Addressing Biometrics Security and Privacy Related Challenges in China

Sum Yu Mok, Ajay Kumar
Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong SAR China
Email: *09165671d@polyu.edu.hk*, *ajaykr@ieee.org*

***Abstract*:** There has been significant advancement improvement in the capabilities of biometrics and data protection technologies in last decade. The significant reduction in cost, improvements in speed and accuracy has resulted in increased deployment of such technologies in day-to-day business and public utilities. The increasing use of biometrics and data protection technologies has also raised concern on the unethical use of personal information. There are increasing number of incidents and concerns in the public over the infringement of personal privacy in China. This paper has investigated such emerging privacy related concerns in the deployment of biometrics and data protection technologies in China. This paper also includes a study on public attitudes toward such technologies and attempts to make comparison with the same in the difference with such emerging concerns in other developed countries. This paper has developed an online survey to ascertain people's understanding on the various aspects of privacy and thus willingness to trade-off with the benefits of increased security. The online survey was conducted in February – March 2012 and revealed great deal of information from the 305 Hong Kong people. We have attempted to analyse the survey results which illustrate interesting findings on the use of CCTV, biometrics technologies, social networking, disclosure of personal information and recent (2012) privacy policy adjustments in popular websites.

I. Introduction

THE use of biometrics and social networking technologies has significantly increased over last few years and have raised high concerns in the unwanted disclosure of personal privacy. For example, recent news summary titled "*Free apps 'can spy on texts and calls'*: *Smartphone users warned of privacy dangers*" published in February 2012 [1], discloses how Facebook and Flicker tracked/accessed our contact book list and day-to-day messages. Some commercial firms and e-business entities share or sell associated personal identities and pose risks which are not known to the large section of population. At the same time, there is always some tradeoff between the available privacy and security offered from the emerging biometrics technologies. Such tradeoff need to be carefully studied and included in the policy formulation for the regulation of new technologies. This can ensure that citizens can benefit from the technological advancements while ensuring reasonable privacy tradeoff for the increased convenience or security.

The dual use of biometrics technologies for any possible medical diagnosis need to be carefully regulated as such use can generate huge privacy concerns. The hospitals typically maintain huge database systems with numerous patients' personal confidential data residing inside which often include their medical records and blood type. Such vital information is potentially attractive in the underground servers as they can have large commercial/marketing applications. Besides, some tricksters can possibly make use of such dual use information contents for fraud or to cheat for money.

The notion of personal privacy varies from culture to culture and this could be the plausible reason for varying privacy protection policies among different geopolitical regions. Recent survey [3] in China suggests that 88.8% of the population have encountered the problems relating to the personal information disclosure, especially with the mobile phone number, and 83.2% of them feel that the government should try to establish laws to protect personal phone number privacy of residents. This suggests that policy makers in China are yet to be successful in enforcing a specialized law that can protect residents from increasing incidents of privacy infringements which are now more frequently reported/shared using popular social networking technologies. Our survey in this area suggests lack of any systematic study, at least in public domain, that could compare challenges to the current privacy protection regulations/practices in China with those in other developed countries. On the other hand, there has been significant advancement in the development/deployment of biometrics and social networking technologies in China [18], [21], *i.e.*, from the largest CCTV network in Beijing to the use of biometrics technologies at automated border crossings in China.

A. *Our Work*

Emerging deployment of biometrics and social networking technologies has posed new policy related challenges among the stakeholders. In this context, there have been number of related studies [2], [27] and efforts to develop new policies from the emerging technological challenges, one such example is the new EU framework on privacy and data protection [28]. However there is lack of such studies that could focus on public attitudes and social concerns on the deployment of emerging technologies in China. Therefore the key objective of this paper is to study such emerging challenges in China to ascertain differences and similarities with other developed countries. Our study is largely based on the survey conducted in China on 305 Hong Kong residents between February – April 2012. This study reveals new insights on the emerging public attitude towards biometrics, CCTV deployments and importantly the extent of tradeoff for needed privacy for a better security. Finally, trends and emerging views on privacy, biometrics security and preferences/selection of modalities are presented from the survey result analysis.

II. EMERGING PRIVACY RELATED CHALLENGES

A. *Privacy Related Laws and Biometrics usage in China*

Privacy

China has largest population of internet users[†] and very strong social media usage which outnumber Americans by a ratio of 3-to-1. However, the regulatory guidelines in China have not yet matured and there is need to provide more comprehensive laws that can protect residents in China with emerging technologies and dual use of biometrics related information. In this context, the well-known regulatory guidelines have evolved from the Constitution of the People's Republic of China ("PRC Constitution"), article 38 about oneself free from defamation and article 40 which is about one's freedom of communications and privacy of communication [5]. In this context, a new privacy regulation by the Ministry of Industry and Information Technology of the People's Republic of China has been recently enacted (15 March 2012). This regulation entitled *Several Provisions on Regulation of the Order of Internet Information Service Market*, is probably first national level regulation that use the definition of *user personal information* [22]. This "user personal information" will include biometrics information as it is defined as the information relevant to the users that can ascertain the identity of the users. This new regulation is expected to provide stronger protection for the collection/use of sensitive biometrics data.

It is widely believed that US, on the contrary, have more comprehensive legislations on protecting the sensitive personal information relating to the citizens. In this context, there are four categories of privacy invasion that are included in the Modern Tort law: Intrusion of solitude, Public disclosure of private facts, False light and Appropriation. These laws are more *systematic* and effective. Besides, these laws have quite matured to address range of popular social practices such as personal security, business privacy, children's privacy and security, security cameras, collection of personal information on hospital and government [6].

In addition to the development of regulations and policies, an effective industry oriented self-regulatory mechanism that can also strengthen the international data sharing/exchange is necessary to benefit from the emerging biometrics technologies for public good.

Biometrics usage

Various historical accounts suggest that the use of fingerprints in China began during the third century B. C. as a testament on the official documents [23]. The large scale development and deployment of biometrics technologies in post 9/11 USA has also raised concerns on individual privacy. In this context, the emerging challenges in China are quite similar but at slower pace facing the same question: how to strike a balance between the security and privacy effectively and efficiently? Such challenges can be possibly met with the development of novel technologies than can ensure such balance and ensuring that privacy is a mandatory element in the design of emerging technologies.

With respect to the above case, the following questions were included in our survey:

- Nowadays biometrics technology has been used on many areas, but some people cannot accept all the biometrics access control, please rate your acceptance level for the following cases; (see [30])
- If you are suggested to use your biometrics information, under which situation or the area where you feel acceptable?

The objective of above question(s) was to (i) ascertain the acceptance of using biometrics in different areas; (ii) provide some background to the respondents on the use of biometrics technologies.

B. *Recent Concerns on Privacy Related Issue*

1) *Sina Weibo Privacy Concern*

Sina Weibo is a famous and popular blogging website, besides the Facebook and Twitter, in China. It is in use by well over 30% of internet users. However, this blogging website/system has reportedly failed to protect users' personal information and is easily shared with others [9]. Other users can read your blogging by "being your fan". Then they can see your email address and QQ number in your info page or even know where you live and work by reading your blogging details and photos, because they can also determine/identify your place by looking at the photos' background. Some people will make use of your uploaded photo for some unethical use. Please refer to [9] for details on some real cases. Social networking technologies are increasingly occupying special role and privileges in our day-to-day life. However, these technologies and applications need to educate the uses of potential risks. The incident highlighted in this study/section suggests failure to include *privacy-by-design* (fail safe) element in the emerging social media and networking technologies.

2) *Privacy Challenge from the use of QR code*

The QR code is essentially a 2D bar code and it can store lot of information. This information can however be easily be read by popular software or mobile phone applications which can decode such 2D bar code from the images acquired using (embedded) camera.

Residents in China travel in mass around the national day holidays, mostly using railroads/trains. In such train tickets, as reproduced from a sample in figure 12, at the right bottom corner of the train ticket, there is a QR code. Once a person picks up the ticket and scans for the QR code through some mobile phone applications, he/she will know the ticket owners' ticket number, train leaving time and ID card number [10]. This problem has been widely reported and can be attributed to the limitations of deployed technology.

[†] According to recent *Netpop Research* [21] study, China has 411 million broadband users above 13+ years while 169 million in USA.

3) *Taxi Cab Recorders Bring New Privacy Concerns*

Recently, 6000 taxies in Nanjing (China) deployed video cameras and sound recorders inside the passenger taxis. The recorders will run in every second and the cameras can to take eight pictures per minute. They will be sent to the police database system through the GPS system. The cameras and recorders originally designed as a safety measure to protect the taxi driver on work and also ensure rights of passengers during/after travel [11]. However, such deployment has raised wide awareness and concerns relating to the personal privacy of the general public.

With such widely discussed privacy implications in our mind, we included following questions in our survey:

- Installing security cameras (CCTV) is now very common in the world, what is your level of acceptance for the following cases? (Airport, banks, Taxi, School/workplace apartment's water/electricity supply system area, Area of investigation for the acid attacks in *Mong Kok* [34], Traffic Red light intersections);
- Do you feel any uncomfortable or infringing your privacy when you are under monitoring by security cameras?
- Do you feel more secure with the security camera(s) monitoring?
- After reading the news, what do you think about the number of security cameras in Hong Kong?

The aims of the above questions was to ascertain (i) the level of acceptance in installing cameras in different areas; (ii) general feelings: whether more secure or uncomfortable under the monitor or cameras; (iii) change in priority for widely reported acid-attack incident investigations.

Table 1: Recent Incidents of Privacy Challenges in China.

Technology Deployment	Reference	Benefit	Concerns
Biometric fingerprint time and attendance system	[8]	Verification	Biometrics information protection
Social Media	[9]	Entertainment, Commutation	Personal Privacy
QR Code	[10]	Save data	Leakage of privacy and information
CCTV inside taxi	[11]	Security monitoring	Privacy Right

III. SURVEY

A. *Introduction*

The second part of this paper is focused on acquiring the primary source of data by conducting an online survey. The deployment of advanced technologies does bring benefits to us in daily life for example shortens the people-to-people distance, better security control and new kinds of entertainment. However, they also generate privacy concerns and it is necessary to ascertain them so that they can be addressed in the design and policy formulation. Therefore questions like – How much concerns people in general have on sharing their personal information? What are their concerns for tradeoff on sharing sensitive biometrics data/privacy to avail better security? Therefore there was a need to firstly design a *user friendly survey* that can effectively acquire such data and help us to ascertain the public attitude towards emerging technologies. This survey result will be helpful in answering such questions.

B. *Survey Design*

There were total of 18 questions in the survey and four social issues were included in the questions: Deployment of security cameras and the biometrics technologies, Social networking service website, and Google's new privacy policy. The respondents' background information is also acquired with respect to their age, gender and education level.

The key motivation in the design of this survey is to ensure user friendliness and ease in the acquisition of information. Some related and recent news was extracted from the web and a YouTube video was also included in the questions for two purposes: One is to make use of the characteristic of online survey, try to add some multimedia element to enrich the survey questions from traditional boring words. Another purpose is to provide background information to the respondents in case they do not remember or suffer from lack of knowledge on specific topic in the survey.

The survey aimed to find out people's behavior between the privacy and security in different cases. For easier analysis, some of the answers are group together for example "1" and "2", and "4" and "5" as two groups respectively.

We also attempted to prevent redundant answers from the same respondent and the respondents' IP addresses were automatically acquired when they submit the survey. This information is used to check integrity, *e.g.*, if same answers are found from the same IP address, only one record was kept in our database.

We developed [30] a specialized PHP based user interface (figure 11) and the questions layout was customized as per our observations and some additional multimedia element such as YouTube are added in between the questions. Since the mother language of each respondent can be different, both Chinese and English versions are set in the survey. The data generated from the survey is saved and managed by MySQL.

C. *Survey Respondents*

The total number of respondents took part in the survey is 305 and all the respondents are Hong Kong residents. The percentage of female and male are evenly distributed as ~50% (153 Males). Here is table of their age and education level:

Table 2: Age distribution of respondents.

Age	Number	Percentage (%)
Under 16	5	2
16-22	177	58
23-30	88	29
31-40	11	4
41-50	15	5
Above 50	9	3
Total	305	100

Table 3: Education level distribution of respondents.

Education Level	Number	Percentage (%)
Primary or lower	1	0
Secondary	24	8
Post-secondary	33	11
University degree or above	247	81
Total	305	100

IV. Survey Findings and Analysis

1) *People prefer to increase the number of CCTV in HK*

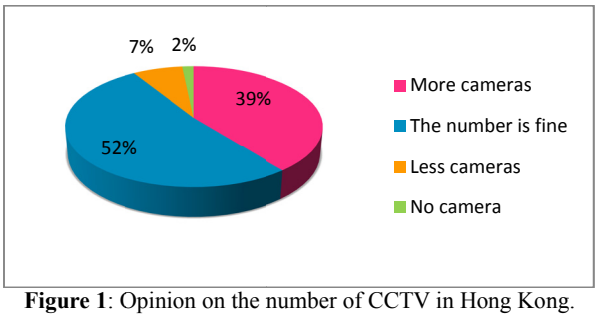

Figure 1: Opinion on the number of CCTV in Hong Kong.

This trend in favor of CCTV is an important feedback in that this may help to improve our city facilities planning in determining and designing the number of cameras in the public places. Half of the respondents think that the number is sufficient while about 40% of the respondents think that more cameras should be installed.

2) *Privacy tradeoff for increased security at workplaces*

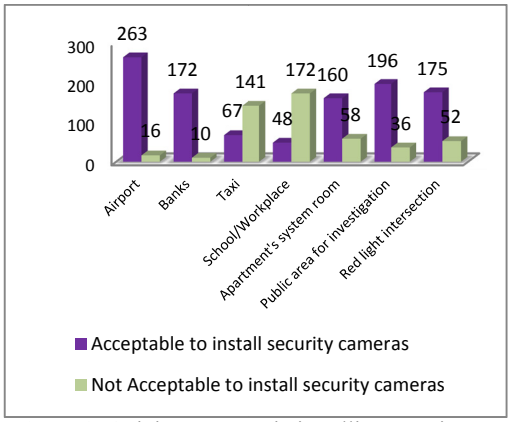

Figure 2: Opinion on areas in installing security cameras.

Most of the respondents agree to have cameras equipped in banks and airport. About 65% of them chose accept to have cameras especially in the case of the cameras installation for investigation, for example recent acid attacks in Mong Kok [34]. Yet, the result also shows the antipathy on cameras installation in taxi and school/workplace. The trends clearly suggest that most people treat these two areas are quite private. Higher rejection in schools (as compared to Taxi's) could possibly due to the fact that respondents were largely teenagers. In 2002, the Hong Kong Police planned to equip CCTV cameras in Lan Kwai Fong for crime prevention and conducted a household survey [12]. Therefore the trends suggest that HK people may have accustomed to have CCTV monitoring to at some specific/popular locations were security concerns are high due to some accidents.

Moreover, there is some concern in the general public about installing CCTV in public transport such as taxi and MTR trains since 2008. Two voices are arguing on this issue. The cons side is afraid of being taken exposing photos, wastage of money and invasion of privacy [13]. However, taxi robbery and number of indecent cases increase in these years, taxi drivers and claimed for CCTV installation for personal security purpose [14][15]. Actually in January 2012, the Secretary of Transport and Housing Bureau (Hong Kong) stated that actually some buses, trams and MTR trains have already installed CCTV for security control and monitor purposes [16]. For taxies, *they can install CCTV without the approval* of Transport Department.

3) *Fingerprint is the most accepted biometrics modality*

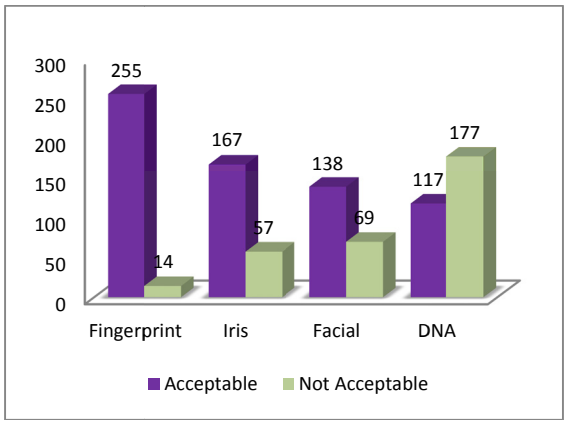

Figure 3: Acceptance of biometrics modality/technology.

Different kinds of biometrics are being used nowadays. In the survey we have chosen the four most common types of biometrics and asked the respondents' for their preference. The results and trends from this survey should not be surprising as fingerprint is commonly employed in HK border crossings (residents avail the benefits of efficient and high speed border crossings) and is essential component of mandatory HK ID cards since 2005. There are high privacy concerns with the DNA as it is well known to provide most details from human body which may highly be personal.

4) *Airport and Bank security are the most preferred venues of deploying biometrics technologies*

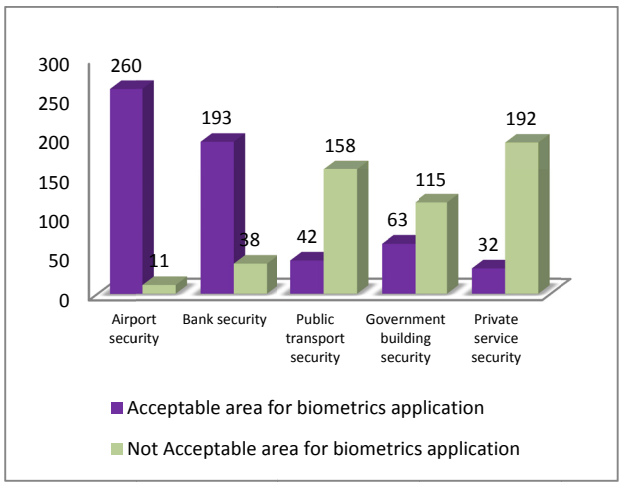

Figure 4: Opinion on areas with the biometrics based security.

It can be observed from the figure 4 that the biometrics deployment in airport security control is the most acceptable venue. In Hong Kong, the government has already introduced biometrics based *E-Channels* for airport departure since 2004, people are well familiar with such practice and avail convenience from the biometrics technology. Next, the survey suggests that people equally care for their financial security and there is no suggestion to favor personal privacy here as the bank security is also the most preferred place for biometrics deployment and ranked in second place. The other three choices: public transport, government building and private service, are to large extent unacceptable to the respondents; or to conclude, they are not willing to accept biometrics usage in such public places. The survey by Unisys in 2010 [17] stated that 73% Hong Kong people prefer giving their biometric information to Hospital Authority and Department of Health while only 34% to the banks. But from our survey, it is suggested that they have higher confidence and open mindedness to share their biometric information with the banks because 63% respondents chosen "4" and "5" (acceptable).

5) *People's concern and acceptance on disclosing personal information*

The trends here indicate that the respondents' are rational and pay attention to their personal information. They will not disclose their information if they do not trust or are not familiar with the company and when being asked for sensitive information. The percentage of such resistance slightly decreases *if they will receive a gift*. Therefore people can sometimes be greedy in that they will use their information in exchange for gift and such tradeoff is better illustrated in [26]. Another point people concern about whether they could be in the status of being anonymous.

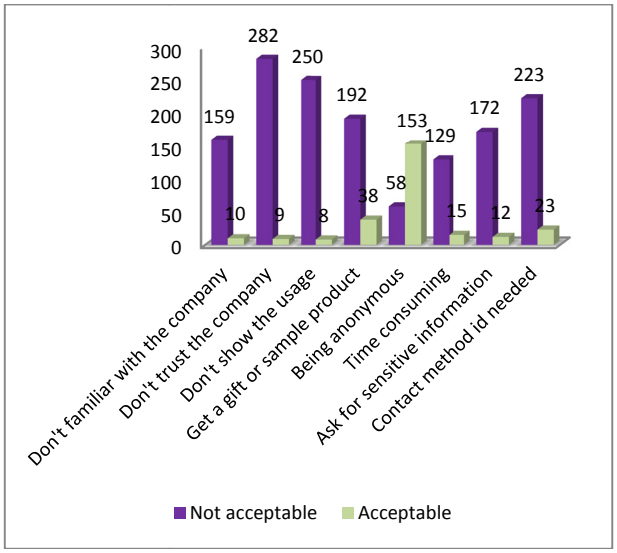

Figure 5: Scenarios on preferences for sharing personal information.

6) *Social networking website in our day-to-day life*

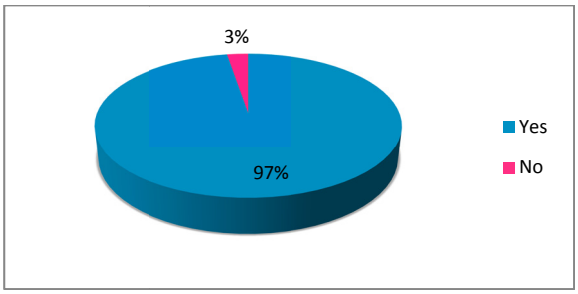

Figure 6: Use of social networking service websites.

Nearly all respondents stated that they use or participate in the social networking websites on the internet, like Facebook or Twitter. These kinds of websites were introduced about year ago, in 2007, and being used for around 5 years untill now. It is not difficult to see people are surfing on these websites by Smartphone in the buses or metro's (MTR). According to Ketchum's press released in August 2011, *92% of HongKongers surf on Facebook every week and 77% read blogs* [18]. These results [18] support our survey findings which suggest that the social media is now deeply engaged to become part of individual's lifestyle.

7) *Females are more prevalent than males for sharing the photos on social networking sites*

There is an interesting trend for the habit of sharing photos or checking in their current location on social networking websites. Figure 7 suggests that female gender loves to upload their photos or locations more than male's. This implies that female seems to have lower sense of privacy concern that they may let others take advantage of own photos for other purposes as mentioned in the earlier discussion. The trends also suggest that female is more likely to have the habit of sharing their experience in daily life.

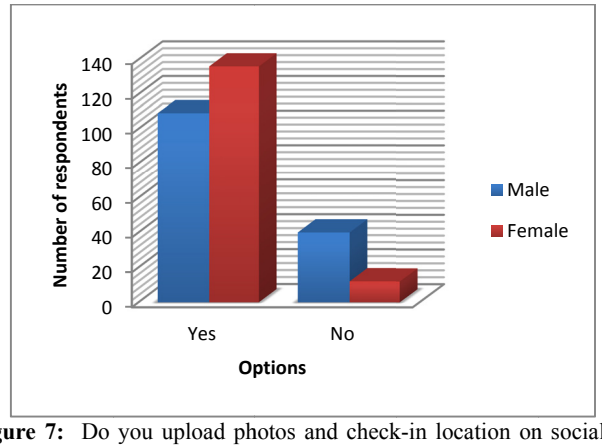

Figure 7: Do you upload photos and check-in location on social networking website?

8) *Installing Cameras in Taxi is Least Acceptable*

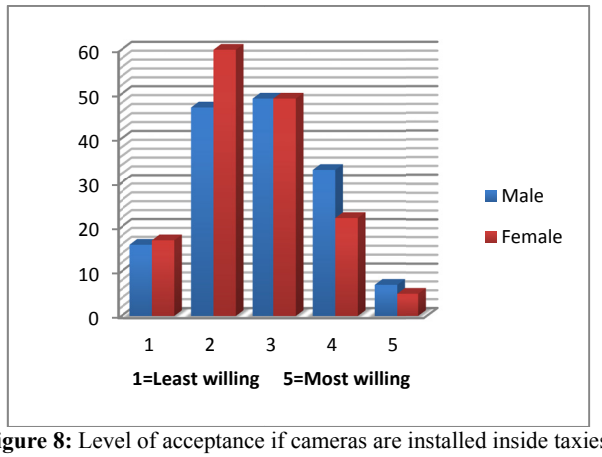

Figure 8: Level of acceptance if cameras are installed inside taxies.

In question 9, one of the cases is about the security cameras to be installed in taxi. Before the commencement of survey, we expected that this proposal will be more opposed by female's in general than males because from the research that some women in mainland China commented that they are afraid of the camera will take their exposed photos of events like personal makeup. However the result of this survey suggests that both male and female are concerned (figure 8) about the privacy when camera installing inside a taxi. Many of them chose"2" which means that they are not willing to have camera installed inside a taxi. There is some minority chose "5" in *very willing* to install the cameras, these response may be outliers or from people (like elderly) who have most concerns about security or health.

9) *Preference for Security or Privacy?*

Privacy and Security, which one you concern more? Males' answers are quite evenly distributed from choices "2" to "6". On the other hand female here shows a larger proportion over the answer "5", that is the preference of having more security. It reflects that most female feel insecure easily than male and seeks for higher security instead of worrying for privacy. This finding correlates with the earlier study by the Unisys Security Index in May 2011 [19], which also suggested that women are more concerned about their overall personal safety than males.

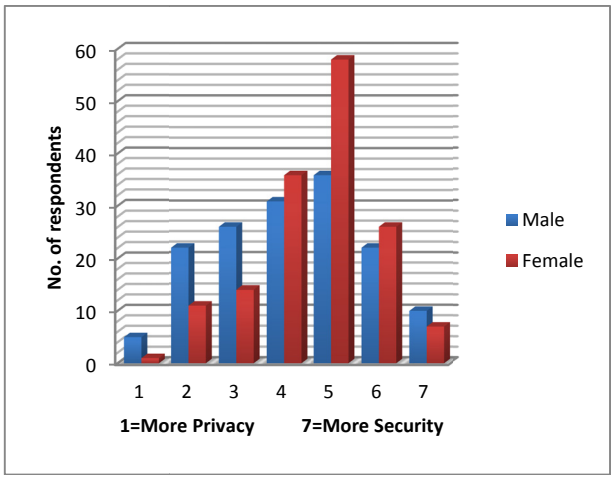

Figure 9: Choice between security and privacy (female and male).

10) *Personal Privacy is more important for Elderly than Youngsters*

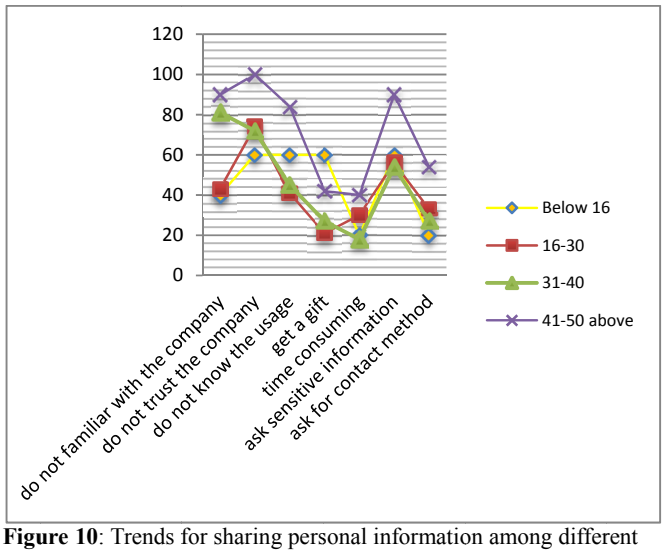

Figure 10: Trends for sharing personal information among different age groups.

Age group of 16-22 and 23-30, 41 -50 and 50 above are combined for easier analysis. In overall, the elder age group (41-50 above) has a more negative response in answering the convenience of disclosing personal information. They often rated "4" and "5" [30] which means they are unaccepted in some cases while other age groups rated "3", neutral only. The elder age group has a higher score and trend than those from other age groups, which reflects that have higher concerns or better understanding on the possible misuse of sharing personal information in different domains.

Limitations

The first limitation is that this is an online survey and did not involve any distribution of the hardcopy in person. Therefore the pool of respondents was limited. The distribution of questions was also not even and the questions on biometrics were smaller than those attempting to assess the privacy related concerns and preferences from emerging social networking technologies.

Besides, the age distribution during the survey is not even and the size of the survey is not very large. The majority of the respondents are between 16 and 30 year-old. The above age analysis is compared by enlarging the number of 31-50 above age group in ratio as estimation. Therefore, there are not sufficient findings available when compared with the answers received from respondents in other/different age group. The final result will be more accurate if more respondents the age group of 31-50+ participated in this survey. The total number of respondents is 305 and increase in this number would have helped to generate more confidence in the reliability of the survey about Hong Kong peoples' attitude and habits.

Figure 11: Developed user interface for survey in Chinese language.

Figure 12: The QR code printed on the train ticket.

V. CONCLUSIONS

This paper has presented a unified study on the privacy related challenges from the emerging technologies. We also designed and developed an online survey to ascertain people's understanding on the various aspects of privacy and their willingness to tradeoff some privacy with the benefits of increased security. The online survey from 305 participants revealed great deal of information on public attitude towards emerging biometrics and social networking technologies.

The survey results from the public opinion on the installation of security cameras points towards the endorsement in the (further) deployments for the CCTV in Hong Kong for monitoring in facilities like airport, banks and also in some public areas. Figure 1 illustrate that about 40% people are in favor of more cameras for better security measures while Figure 2 shows the favorable areas where they are willing to have cameras monitoring. This trend indicates people's confidence in some of the emerging technologies and opinion to exploit them for public good and security.

The survey trends for the acceptability of CCTV in Hong Kong[‡] taxis are not positive. For most of the respondents, taxi is regarded as a private place therefore the taxi owners/drivers can seek for general acceptance or second opinion, before they finally decide to install them or can explore another alternative to safeguard them. This decision may have some financial implications it may result in decline in business (income) for taxis as the passengers might not want to board taxis for privacy concern and prefer alternate mode of transportation. In this context, it is reasonable to mention that public sensitivities should not be ignored for better security, especially when preference/business places have some elements of personal activities. Therefore a formal announcement, proper public promotion and education is deemed to be more appropriate when/if taxis equip themselves with CCTV inside.

This survey results also reflects that people in Hong Kong prefer fingerprint as the most convenient biometric modality followed by the iris. Such opinion possibly reflects the convenience availed by the Hong Kong residents in the day-to-day practice of using fingerprint based Hong Kong ID card or *e*-channel in border crossings. The choice of iris and face as the preferred biometric modality among large number of residents (figure 3) can be attributed to the failure[§] of current fingerprint technologies for authentication among large number of residents (like elderly, manual laborers, *etc*.). The lack of privacy concerns in the usage of emerging social networking technologies could possibly due to the enhanced convenience in instantly sharing the information and also due to the lack of awareness with the potential security/privacy related hazards [20], [32]-[33] with the usage of such technologies. Therefore there is pressing need to caution on the risks bore by users and the service providers, including for the privacy and biometrics security, while engaging in social networking. The economic well-being of residents and resulting sense of security can also motivate individuals to trade-off privacy for better security, especially in areas like banks and airports. Development of novel biometrics and

[‡] Taxi drivers in the city of oxford (UK) have been told to install CCTV in taxis by 2015 else their license will be revoked [29].

[§] A large scale proof of concept study conducted by UIDAI has recently estimated [24] that ~1.9% of people cannot be reliably authenticated using fingerprints. Earlier study from NIST has also estimated [25] that about 2% of the user population *do not* have sufficient quality fingerprints to be used in fingerprint identification systems.

social networking technologies that can simultaneously ensure high degree of anonymity [4], accountability and security can help to address wide range of social concerns in the deployment of emerging technologies. Early societal intervention in the research and development process can help to ensure that the developed solutions also embed the solutions resulting from the negative impacts of the technologies [31]. It has often shown that when social factors are integrated into the design and decision making process, the solutions tends to be long lasting and cost effective.

Acknowledgement: This work is partially supported by the project no. PolyU5011-PPR-12.

VI. REFERENCES

[1] *Free apps 'can spy on texts and calls': Smartphone users warned of privacy dangers.* (2012). Mail Online. http://www.dailymail.co.uk/sciencetech/article-2106627/Internet-firms-access-texts-emails-pictures-spying-smartphone-apps.html, accessed February 15, 2012.

[2] *Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini and D. Tzovaras (*Eds*), Springer 2012.

[3] 88.8%的人表示曾因個人信息泄露遭遇困擾. (2011). Sohu.com Inc. http://cul.sohu.com/20110421/n306231360.shtml, accessed January 4, 2012.

[4] A. Shamir, "Adding Privacy to Biometrics Databases: A SetBase Approach," *Int. Conf. on Data Protection and Privacy Commissioners*, Madrid, Nov. 2009 http://www.privacyconference2009.org/program/Presentaciones/common/pdfs/adhi_shamir_madrid.pdf

[5] *China Publishes Draft Privacy Guideline,* (2011). http://www.hldataprotection.com/2011/04/articles/international-eu-privacy/china-publishes-draft-privacy-guidelines/, accessed December 22, 2011.

[6] Privacy laws of United States, http://en.wikipedia.org/wiki/Privacy_laws_of_the_United_States. accessed February 6, 2012.

[7] US-VISIT Electronic Privacy Information Center. (2012). http://epic.org/privacy/us-visit/ accessed February 6, 2012.

[8] US-VISIT: Biometrics Are Here to Stay. 2012, http://crisisboom.com/2012/02/21/biometrics-are-here-to-stay, accessed February 6, 2012

[9] Sina Weibo privacy concerns - Leakage of information from blogging, CQ.XINHUANET.com.煩惱：微博泄隱私每天收百封垃圾信. (2011). http://big5.xinhuanet.com/gate/big5/www.cq.xinhuanet.com/news/2011-11/16/content_24134046.htm, accessed December 6, 2012.

[10] 小心二维码"出卖"你个人隐私. (2011). http://news.5sw.com.cn/html/s4/c17/7402.html, accessed December 6, 2012.

[11] Taxi cab recorders bring up privacy doubts. (2012). http://english.sina.com/china/2011/1124/417368.html, accessed April 6, 2012.

[12] *Survey on Public Place Surveillance*. Social Sciences Research Centre of The University of Hong Kong, 2002.

[13] 反對意見. Wenweipo.(2008). http://paper.wenweipo.com/2008/02/01/ED0802010017.htm, accessed December 6, 2011

[14] 業界聲音安裝閉路電視防罪案. Apply Daily. (2009). http://hk.apple.nextmedia.com/template/apple/art_main.php?iss_id=20090209&sec_id=4104&subsec_id=11866&art_id=12181956, accessed December 6, 2011.

[15] 婦聯要求港鐵裝閉路電視. Macao Daily News.(2011). http://www.macaodaily.com/html/2011-01/31/content_559053.htm, accessed December 6, 2011.

[16] 立法會十二題：公共交通工具安裝閉路電視監察系統. (2012). http://www.info.gov.hk/gia/general/201201/11/P201201110220.htm, accessed February 15, 2012.

[17] 香港人缺乏安全感？. Hong Kong Economic Journal.(2010). http://www.hkej.com/template/forum/php/forum_details.php?blog_posts_id=59845, accessed February 15, 2012.

[18] Social Media Matters: Hong Kong Addicted to Facebook. (2011). http://www.cprfhk.org/media/Ketchum_Social%20Media%20Matters_Hong%20Kong%20Addicted%20to%20Facebook.pdf

[19] Unisys Security Index – Hong Kong. UNISYS. (2011). http://www.unisys.com/unisys/countrysite/news/index.jsp;jsessionid=FD5DA068BDD4AA6B9B7833511BD31BBA?cid=900004&id=5100014

[20] More than facial recognition – Tagging your friends in a facebook photo – a potential danger, http://innovya.com/2011/11/more-than-facial-recognition-tagging-your-friend-in-a-facebook-photo-potential-danger, Accessed 12 May 2012.

[21] *Social Media Involvement Greater in China than U.S.*, http://www.webpronews.com/social-media-involvement-greater-in-china-than-u-s-2011-04, Accessed April 2012

[22] China's New Privacy Regulations Go Into Effect, http://www.hldataprotection.com/2012/03/articles/international-eu-privacy/chinas-new-privacy-regulations-go-into-effect/#more, Accessed May 10, 2012

[23] History of Fingerprinting http://www.fingerprinting.com/history-of-fingerprinting.php, Accessed 10th May 2012

[24] *Role of biometric technology in Aadhaar authentication*, Authentication Accuracy Report, UIDAI, 27th March 2012. http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf

[25] NIST Report to the United States Congress (2002), *Summary of NIST Standards for Biometric Accuracy, Tamper Resistance and Interoperability*

[26] J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research*, vol. 22, pp. 254-268, 2011. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf

[27] Raising Pan European and International Awareness of Biometrics and Security Ethics (RISE), http://www.riseproject.eu/

[28] *Commission proposes comprehensive reform on data protection rules*, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm, accessed 12th May 2012,

[29] *CCTV taxi plan 'a staggering invasion of privacy'*, http://www.independent.co.uk/news/uk/home-news/cctv-taxi-plan-a-staggering-invasion-of-privacy-6262221.html accessed 12th May 2012,

[30] A survey on privacy-aware security technology deployment in Hong Kong, http://www4.comp.polyu.edu.hk/~csajaykr/FYP2012/surveyPJ/survey/

[31] *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Field*, René Von Schomberg (*Ed.*), November 2011. http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf

[32] Amy Wong (2010, Aug 4). Octopus chief resigns over data sales scandal, revenue donated to charity. *International Business Times*. Accessed 15 May 2012 http://www.ibtimes.com/articles/40913/20100804/octopus-scandal.htm

[33] Priscilla Jiao (2010, Nov 9). Tencent and Qihoo trade theft accusations. Mainland cyberwar raises fears for privacy. *South China Morning Post*, pp. A1, A3.

[34] http://en.wikipedia.org/wiki/Hong_Kong_acid_attacks, accessed 12th May 2012.