of information and preventing physical intrusion. She further elaborated privacy protection enables a person to construct his or her own identity and ward off the manipulation of desire.

In their views, privacy is associated with individual autonomy instead of just protecting personal information from sharing publicly without a previous consent. Privacy is a concept apart from "right to be let alone" (Warren & Brandeis, 1890)[4], the importance of privacy protection also enables a person to construct his/ her own identity by preventing the manipulation of desire.

Emergency of data economy in Information Society

Economy of Hong Kong shifts away from manufacturing to service industry since the 80s. GDP contributed by industrial production decreased from 22.8% in 1980 to 16.7% ten years later. While the share from service industries increased from 68.3% to 75.4% in the same period according the figures from Census and Statistics Department in Hong Kong[5].

As suggested by Manuel Castells, in information society, the creation, distribution, use, integration and manipulation of information become one of the significant economic, political, and cultural activities[6]. In view of this, Hong Kong has also changed from industrial society to information society. Citizens are becoming highly technology mediated in their daily lives. Nowadays, we are relying on technologies such as Octopus card, credit cards or access card for transportation, settling

payments, accessing premises; communication technologies like ubiquitous Wi-Fi/ 3G connection to get connected with each other in the world anytime anywhere; interacting with various web platforms or applications to complete banking transactions or passport application and involve in a political discussion or pictures sharing online. Citizens actively engage with systems and generate a vast amount of person-specific data upon every interaction or dialogue with technologies in both their public or private sphere. Besides, the distribution, use, integration and manipulation of data become more significant in both public and private bodies nowadays.

Both public and private bodies are motivated to gather personal data in a new stage of capitalist economy called post-fordism in order to improve product or service design and differentiation. According to Stuart Hall's article "Brave New World"[7], socio-economic order of capital accumulation changed from mass production to flexible accumulation, production and consumption. Post-fordism not only associated with the shift of economic system, but also social and cultural changes through the maximization of the individual choices. Technology innovations enable flexible specification of production in small-batch and quick changeover of product lines to support the differentiated consumption behaviour. In view of this, collection of customer data became useful in personalisation of product and communication to different customers. In the late 80s, database marketing emerged as a new marketing discipline, with new technologies enabling customer personal data and responses to be recorded with the aim of opening up a two-way communication, or dialogue, with the individuals. Since then, customer data become a profitable business discipline[8]. According to Hong Kong Direct Marketing Association (HKDMA) in Hong Kong, direct marketing in electronic form riding on database or traditional channels is now recognized not just as the fastest growing segment of the marketing business, but also the segment that produces the most substantial profits for every business from financial services to fast moving consumer goods[9]. In 2005, direct marketing sales accounted for 10.2% of the total US Gross Domestic Product (GDP). HLDMA estimated that the size of direct marketing business in Hong Kong is roughly a tenth of that in the United States as it relates to direct mail.

Ubiquitous Surveillance in Information Society

As proposed by Surveillance Studies Network (SSN) in the United Kingdom, ubiquitous surveillance society is a society which is organised and structured using technologies for extensive collection, recording, storage of data for the individuals or groups about their activities or movements in public or private spaces and also analysis, sorting, categorising and using as a basis for decision-making in private or public organisations[10]. Information society provides the technology platform for the emergence of surveillance society. However, without the political economy working together, ubiquitous surveillance may not able to be formed in the society. As discussed previously, public and private bodies in Hong Kong actively collect, record, analyze and use of individual data with the purpose of governing, regulating, managing or influencing what they do in the future. Octopus card transactions, retail loyalty programmes, website cookies, IP address, GPS, mobile calls, identity card scheme and routine health screening are all qualified as surveillance at private or public organisations. Besides, the enhanced data mining and profiling technology nowadays are able to process massive personal data rapidly, with low cost to provide a full description of a person with attribute descriptions such as geographical location, web browsing behaviour, purchase preference, dining habit, demographics data like gender, income bracket, schooling levels, professional qualifications, marriage status etc. It is a systematic use of personal data systems in the investigation or monitoring of the actions or communications. In Roger Clarke's view, such activities are regarded as data surveillance at individual level[11]. In this sense, technologies assist the formation of surveillance society in Hong Kong in the era of post-fordism. Data collection at individual level is justified in the name of providing personalised products and services.

Unprecedented challenges to Data Protection

In view of this, individuals have to face unprecedented challenges below to personal privacy in the information age under neo-liberal rules[12].

- Enormous amount of data

Interactive nature of internet generates vast amount of person-specific information as every interaction or dialogue; such as simply a click on a button; between a user and a system will be captured. All these leave traces can create challenges in data handling

- Increase difficulties in identify Personal Identifiable Information (PII)

Personal identifiable information (PII) is a legal concept to define “Personal Data”. In Hong Kong, only data that can be classified as “personal data” will be protected by law. Nowadays, PII becomes harder to define and identify as the absence of PII does not mean that the remaining data does not identify individuals. Some attributes may be able to identify an individual on their own. However, some attributes in combination with others with modern re-identification technologies are also able to identify an individual. Cookies and Internet Protocol Address (IP Address) are some of the examples of possible hidden PII nowadays.

- Extensive cross-border data movement

Data travel silently across international boundaries nowadays. It is also common for private corporations to gather data in one place, store and analyze data at the other country. It is harder to identify and regulate non-compliance cases.

- Privatised and decentralised data storage

it is also to point out that data storage become privatized and decentralised with the pro-market and pro-privatisation strategy in neo-liberal economic order in Hong Kong. In the past, data storage was relatively centralised in government bodies. However, privatization has been increased after 1997 as suggested by Yun Chung CHEN, Ngai PUN in Neoliberalization and Privatization in Hong Kong after the 1997

Financial Crisis in 2007[13], a number of public utilities such as MTR and public housing assets Links Management etc. have been privatized in the last decade. Massive amount of personal data is now sitting in a decentralised way at different private organisations at different part of the world. That increases the difficulties in data storage management.

- High processing power but affordable technologies

Finally, surveillance becomes ubiquitous with the increase of processing power technologies available and affordable in the market.

Effectiveness of privacy protection in a technology-mediated society

International & Local Privacy Legislation

Before jumping into the case, it is to briefly introduce the right to privacy and the related international and local legislations.

- **International Privacy Laws**

Right to privacy originally cover physical property protection of an individual only. Later, the right incorporated in the legal systems broadened as a civil liberty to safeguarding the privacy of individuals as what Brandeis's suggested "right to be let alone" in 1890[14]. Nowadays, the term right to privacy refers to both tangible properties and intangible aspects such as feeling and intellect.

Privacy is a fundamental human rights recognised in the UN Declaration of Human Rights in 1945, the International covenant on Civil and Political Rights (ICCPR) in 1976.

In Universal Declaration of Human Rights, Article 12 states[15]:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.*

Everyone has the right to the protection of the law against such interference or attacks.

In ICCPR, Article 17 states[16]:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

2. *Everyone has the right to the protection of the law against such interference or attacks.*

This section will focus on the discussion of the effectiveness of privacy protection from civil and political perspective although some scholars such as Habermas have reframed social and economic rights as basic guarantors of individual autonomy. On the other hand, this view has been constantly opposed by some other scholars or the United States in particular, as this view is seen to conflict with the notions of personal autonomy and freedom by taking away a person's property with no consent. This gives us a wider perspective in considering the protection of individual autonomy. This also reminds us that any state actions to protect the autonomy of some will inevitably impact the autonomy of others.

Interest in the right to privacy increased since 1970s with the introduction of information technology in Europe. The surveillance power of computer systems prompted demands for specific regulations governing collection, handling and use of personal data. The first data protection law in the world was enacted in Hesse in Germany in 1970s[17].

- **Hong Kong Privacy law**

Hong Kong SAR has signed and ratified ICCPR since 1991 with the passage's of the Hong Kong Bills of Rights. The right to privacy is protected by Article 30[18] of the Basic Law and Article 14 of the Bill of Rights[19] in Hong Kong. However, People's Republic of

China has only signed ICCPR in 1998 but not yet ratified. In Basic Law of Hong Kong SAR, article 30 states:

> *The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.*

In Bills of Rights of Hong Kong, article 14 states:

> *Protection of privacy, family, home, correspondence, honour and reputation*
> *(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
> *(2) Everyone has the right to the protection of the law against such interference or attacks.*

The Personal Data (Privacy) Ordinance in Hong Kong

The Hong Kong legislation controls personal information collected and held by both public and private bodies and applies to automated and non-automated data. The regulatory model adopted by Hong Kong is through a public official known as Commissioner who is responsible to monitor compliance with the laws and conduct investigation, public education and international liaison in data protection and data transfer.

The ordinance specifies six data protection principles below which must be adhered to when dealing with personal data.

> Principle 1: purpose and manner of collection of personal data
> Principle 2: accuracy and duration of retention of personal data

Principle 3: use of personal data

Principle 4: security of personal data

Principle 5: information to be generally available

Principle 6: access to personal data

Privacy in Hong Kong - Yahoo! Shitao Case Study

A case study approach was chosen to review and discuss the effectiveness of the privacy laws in Hong Kong in the first part of the study. Yahoo! Shitao case in 2005 was selected to be scrutinized in this paper as this case touches on a number of controversial privacy issues uniquely to this digital era such as definition of "personal data" in digital realm and cross-border data transfer etc. The section is to discuss and unfold the unprecedented challenges posed to privacy protection and the ambiguity of the local legal legislations under the development information and communication technologies in an information society.

The Personal Data (Privacy) Ordinance[20] in Hong Kong and The Interception of Communications and Surveillance Ordinance[21] are the 2 legislations involved in the discussion. The key focuses of this section will focus on the areas below:

1. Definition of personally-identifiable data
2. Prescribed Consent for new purpose of data usage
3. Extra-territorial Law enforcement
4. E-mail Surveillance in the name of crime detection

- **Case Background**

Yahoo! is one of the leading corporations founded in the digital era providing extensive services internationally riding on a virtual online platform crossing terrestrial and national borders. Yahoo! HK is a subsidiary of Yahoo! registered in

Hong Kong providing services to the people both in Hong Kong and Mainland China at the time the case concern below. The case[22] is about an appellant appealed to the administrative Appeal Board, contending the commissioner erred in law in concluding that Yahoo! Hong Kong has not violated the Ordinance in furnishing account holder information to the Mainland Authorities.

In 2005, a journalist called Shitao employed by Hunan's Contemporary Business News in Mainland China, was convicted of the crime of illegally providing state secrets to foreign entities outside the People's Republic of China (PRC) and was sentenced to 10 years' imprisonment. The "state secret" document was sent out from Communist Party authorities in Apr 2004 recommending media members not to report on the upcoming fifteenth anniversary of the "June 4th Tiananmen Incident" and also media to correctly direct public opinion and not to release any opinions that are inconsistent with central policies. Tiananmen Incident on June 4th 1989 were a student-led demonstrations in Beijing in 1989 received broad support from city residents. The protests were forcibly suppressed by leaders who ordered the military to enforce martial law. The crackdown that initiated on June 3 to 4 became known as the Tiananmen Square Massacre. The journalist used his personal Yahoo! email account (huoyan-1989@yahoo.com.cn) in his office to send an anonymous post attached with the document to one of the founders of the "Asia Democracy Foundation" located in New York, USA and editor-in-chief of the foreign web site "Democracy Forum" and the electronic publication "Democracy News." afterwards.

In the Verdict from the China court, it stated that Yahoo! Beijing office had provided the State Security Bureau of Mainland China (SSB)'s user registration information including business address and contact number, Internet Protocol (IP) address, log-in information such as time and date and certain email contents. As Yahoo! China website is owned by Yahoo! Hong Kong at the material time. Privacy Commissioner of Personal Data Hong Kong received complaints and carried out investigation. After hearing, Members of Administrative Appeal Board held unanimously and confirmed to dismiss the appeal on November 2007. The conclusion is mainly based on the

argument that the IP address of an internet account holder was not constituted as personal data within the meaning of the Personal Data (Privacy) Ordinance (Cap 486).

- **Definition of Personally-identifiable data?**

Although the information released by Yahoo! HK had undoubtedly led to the revelation of the journalist's identity, and assist the China Authorities to identify the individual. However, these information were not constituted as “Personal Data” according to the current definition in the Ordinance as stated above. If data is not regard as personal data, it is by no means caught by the law. The definition of the “Personal Data” is the key piece of law to refer to here.

In section 2 of the Personal Data (Privacy) Ordinance states that "personal data" means any data

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable

According to the arguments by the Commissioner, an IP address on its own is not a personal data because it refers to a computer but not an individual. It cannot reveal the exact location of the individual. Even, IP address combined with the user information including the business address and telephone number provided by Yahoo!, it is also not constituted as a personal data since the Commissioner argued there is no evidence to show the user registration information are real or belong to a living individual as no verification has been made before by the company. As a result, it is believed by the Commissioner that the information provided by Yahoo! IP address and user registration information only disclosed that the email was sent from a computer located at the address of a business entity, and the date and time of the transaction. Without additional evidence such as CCTV, it would not be

reasonably practicable to ascertain it was the appellant who used the computer identified by the IP address to send out the relevant email at the material time.

To address the challenge to define PII (or "Personal Data" mentioned in this case) from the perspective of privacy protection, new thinking that should be injected in the legal framework. Instead of just discussing whether the data provided by Yahoo! is practicable to identify an individual or not after sharing the information, it is suggested to look into the issue from an opposite view. We should ask whether Yahoo! is able to differentiate and confirm if the data is going to be shared is definitely not practicable to ascertain any individual before they use. It is doubted if the company is able to make an accurate assessment in dealing with the data like IP address. If not, It is to argue the data such as IP Address should be included in the definition of "Personal data" by default to eliminate the ambiguity in evaluation and protect the data owners from violation of the Ordinance. It is also a measure to provide a better protection to the data subjects as well. Here below is to further explain the argument in details.

Although IP address on its own is not practicable to identify an individual. However, when it combines with other personal information, it is in many ways possible. According to an advice provided by an independent EU advisory body called the Article 29 Data Protection Working Party in 2010[23], it proposed that it is possible to identify an individual by linking the IP address with other personal information; especially with the support of the modern and powerful technologies for data collection and data mining nowadays. Besides, on 25 January 2012, the European Commission unveiled a draft legislative package to establish a unified European data protection law[24]; in which explicitly pointed out that any IP address should be treated as personal data.

In Yahoo! Shitao case above, there was no such discussion raised in the court or among media during and after the hearing. To address the challenges of data protection, law makers should have to understand the complexity of data which may incur ambiguity in law compliance. Legislations are required to address these

ambiguities in order to protect privacy of the data subject and also prevent the corporations from violating the law with uncertainty.

- **Prescribed Consent for new purpose of data usage**

This section is to point out that the prescribed consent on the new purposes of data usage (not consistent with the original purpose upon collection) in a form of Terms of Service (TOS) upon service subscription suggested by Yahoo! Hong Kong is not effective enough to protect the privacy of the data subject. This acceptance of TOS as a prescribed consent solution actually creates uncertainty to data subjects and also legitimizes monitoring activities and intrusion of individual autonomy.

In the Data Protection Principle 3 of the Ordinance, it clearly states that unless having a prescribed consent with the data subject, personal data shall only be used for a purpose consistent with the original purpose of collection. Prescribed consent can be understood as expressing consent given voluntarily.
In the Yahoo! Shitao case, the prescribed consent is one of the reasons for the Appeal Board to dismiss the appeal as it argued that the prescribed consent has been included in the TOS which stated that Yahoo! China might preserve and disclose a user's account information and content if required to do so by the local law.
As the appellant was accepted TOS upon subscription of the Yahoo! email service, the Appeal Broad then agreed that appellant has given consent voluntarily to Yahoo! China to share his personal information to the local authority if required by the local law.

However, it is to suggest that although the information was included in the TOS, it still should not be regard as a prescribed consent blindly without reviewing the presentation or delivery of those information to the data subject. Font size, colors, style of writing employed and amount of information included in the TOS can affect information understanding and comprehension. Although we cannot go back to the

time when the appellant subscribed the Yahoo! Service to study the design and delivery of TOS, it is to point out the common problems of TOS delivery by reviewing the online subscription flow of the Yahoo! HK mail nowadays[25]. Having reviewed the existing TOS of Yahoo! Hong Kong mail service, it just mentioned Yahoo! HK will not share the personal data to third party unless it is requested by the relevant authorities under the section 58 in the ordinance. It does not mentioned the personal information will be shared to the state explicitly. Such style of writing is not easy for the user to understand, and needless to say, to agree to provide consent to Yahoo! voluntarily. Besides, the TOS will updated from time to time, and Yahoo! will only posted in website, and this also create confusion to the data subject, and unfair to imply that they have provided a prescribed consent to the amendments.

- **Extra-territorial Law enforcement**

The case also raised public's concern on the absence of provisions in the Ordinance governing extra-territorial data protection. Section 33[26] in the Ordinance regarding "prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances" was enacted in 1995 but has not put into operation until now, even after the latest amendments in 2012. Although this is not the main reason for the dismissal of the appeal but it clearly creates a loophole in data protection in the information age.

It is not uncommon that a company collect customer's information in Kong Kong, with database server located in country B and data processing taken place in country C, and set up call centre services located in country D nowadays in globalisation and in neo-liberal economic order. A lot of telecommunication companies such as PCCW, they operate telecommunication business in Hong Kong, and set up call centers in southern China providing service to customer in Hong Kong. With the section 33 put in operation, it controls personal data transfer outside Hong Kong except complying with the requirements below. Data subjects can at least enjoy the minimal privacy protection with section 33.

- Where the Commissioner has reasonable grounds for believing that there is in force in a place outside Hong Kong any law which is substantially similar to, or serves the same purposes as, this Ordinance, he may, by notice in the Gazette, specify that place for the purposes of this section
- the user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, this Ordinance;
- the data subject has consented in writing to the transfer;

Data protection law nowadays cannot design only under the imagination of national border. It should also address the frequent trans-border data movement for better data and privacy protection for the citizens.

- **E-mail Surveillance in the name of Crime Detection**

When reviewing the Yahoo! Shitao case above, a question that has to be raised: whether China authority has consistently monitored e-mail contents of their citizens in Mainland China? If not, why the authority will request Yahoo! China to provide the specific account holder's information to them? Although the case happened in Mainland China, it is worth to ask if Hong Kong people, as China citizens in a Special Administrative Region (SAR), enjoy enough protection from e-mail surveillance with the Basic Law Section 30 and Bills of right Section 14? In this part, it is to discuss the effectiveness of laws in against HK government from exercising e-mail surveillance to the citizens.

The Interception of Communications and Surveillance Ordinance (ICSO) was passed in 2006 in Hong Kong. The direction of this ordinance is to balance the needs of public security or crime investigation, and freedoms and rights. Before 2006, communication interception or covert surveillance carried out by law enforcement officers had been largely unchecked. The Ordinance provides the basic protection by

specifying the adequate purposes, authorization procedures required and the departments allowed for carrying out communication interception or covert surveillance. Only 4 departments namely Hong Kong Police Force, Independent Commission Against Corruption (ICAC), Customs and Excise Department and Immigration Department are allowed to carry out communication interception or covert surveillance if with prescribed authorization for the purpose of preventing or detecting serious crime or protecting public security.

The number of cases on communication interception and covert surveillance has decreased significantly since the implementation of the Ordinance as claimed by the Commissioner. However, according to the commissioner's annual report in 2010[27], Mr Justice Woo Kwok-hing stated that "the commission exists in name only" as the punishments were too soft even for some serious non-compliance cases which cannot create a deterrent effect to the parties involved. Besides, the goal keeping practice is also not effective enough as the Commissioner has no power to listen to audio intercept in investigating the potential non-compliance. In the annual report 2008[28], he also criticized that some law enforcement officers were dishonest and unwilling to cooperate, behaved in an arrogant and disobeyed orders by deleting relevant recordings of covert surveillance. The departments involved have not responded to the accusations made by the Commissioner after the report issued. Although the government has expressed that they will consider the Commissioner's suggestions to study the possibilities to increase the Commissioner's power in case investigation, but there is no further follow up from the government after that. It seems that although there is a law in place to protect us from being monitored, but it is not effectively enforced.

In this section, it is clearly show that privacy laws nowadays are unable to address the challenges that posed in information age in privacy protection especially in the areas that we have highlighted through studying the Yahoo! Shitao case. Although, The Personal Data (Privacy) Ordinance in Hong Kong has been updated in 2012, the issue of IP address and extra-territorial law enforcement discussed above that still

have not been addressed. It is to point out that the ambiguity of legal legislation actually authorizes and legalise surveillance practices in the society. On the other hand, the European Commission has unveiled a draft legislative package to establish a unified European data protection law on January 2012 which show determine to face and address the unprecedented challenges to privacy protection nowadays.

Governmentality of technologies & Surveillance

Development of technologies and surveillance

Furthermore, this study also aims to examine privacy intrusion and surveillance by introducing a cultural studies perspective. Michel Foucault's concept of governmentality is employed as a framework to understand the development of surveillance from the 18th century to the information age nowadays. It is to provide an alternative account on technologies and surveillance, and normalisation of surveillance under a neo-liberal framework so as to cover a comprehensive discussion on privacy in Hong Kong.

Governmentality is a concept first developed by Michel Foucault in the 70s. In his lectures at the Collège de France, he defines governmentality as the "art of government" in a wide sense. This suggested "government" is not only limited to state politics, but also includes a wide range of control techniques or technologies applied to a wide variety of objects, which is particularly linked to the concept of self-control and power-knowledge[29].

According to Michell Dean's words, "Governmentality: How we think about governing others and ourselves in a wide variety of contexts..."[30] (Mitchell Dean, 1999). This raises an interesting point that those who are governed may not understand the unnaturalness of both the way they live and may also take this way of life for granted. Thus, to analyze government, apart from looking into the political structure, is to analyse the mechanisms that try to shape, sculpt, mobilise and work

through the choices, desires, aspirations, needs, wants and lifestyles of individuals and groups

- ***New form of surveillance in the 18th Century - Panopticon***

Panopticon was a prison building designed in the 18th Century by a philosopher called Jeremy Bentham. In this design & construction technology, all the "cells" were built around a tall central tower; which facilitates a total surveillance with very little cost in terms of money or manpower as anyone standing at the top of the tower is able to see all the cells outside the windows. As Foucault pointed out in Discipline & Punish[31], Panopticon enforced discipline not by constant presence of a guard but by the simple fact that prisoners know that they may be observed at any moment. The prisoners exercised self-control finally. The surveillance becomes "permanent in effects, even if it is discontinuous in its action…" (G Sewell, B Wilkinson 1992) [32]

- ***Migrated the Panopticon concept to modern surveillance society***

As Foucault suggested, the 18th century prison system was migrated into the modern surveillance for social control of the population. The exercise of power is dispersed rather than centralised in one authority and achieves effective control by using technologies and practices. Other than top down control, we also police our own behaviour due to external "gazing" by others or even without intervention from outside.

According to Mitchell Dean's, he connects "technologies of power"[33] to the concept of governmentality to explain the self-governing behaviour of individual in a surveillance society. Technology of power is those "technologies imbued with aspirations for the shaping of conduct in the hope of producing certain desired effects and averting certain undesired ones" (Rose, 1999)[34]. Foucault defined technologies of the self as techniques that allow individuals to exercise on their own bodies, minds, souls, and lifestyle, so as to attain a certain state of happiness, and quality of life[35]. Such continuous self-monitoring activities inside a body with an

objective to shape citizens' behaviour are actually a kind of self-surveillance in modern state.

Another concept of self-governing is gazing that proposed by Foucault. In his Discipline & Punish, gaze is to illustrate a particular dynamic in power relations and disciplinary mechanisms. In his Discipline & Punish, gaze is one of the concepts to explain self-regulation under systems of surveillance as suggested in Panopticon. This refers to how people modify their behaviour under the belief that they are constantly being watched even if they cannot directly see who or what is watching them. This possible surveillance, whether real or unreal, continuous or interrupted, has self-regulating effects. CCTV is a good example to illustrate the gazing effect. Surveillance of the public using CCTV is particularly common in many areas around the world. It is a video tracking device in public or private areas such as banks, casinos, airports, in the name of security for crime detection, property protection etc. People police their own behaviour and social interaction in front of CCTVs with a brief that they are constantly being gazed even though it is off.

As Foucault suggested, statistic is a kind of technology that the state employed to gather citizens' information to build a database and exert control in a way to reinforce gaze, surveillance and nomination[36]. We actually internalize the rules that limit our conduct and social interaction. As in the original panopticon building, even in absence of direct surveillance, we examine ourselves and monitor our actions for any taint of "abnormality". In Foucault's view, a perpetual victory avoiding physical confrontation is decided in advanced.

- ***Ubiquitous Surveillance in informational society in the 21 Century***

In contemporary culture, new technologies enable ubiquitous surveillance in the 21st Century under neo-liberal capitalism as discussed in the beginning. Surveillance practices expand its scopes in terms of intensity and capacity. Data surveillance emerged as a new form of surveillance practice; which further escalates social control to the individuals in the society. William Staples suggested "It is no longer considered efficient and effective to simply gaze at the body – or train it in hopes of

rendering it docile – rather, we must surveil its inner evidence and secrets" (Shelley Feldman, 2011)[37]. This opens a new dimension in social control shifting surveillance society by simply gazing to ubiquitous surveillances monitoring inner secrets of the population.

Data surveillance can monitor individual's secrets by actively collecting personal data, analysing and mining to develop a profile for each individual. The profile is possible to describe a person demographically such as age, sex, occupation, income range, education level etc. Besides, it can also describe your taste, habit, work and leisure schedule by analysing shopping or dining transactions, frequently visit locations (such as Octopus or Mobile GPRS) etc. The most powerful of data mining technologies is to understand individual's psychological state or secrets by running semantic analysis on posts tweeted or posted at social media sites, by understanding the web surfing behaviour through studying cookies stored in your computer. These data may be stored at different companies, but it is possible to map those separately stored information by a unique identifier such as HKID, e-mail address etc. to enrich into 1 profile. With such a powerful profile, public or private body are able to manipulate individual's behaviour and thinking precisely, effectively and efficiently.

From the discussion above on the development of surveillance form 18th to 21st century, technologies are actually underpinned by mentality of government that seeks to shape our behavior and mind and to transform a citizen into an individual that fit political objectives. Nowadays, in the information age, apart from top down power and gaze, new technologies enable ubiquitous surveillance can shape our behaviour and mind through monitoring individual's secrets by actively collecting personal data, analysing and mining to develop a profile for each individual.

Normalisation of Ubiquitous Surveillance

According to Shelley Feldman's Surveillance and Securitization[38] – the new politics of social reproduction, ubiquitous surveillance is operated in the name of security.

Normalisation of surveillance practices was enforced by multiple actors in different fields from both public and private. One of the common discourses of surveillance is security which is operated by manipulating fear in areas of death, loss of property, job security and reputation etc. This becomes even more obvious after 911 Incident as fear of death is invocated. This makes strengthen control and surveillance justified in the name of public security. On the other hand, in Feldman's view, under the neo-liberal rule of promoting privatisation and individual responsibility but retreating from social welfare, "fear is normalised in ways that make opposition difficult. (Shelley Feldman, 2012)".

Conclusion

Under the rapid growth technological innovations since the 80s such as internet and e-mail communication under a neo-liberal economic order, people in Hong Kong nowadays become highly technology-mediated in their daily lives across different disciplines including political, economic and cultural activities. This poses new challenges to privacy protection as vast amount of personal data are being generated by the individuals in every interactions with technologies and being collected by both public and private sectors with political or economic motivation. However, Facebook founder, Mark Zuckerberg, claimed "privacy is dead" and described it as an obsolete social norm in this context. To respond to Mark's claim, this paper reinstated the importance of privacy protection by associating privacy with individual autonomy and the construction of personal identity. Apart from protecting personal data from sharing publicly without consent or "the right to be let alone" (Warren & Brandeis, 1890)[39], In Jurgen Habermas and Beate Roessler's view, the importance of privacy protection also enables a person to construct his or her own identity by preventing the manipulation of desire. To protect individual's autonomy, the significance of privacy should be reinstated and reiterated in the community.

Through scrutinizing the Yahoo! Shitao case, it clearly showed that privacy laws nowadays in Hong Kong are unable to address the challenges posed on privacy protection in a technology-mediated society. Definition of "Personal Data", cross-border data movement and privacy protection on covert surveillance or communication interception by the government are some of the controversial issues that are unable to be handled in the current laws as reflected in this case. The ambiguity of legal legislation actually authorizes and legalise surveillance practices in the society.

Surveillance becomes decentralised and ubiquitous with the development of technological innovations in neo-liberal economic order. To examine privacy intrusion and surveillance from a cultural studies perspective by using the conceptual framework suggested by Michel Foucault, technologies are actually underpinned by mentality of government that seeks to shape our behavior and mind and to transform a citizen into an individual that fit political objectives. Surveillance nowadays is not only riding on a top down power or gaze, it is actually through surveilling individuals' inner secret to attain higher efficiency and effectiveness of social control and manipulate autonomy. According to Shelley Feldman, the normalisation of ubiquitous surveillance is operated in the name of security. In her view, under the neo-liberal rule of promoting privatisation and individual responsibility but retreating from social welfare, "fear is normalised in ways that make opposition difficult. Perhaps, surveillance in the name of security is a part of the political project to legitimate the suspension of law and right in privacy protection.

[1] Privacy no longer a social norm, says Facebook founder, Guardian.co.uk, Jan 2010, retrieved on Dec 21 2012: http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

[2] Jurgen Habermas, Structural transformation of the public sphere, Polity press, 1994

[3] Beate Roessler, The value of privacy, Polity Press, 2004

[4] Warren and Brandeis, "The Right To Privacy", 4 Harvard Law Review 193, 1890

[5] Data from Census and Statistics Department in Hong Kong; retrieved in 19 Dec 2012

[6] Manuel Castells, The rise of the network society, Malden, MA: Blackwell, 1996

[7] Stuart Hall, "Brave New World", Marxism Today, October 1988

[8] D. Zwick, N. Dholakia / Information and Organization 14 (2004) 211–236

[9] HKDMA (2012, December 15). Retrieved on 19 Dec2012 from http://www.hkdma.com/industry.html

[10] A Report on the Surveillance Society: Public Discussion Document, by the Surveillance Studies Network, 2006

[11] Roger Clarke, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, 2006, Retrieved from http://www.cse.unsw.edu.au/~cs4920/seminars/resources/Roger-Clarke-Intro.pdf

[12] YVES POULLET AND J. MARC DINANT, The internet and private life in Europe: Risks and aspirations, New dimensions in privacy law, Cambridge University Press, 2006

[13] Yun Chung CHEN, Ngai PUN, Neoliberalization and Privatization in Hong Kong after the 1997 Financial Crisis, 2007

[14] Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy; Bratman, Benjamin E., 2001-2002

[15] The Universal Declaration of Human Rights, retrieved from United Nations Website on 12 Dec 2012: http://www.un.org/en/documents/udhr/

[16] International Covenant on Civil and Political Rights, retrieved from United Nations Website on 12 Dec 2012: http://www2.ohchr.org/english/law/ccpr.htm

[17] Fred H. Cate , The EU Data Protection Directive, Information Privacy, and the Public Interest, 1995

[18] Basic Law of the Hong Kong Special Administrative Region; retrieved on 20 Dec 2012: http://www.basiclaw.gov.hk/en/basiclawtext/chapter_3.html

[19] Hong Kong Bills of Rights Ordinance , retrieved on 20 Dec 2012: http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/AE5E078A7CF8E845482575EE007916D8?OpenDocument&bt=0

[20] The Personal Data (Privacy) Ordinance, retrieved on 20 Dec 2012: http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf

[21] The Interception of Communications and Surveillance Ordinance, retrieved on 20 Dec 2012, http://www.legislation.gov.hk/blis_ind.nsf/CURALLENGDOC/D56C9DF36754402E482571DF0015701A?OpenDocument

[22] Shi Tao v Privacy Commissioner for Personal Data, 26 November 2007, LexisNexis Asia 2008

[23] an independent European advisory body on data protection and privacy “Article 29 Data Protection Working Party”, Opinion 2/2010 on online behavioural advertising, 2010, retrieved on 20 Dec 2012: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[24] European Commission, Commission proposes a comprehensive reform of the data protection rules, 2012, retrieved on 20 Dec 2012: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[25] Terms of Service (TOS) of Yahoo! Mail Service Hong Kong, retrieved 19 Dec 2012: http://info.yahoo.com/privacy/hk/yahoo/mail/

[26] Section 33, The Personal Data (Privacy) Ordinance, retrieved on 20 Dec 2012: http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf

[27] The Commissioner of Communication Interception and Covert Surveillance annual report in 2010, retrieved on 20 Dec 2012: http://www.info.gov.hk/info/sciocs/eng/pdf/Annual_Report_2010_Summary.pdf

[28] The Commissioner of Communication Interception and Covert Surveillance annual report in 2008, retrieved on 20 Dec 2012: http://www.info.gov.hk/info/sciocs/eng/images/Annual_Report_2008_Summary.pdf

[29] Thomas Lemke, Foucault, Governmentality, and Critique, Rethinking Marxism, Vol. 14, Iss. 3, 2002

[30] Dean, M., Governmentality: Power and Rule in Modern Society. London: Sage, 1999

[31] Michel Foucault, Discipline & Punish: The Birth of the Prison, Vintage; 2nd Edition edition, April 1995

[32] G Sewell, B Wilkinson, Someone to Watch Over Me: Surveillance, Discipline and the Just-in-Time Labour Process, Sage, 1992

[33] Lemke.T, The birth of bio-politics: Michael Foucault's lectures at the College de France on neo-liberal governmentality' in Economy and Society v.30, 2001

[34] Rose, N. , Powers of Freedom: reframing political thought. Cambridge: Cambridge University Press, 1999

[35] Michel Foucault, The Subject and Power, Critical Inquiry , Vol. 8, No. 4 (Summer, 1982), pp. 777-795

[36] Rodney Fopp1, Surveillance & Society, Increasing the Potential for Gaze, Surveillance and Normalisation: the transformation of an Australian policy for people who are homeless, 2002, retrieved on 20 Dec 2012: http://www.surveillance-and-society.org/articles1/homeless.pdf

[37] Shelley Feldman, Surveillance and Securitization The New Politics of Social Reproduction, Accumulating Insecurity: Violence and Dispossession in the Making of Everyday Life, University of Georgia Press, 2011

[38] Shelley Feldman, Surveillance and Securitization The New Politics of Social Reproduction, Accumulating Insecurity: Violence and Dispossession in the Making of Everyday Life, University of Georgia Press, 2011

[39] Warren and Brandeis, "The Right To Privacy", 4 Harvard Law Review 193, 1890