Analyzing Privacy and Security Issues in the Information Age - an Ethical Perspective

JI-XUAN FENG
School of Computing and Information Science
Zhejiang Wanli University
8 South Qianhu Road, Ningbo, Zhejiang
PRC

JANET HUGHES
School of Computing
University of Dundee
Dundee DD1 4HN, Scotland
UK

Abstract: - Associated with expanding using ICT across the global, there is more and more concern about privacy and security issues. Today, people find that their personal information is hard to protect. Results from a literature review, from a survey and from case studies all indicate a clear solution: the key is people. It is people who develop ICT, and people who decide the different ways that ICT is used. Therefore education about international law and ethics, and education to develop an understanding of cultural differences will provide a positive attitude to promote the improvement of the privacy and security situation in the information age. Finally, there is a discussion about how to establish a viable security culture environment.

Keywords: - Security, Privacy, Law, Ethics, Core value, Global culture education

1 Introduction

It is well known that we are living in a fast-growing Information and Communication Technology (ICT) Age, that is to say, the information and communication technology - ICT is involved in our life every day, and it is expected that in future it will be much more deeply blended with our life. Meanwhile, the Internet means we live in a global village. Everyone could meet anyone who is online at anywhere, and at any time.

If I really could lookout the electronic window of my living room in Boston and see the Alps, hear the cowbells, and smell the (digital) manure in summer, in a way I am very much in Switzerland.

This is what Dr. Nichloas Negroponte describes the "place without space" of America in Information Age. ICT, anyway, does not only play role in developed country. In China, for example, especially in the recent years, with the dramatic combination of "electronic digitalization" with various aspects of society, economy and culture, many projects have been put forward and implemented, such as "digital area" and "digital city". These information systems, aiming to realize e-government and e-commerce, has established a number of urban information infrastructure featured with digitalization, the Internet, artificial intelligence and developed all-round and integrated information resources from governments, enterprises and the society.

Does ICT bring us all good effects, and always have a positive side? Clearly, the answer is "No". E-commerce has not only brought people lots of conviniences, but also possibilities of fraud. Here is an example:

In January, 2006, phishers have crafted a URL on geocities that is nearly a version of home page of UTI bank and send it to customers via email with intentions, get personal information of more than 100.000 customers of UTI.

Actually, there are much potential physical and mental health risks to human beings associated with the expanding of use of ICT, including negative effects on our environment such as heavy metal contamination caused by the manufacture of the ICT-related products. Among the negative effects are world-wide concerns about privacy issues also. However, there are notable differences between Western culture and Chinese culture in many of these areas, such as "what is privacy" and what reaction there is against invasion to personal privacy. Methods used in this study to investigate these differences were a literature review, identification of

case studies, and a survey of university students. The aim was to identify ways to better preserve our right to privacy in today's ultra-modern world, as well as to secure a safer life and promote ways of harmony.

2 Some Differences in Understanding of the Concept of 'Privacy'

The concept of 'privacy' is dynamic, and has changed as society has evolved. Privacy is also interpreted differently in different cultures.

2.1 Historical differences

The term 'privacy' changes as the times we live in change, and such transformations will continue, as the term 'privacy' had become "informationally enriched" by computer technology [1]. In the early twentieth century in China there was almost no home telephone number, no credit card, no personal social security number, and of course no information system (IS). Compared to today, the meaning of privacy was rather narrow. Currently, data such as your credit card password, email account password, fingerprint, digital photos, cell-phone number, and even your CV document are judged to be items that should be private. The concept of privacy has become more complicated and has broadened.

Westerner describes privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [2]. In Western, privacy has been considered as one of the most important needs of people. "Without privacy, we lose our very integrity as persons." (Charles Fried, 1968).

Clearly the increasing development of ICT as a communication mode therefore is a factor in the concern about privacy: widespread use of ICT itself threatens personal information security. For instance, RFID (Radio Frequency Identification) technology, database data mining techniques, and wireless home networks result in significant potential risks that such sensitive data might be leaked to others or to the public. So we can say the more advanced ICT becomes, the more risk there is to the safety of personal details.

Scholars in China consider the personal information as data like name, date of birth, identification card number, Hu Kou, genetic data, fingerprint, marriage, family, education, profession, health, financial condition and whatever to identify the person. Personal Information Protection Law(Draft), which was started in 2005, has been submitted to the State Council for discussion. In this draft of law, personal information is defined as all information to identify one particular person including paper document, audio and vidio records, fingerprint or even archives. And even more, on the 25th of August 2008, the 4th Conference of the Standing Committee of the 11th National People's Congress (NPC) deliberated on The 7th Amendment to the PRC Criminal Law (draft). The Draft is the first time a proposal for providing protection of personal information by imposing criminal charges for violations on such information was put forward.

2.2 Cultural differences

Mirroring historical differences in the understanding of privacy is the fact that generations of young people in different cultures hold different views about the scope of privacy. The ETHICOMP survey of professional practice [3] indicated that college students in both the UK and China thought that the privacy of data was not very important. The Chinese perspective and understanding is that private data are data that you do not wish others to know about, such as information about your family's property, love life, and health condition. However, in Western cultures, there is a much larger range of items that are held to be sensitive personal data, including salary, religion, the number of children in your family, personal medical records, a woman's age, marital status, sexual life, and political preference. Thus compared with Chinese culture, Western culture is more sensitive about personal privacy and the meaning of 'privacy' is considerably wider [4]. In China, people are not particularly anxious about discussing topics such as "How much money do you earn", "Have you married", "What kind of illness do you have". Thus an information system that includes personal data may be acceptable in one country, but it may be considered insecure in another country. Perceptions of security are affected by cultural differences and social environments.

According to Moor's theory of privacy [1], privacy is one expression of the core values of security, and therefore privacy must be maintained and respected. Privacy corresponds to security: you will feel safe living in a society in which your privacy is well preserved, and vice versa. Currently when one talks about privacy and security, it is information system security that is considered, because in this Internet world, our personal data is stored in IS systems [5].

3 Security of Private Data in the Information age

Through nearly 20 years of effort, the Internet has linked people across every corner across the world, meeting together on the Web anytime and anywhere. People can talk using web cameras, headphones, and chat rooms, and can send instant messages and e-mail each other. Personal information can be spread easily across the world via these web techniques. It is extremely easy to copy information from the Web and paste it back to another website again, and so information can be broadcast immediately all over the world. As a result, it can be very difficult to control the dispersal of personal information in this information age. Simultaneously, new ICT techniques and tools have made personal data more vulnerable to privacy violation.

A search of www.bbc.co.uk using the keywords "computer" and "privacy" identified 154 separate items relating to disquiet about privacy breaches (29 November 2008). However, unease about privacy violations is less-and-less exclusively a Western concern: the same search of www.china.org.cn identified 44 separate items relating to disquiet about privacy breaches. The same concerns exist in both cultures: concern about pornography, lack of privacy, and lack of control. The People's Daily reported that in 2000, at the 16th World Computing Congress in Beijing, President Jiang Zemin warned that the Internet contains "some garbage like hacker, privacy violating, misleading information and security problems." He called upon the international community hurry up the progress to launch an international Internet convention to better serve and safeguard the Internet surfers.

The belief that legislation can be a means of securing private data is evident from a series of reports in the Chinese press. The press has begun to report the need for legislation to control Internet-based software that "might steal personal information or introduce viruses". Recently, individuals and organisations have started to use the law to challenge bad behaviour. An example reported by the Xinhua News Agency on October 18, 2006 was of a grassroots "netizen" organisation challenging a major corporation:

The Beijing-based Anti-Hooligan Software Federation began court proceedings against Yahoo! China in the Haidian District People's Court on Monday. Experts said the absence of legislation in preventing hooligan software has added to the difficulties involved in fighting such cases.
Generally, hooligan software includes such things as adverts (which you don't want to look at), spyware (which can steal your personal information), trackware (which can find out where you live and work) and malicious software such as pornographic information.

Similarly, in 2007 an individual university student challenged Microsoft:

Peking University student Lu Feng believes that Microsoft's newly launched "WGA Notification" program violates his safety of personal information and his privacy. He decided to bring both Microsoft Corporation and Microsoft (China) Co. Ltd. before the court, and recently the First Intermediate People's Court of Beijing accepted this case.
(www.china.org.cn, September 12 2007)

However, it appears that there is a long way to go before people feel secure about their private data. On February 20th 2008 the Xinhua News Agency reported: *"A survey by the Shanghai University showed that 85 percent of the more than 100 primary school teachers polled and 73.4 percent of the 200 parents expressed anxiety about porn and violence on the Internet, but 56.8 percent of the teachers and 29.2 percent of the parents felt helpless in tackling the problem."*

An article in the Beijing News, reported in China Daily, March 18 2008, noted:
"The rampant spreading of personal information has left us no privacy."
and it called for legislation to protect personal information. The same concerns about security of personal information exist in the West, despite legislation dating back at least 25 years to try to provide privacy – whether personal, family, business or professional. The existence of legislation does not prevent security breaches. In the United Kingdom, data privacy problems emerge regularly despite the evolution of legislation from 1994 to the present. Problems arise from both private companies and from public institutions. As examples, the Information Commissioner's Office (ICO) in the United Kingdom (i) in 2007 found 11 banks and other financial institutions in breach of the Data Protection Act after investigating complaints concerning the disposal of customer information [6], and (ii) in 2008 found the National Health Service in Tayside and in Lanarkshire in breach of the Data Protection Act after investigating complaints concerning the disposal of patient information at Strathmartine Hospital in Dundee and Law Hospital in Carluke. The ICO was alerted to both data breaches earlier this year when members of the public found confidential health records in buildings on the site of the former hospitals [7].

That the law may not protect the security of personal data was evident in November 2008, when

the names and other details of 10,000 members of the far-right political group the British National Party (BNP) were published on the internet [8]. Although the original posting on a website was removed promptly after publication, the details were copied by a number of people and republished elsewhere, online. Now the information is available globally, partly because Internet Service Providers and Social Networking Site Providers argue that they cannot be held responsible for information posted by others on their sites, since they do not control that information.

Privacy therefore is no longer a local issue: it has now a global focus. Therefore any consideration of privacy and security concerns should be expanded to become an international project that will benefit from such diversification. Theories about privacy should be globally devised to provide a universal solution, especially with regard to any philosophy of IS security. Central to this should be a focus on people. It is people who hold different viewpoints about privacy, who create the core values of society, who influence different cultures, who develop ICT and who dominate the ways that ICT is used. The next section considers the tension between people wanting to feel secure about their private data, and wanting the benefits that lack of privacy offers.

4 Privacy versus Personalisation

Different responses identified by a survey of reactions to the prospect of someone invading your privacy demonstrate different awareness of privacy issues and different levels of concern. A survey was made of Zhejiang Wanli University students in China. A total of 250 questionnaires were issued; 184 were returned, of which 133 questionnaires were valid. These included a small group of five international students. The Chinese students' answers to the question, "once someone invades your privacy, what is your reaction?" were "angry", but few of them would take legal action. In contrast, the international students said they would take legal action. Another difference found was that there is no independent Privacy Act or Law in China, but there is for almost all of the Western students. 79% of the Chinese students agreed that: "The increasing need for privacy and data protection has changed the way in which I design or develop information systems", and 6% disagreed. 15% of Chinese students neither agreed nor disagreed. More than 20% of the students therefore did not think it worthwhile to act to protect their personal records. This may be due to a conflict of interest for users. Although online users are concerned about their privacy, they also value personalised content, and they are aware that personalisation on web sites can be profitable for web vendors. There is a challenge for web vendors to protect privacy and yet provide users with the benefits of rich communication, such as recommendations and price discounts. A laboratory experiment in 2001 used a questionnaire to test privacy preferences: although a proportion of participants had expressed, they displayed "a surprising readiness to reveal private and even highly personal information". The authors concluded that Internet users have views about privacy but they do not necessarily act according to their stated views [9]. This was confirmed in 2005: Once in an online interaction, users often do not monitor and control their actions strongly, and privacy statements seem to have no impact on behaviour [10]. A study in 2007 of a small number of students at Carnegie Mellon University found that the average willingness-to-accept money to sell personal information was dramatically higher than the average willingness-to-pay to protect personal information. [11]. Huberman et al (2005) found that people were only upset about personal data being used if it was against their interests, and particularly so the more undesirable a personal trait is, as perceived or actual, compared to the group norm [12]. The next section considers examples of cases to illustrate the importance of the privacy and security of data.

5 Case Studies

5.1 Human search *(Ren Rou Sou* in Mandarin phonetic transcription)

The term "Human search" refers to the use of modern information technology to find out about people [13]. (This is different to the traditional network information search or 'machine search' – it is people-powered searching.) In human search, a questioner can ask questions of other people on the Internet to find out about a particular target person. The questions may be about any aspect of the person, such as their professional background or experience. Answers come from other people on the Internet, across the country or the world. After a human search, a target person can be completely revealed on the web: all his/her private information may be posted on the web. It is seriously harmful to the people involved. In fact, using "human search" as a keyword searches on the Web, one may read number

of such cases, even a suicide event related to human search. Recently in China, human search has caused a number of debates: does this invade the person's privacy? Is this a moral manner to solve a problem or to find answers to a question? Is the entitlement to privacy of ordinary citizens reduced if information searching is via the Web?

This case suggests that security is not just a matter of technology: it is a matter of the quality of people who use it. The use of the ICT tools permits one to ask for answers from all the Internet users in the world. However, it is hard to know whether or not the information provided by the Internet is true or not true.

5.2 Medical Information System (MIS) in a hospital

Last year, in a hospital in Ningbo, China, there was a system problem in a hospital MIS that resulted a massive disarray. Doctors, accustomed to using a computer to select prescriptions, were not familiar with writing prescriptions. Whilst the MIS was unavailable, they were faced with several emergencies, and only were able to write prescriptions after several attempts. At the same time, orders and information were lost from the CT scan examination room, the operating room, the medical service and even the pharmacy. The story makes us aware of the vulnerability of data, even within a hospital. If an MIS is at risk, for example because of a power loss, the consequences can be huge, perhaps even fatal. Hence, it is of vital importance to keep the traditional way to run hospital system as the backup system, as a redundancy system.

5.3 Hacker

A secure Information System (IS) is one in which there can be some confidence in the accuracy, integrity, and authenticity of stored data. However one main threat to information systems is that of a hacker. Anecdotal evidence is that almost all hackers are young men or students who hack into information systems just for fun. However, hackers are also known to use backdoor programs, spyware and other ICT skills to demonstrate their intelligence. In the late of 2006, a young man in China designed the computer virus named "Panda Burning Incense". It was then sold to others to infect thousands of computers. With the help of teachers in prison, the hacker was made aware of his mistake, and convinced to write anti-virus software and send an apology to the National People via the Web. This case suggests that education of young people is very necessary. With regard to IS security and privacy, it is more cost-effective and sustainable way to provide improved privacy and security than the development of more security technologies. Moreover, it could construct a vital culture for our society to have a harmonious environment.

Similarly, data suggests that more serious harm and a larger proportion of harm are caused to companies by internal rather than external hackers who attack networks. It is reported that 70% of global losses of the amount of 50,000 U.S. dollars or more are related to an internal network attacker. Furthermore, 80% of internal leaks of confidential data are caused by the leakage of the confidential information by electronic data eg by electronic documents by email [14]. Therefore, again it seems that education is the best way to invest in a security system.

6 Education as a Strategy for Security

A number of authors have suggested that the key to successful information systems security and data privacy is not the law – which can be broken – but the development of a genuine ethical understanding and belief about correct behaviour in the people who develop information systems. Rogerson (2007) states: "we believe it is paramount that computer ethics be embedded within the computer science curriculum" [15] in universities, to develop ethically responsible and virtuous citizens. A number of universities in China do have ethics within the curriculum, but it does not appear to be as commonplace as in the United Kingdom. The prevalence of computer ethics teaching in the United Kingdom is partly related to the desire for many universities to be accredited by the professional body, the British Computer Society (BCS). The BCS was established in 1957. Its objectives are to promote the study and practice of computing and to advance knowledge of and education in IT for the benefit of the public. It has a code of conduct [16] that sets out the professional standards required by BCS as a condition of membership. Universities accredited by the BCS do teach its professional codes, including the public interest, duty to the relevant authority, duty to the profession and professional competence and integrity. The first of these four includes privacy recommendations:

"You shall ensure that within your professional field/s you have knowledge and understanding of relevant legislation, regulations and standards, and that you comply with such requirements.

As examples, relevant legislation could, in the UK, include the Public Interest Disclosure Act, Disability Discrimination Act, Data Protection or Privacy legislation, Computer Misuse Law …"

In China, the professional body for I.T. is the China Computer Federation, established in 1985 (http://www.ccf.org.cn/). It has a similar set of objectives as the BCS: "The aim of CCF is to promote the progress of computer research, education, industry and application in various areas" but it does not have as a primary aim anything relating to "the benefit of the public", and it does not have a particular code of ethics.

Another interesting distinction between the emphasis upon code of practice and ethics in the United Kingdom and in China is evident from the need to obtain ethical approval from student participants to participate in any research. In the United Kingdom, such ethical approval is concerned with such matters as methods of recruitment of study participants, informed consent procedures, information given to participants about the aims and methods of the study, contact information given to participants, and opportunities for feedback from participants to researchers. In addition, it covers the conditions of the study, discussion of any risks involved, freedom of participants to leave the study at any time, and matters of data protection and confidentiality. The ethical approval procedure is typically based upon published standards, such as the "Code of Conduct, Ethical Principles & Guidelines", section on "Ethical principles for conducting research with human participants" published by the British Psychological Society in January 2000. Researchers must gain ethical approval for any study before any students are asked to participate. In contrast, Chinese researchers would not need to obtain ethical approval before asking students questions; if they do not answer a questionnaire there is no problem, and if students do not agree with the viewpoints being stated then they say nothing or do not take part in the activity – and so their actions can indicate as much as their words.

It is clear that an understanding of the different ethical beliefs under which people operate – whether codified or legislated – is essential for success in the global ICS society. Li et al (2007) recommended that "executives and managers who are involved in commerce with Chinese firms need a deeper understanding on how their own value sets diverge from those of their business partners" [17]. Lorents et al (2006) found that for a number of students, the intent of an individual engaging in an activity is an important factor in their value judgement of the acceptability of the actions [18]. They point out that such Computer Science and Information System students will compose our future IT workforce and therefore it is essential to understand their ethical beliefs and value judgments in order to be able to make further influence.

Meanwhile, education will play very important role to increase the awareness to protect the personal information by everyone. The main problem in China nowadays is that most people does not have any idea about the protection of personal data. Hence education would help these people to realize the risk to lose personal data, what privacy is and what right they possess and the value of their data. The government must make efforts to teach people the basic techniques to control the private data in order to increase the ability of protecting themselves. For example, people should be informed that they provide demanded data on Internet unless they make sure the data they provided will be protected well. When people decide to buy something from one website, it is very important to keep the credit card number, account of the bank, and mobile phone number, and so on, in secret mostly. Password must be encrypted and anonymity could be used if possible.

However, it is real that people can not be absolutely sure whether or not to control the leak and the number of leaking their personal information and privacy. Actually, people can not control it. This situation certainly does not mean that people will lose their right to privacy. For example, a person in order to be able to complete one purchase on the Internet, has to disclose his name, home addresse, credit card account number, and other personal information, even though the disclosure of their personal information will be out of control. If the vendors to collect the information are not watching on their own nor leaking the information to others, then the personal information of buyers continues to have been respected and protected. In this sense, control is not a necessary condition for the protection of personal information. However, if the buyers agree to the have their personal information posted on the Internet, it can be said that the people have agreed to give up their privacy. Hence, as long as the individual can effectively control their personal information, privacy is well protected. That is to say, the key of personal information is just in the hand of every people.

7 Further Strategy Suggestions for Security

One aim of developing ICT is to make life safer and healthier, and to help to establish a harmonious

world. Thus, our attention should not only go to the development of new techniques, but also to the needs of people and of the natural environment in which we live. It is interesting to consider that the more privacy concerns we have, the more that security technologies may be used. Imagine that when you enter a house, you were asked to print your fingerprint, scan your iris, provide your signature, and so forth. Although we do have endless number of advanced technologies, but where is our life quality? Would you be comfortable living in such a monitored house?

Security can be a kind of embodiment of privacy. Both terms relate to people's feelings and sensitivities. Logically therefore strategies to ensure security should come from people too. A first strategy for improved information security would be to put more effort into young people's moral and legal education, to make sure they have learned what is right and what is wrong, and practice it in their daily life. At the same time, government officials, judges, lawyers, teachers and doctors should set a moral example for society to develop secure moral surroundings – and thereby reduce concerns about security.

A second strategy for information security would be to take advantage of different language concepts for the design of critical IS or sensitive computer systems. For example, in a Chinese IS a user name is presented using an English name. In an English IS a user name is presented using Chinese characters or it is perhaps mixed in some fields. Typically, a personal medical record could use both of these for increased security, given that most people do not know both languages. This also may result in a decreased development cost. Figure 1 presents the strategy.

In this figure, the patient name and other sensitive data are coded using Chinese character; age is stored using the sign of the Chinese traditional way. This year is the Chinese mouse year, so the patient's age is 34.

No	Name	Age	Order	Entry Date	Disease
1	何英	3Tiger	2653	Oct/21/ 07	肺气肿

Figure 1. Encoded the basic patient information

A third strategy is to consider our personal security. Since computers have become common tools for all of us, we use them every day in many circumstances. Eyestrain and headache, back and neck pain, repetitive strain injury and electromagnetic radiation (EMR) accompany over-use of computers. Children can become immersed in e-games. IAD — Internet addition disorder – is attracting global attention. In this information age, security should mean that both physical and mental health are protected. When we design a security IS, we should also consider how to make people happy and healthy.

A trusted society should have the mechanism of information publicity. Economists like George A. Akerlof, Michael Spence and Joseph Stiglitz proved how important the publicity of information to market economy from their respective angles. However, if the social foundation that bears the weight of information technology is an objective data environment, then the information is a magnifier in fair trades. Once an user exert interest in one company, he just needs to input some related terms on the web page and then can find enough instant and accuracy data, the data can be shown on screen or printed to papers. Conversely, if the objective data in whole society is a rare bird, then the informatization can't improve the whole environment, instead, it will thereby increase the non-objective extent because of speeding up the transmission of the information. Though a secure information system can protect data from being destroyed, changed and leaked by certain occasional elements or problems technologically, it can be vulnerable when attacked by false information. Only through the integration of data and the publicity of information can users possess enough information to select and decide, making those false information disappear.

The establishment of trust requires information's publicity and transparency. Trust information refers to those trust records gathered by governments, business and individuals, which have to be open accessed to the public. However, the mechanism of information publicity should be based on the balance of benefits. Through the games analysis on discredit it is concluded that the increasing of the possibility to reveal the untrust behavior and cost to punish will be the real constrains for opportunistic intend. The publicity of information consists of the governments, the businesses and the individuals.

7.1 The government

In China, governments possess most of information that businesses and individuals need. A survey of Guangdong province shows that over 90% information needed for business groups is controlled in the governments' departments. To make open government information won't increase extra government expenses and social costs but can bring some positive effects. Once the public enjoys useful

and correct information from government, all kinds of frauds (such as diploma forgery, real estate certificate forgery, government qualification, governmental approvals and contracts) will appear. However, government comprises many sub-sectors, in which the information flow is not completely transparent, these sub-sectors are somewhat separated. In addition to involving the national confidential, the major obstacle of government information publicity is to keep the merits balance between various sectors.

7.2 The businesses

According to foreign countries' experience, the publicity of business trust database is through either making laws to force businesses to make their trust information public, or complete market mechanism. In the UK, Italy and Netherlands, certain laws state that financial data about one company such as the Balance Sheet, the Liabilities and Shareholders' Equity, etc. are available to the public as well as business's financial reports owned by related government sectors. But there are not specific laws for business credit inquiry service and trust information in United States. Some American companies are willing to supply their trust information for credit agencies to better public identity. When a credit agent demands an unlisted company to give its financial reports, it can refuse. But in many cases, the companies choose to provide their data since they want to give their data to credit agents so as to make them know and then to expand trust trades. But in China, the stock market is far from developed. Listed companies are fewer, and most SMEs haven't been listed on stock market, so the correct and instant data about the majority of the companies in China is not easy to access. Even some listed companies often falsely declare their annual reports, plus the unintegration and the delay of information, thus making some uninformed shareholders be suffered from financial lose.

7.3 The environment of trust management

The publicity and transparency of information can promote the trust construction, and the interest balance mechanism should be grown in an agreeable trust management environment. Though China's trust management is developing very rapidly, and it has achieved some results, meantime, there also exist some shortcomings:

(1) Laws on the publicity of the trust information are not sound enough. The publicity and use of credit data lack of both definite laws and market mechanism, thus causing some government sectors and special agencies don't publicize businesses' and individuals' information, which should be known.

(2) Management and mechanism and function models are not complete enough. Government sectors, like industrial and commercial administrative bureau, tax bureau, financial sector, which possess related information have visible hurdles each other in terms of information exchanging. Because there hasn't been efficient mechanism of information resources share, information repetition, waste and responsibility shifting emerge in government sectors. The diversity of data formula makes the information process, transfer and storage difficult.

(3) In China nowadays, the level of the related trust data publicity is quite low, for instance the narrow coverage and the small involvement. Some objective and independent trust agencies (trust investigation, credit evaluation and special trust service) are far from mature; they ought to be commercial and social. Furthermore, individual trust investigation market is strictly controlled.

(4) Although the publicity of trust information is highly demanded, the distortion of information is fairly common. What's more, individual and business's needs for trust services are limited, social parties fail to use trust information to protect their rights and lack the aware to take advantage of trust information.

7.4 The approaches to realize the publicity of information

(1) To make clear the principles of the publicity of information in order to get rid of the asymmetry of information.

(2) To perfect the laws on the publicity of information, it includes: laws on credit, laws on trust evaluation, and laws on the publicity of trust information.

(3) To strengthen the leading system and the efficiency of the governments so as to make regulations step by step. Governments should guide the publicity process of individual trust information, business trust information and government information separately. In some special cases, government managements should build some specialized business trust database.

(4) To perform the integration of data resources and break the tangible barriers between various sectors in order to form an open system. In addition, governments should establish and administer an integrated data exchange platform, meanwhile they have to consider the problems of how to establish or administer various network information database. As to those undeveloped network information

systems, they should be integrated by unified data formula once are legally and officially approved.

(5) To establish official membership. The "clustering economy" appears in the East Coast area of China means putting groups of enterprises together in relatively stable and special areas. Although they don't belong to these formal organizations, they posses the shape of organizations and serve as formal ones, moreover, companies' trust information is quite concentrated there. Companies there may consider setting up formal membership organizations as foreign industrial associations do. To establish information database with legal identity and form, set up "information exchange mechanism" under the principle of voluntariness and mutual benefit. Member companies have to share their trust information and related trust records with others, after that, they have the right to inquire other's trust information. As to non-members, they have to pay to get trust information of other companies.

Information technology can provide good support for the collecting, processing and utilization of information and help the publicity of the government, but there must be a well solving for the problem of digital divides. Beside the improvement of the NII throughout the country, the information literacy of businessmen must be strengthening for the judgment of the trust by themselves. Information asymmetry always exists no mater online or offline, if the enterprise is devised by proper knowledge so that he could recognize and identify the fraud information, the trust e-commerce will be actually built up. For this issue, the computer network and Internet can help a lot, which has already been anticipated by Dr. Licklider to be responsive when the idea of network was first envisioned in hope at that time. The framework of information ages proposed by Prof. Buckholtz also included the information proficiency, which indicates the effectiveness of making and implementing of decision by individual or organization.

8 Conclusions

Privacy and security are complementary issues. Humans develop ICT, and humans use ICT – and so key solutions to privacy and security issues and problems depend on people, rather than just technical plans. For example, we could develop an international Computer Ethics course syllabus in all the colleges and universities in the world. Via e-learning, all the students could share their experiences and their understanding. This has been a target for a number of years, eg being suggested for Information Systems Professionals in 1992 [19]. As the process of globalization moves on at a faster and faster pace, international perspectives about privacy and security will soon converge. International laws, global ethics and multi-cultural education will affect our progress towards green life and sustainable surroundings, and help us secure our wish for a safe life.

References:

[1] J. H. Moor. Towards a Theory of Privacy in the Information Age. *Computers and Society*. 27 (September 1997)

[2] A. F. Westin. *Privacy and Freedom*. Atheneum, 1967.

[3] S. Rogerson and M. Prior. Is IT Ethical? The ETHICOMP Survey of Professional Practice. *Originally published as ETHIcol in the IMIS Journal*, Vol. 18, No. 1, 2008 http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/Ecv18no1.html Accessed on Sep. 22 2008.

[4] Li Wei and Li Manli. Differences between Chinese and American Privacy. *Abstracts of 2005 Symposium on International Communication*.

[5] T. W. Bynum and S. Rogerson. *Computer Ethics and Professional Responsibility*. Blackwell Publishing, 2003

[6] Information Commissioner's Office. *Banks in unacceptable Data Protection breach*. March, 2007 http://www.ico.gov.uk/upload/documents/pressreleases/2007/bank_pr_130307.pdf Accessed on November 27 2008.

[7] Information Commissioner's Office. *NHS Tayside and NHS Lanarkshire found in breach of Data Protection Act*. November, 2008 http://www.ico.gov.uk/upload/documents/pressreleases/2008/scottish_nhs_undertakings_press_release.pdf Accessed on November 27 2008.

[8] BBC. *BNP Activists' Details Published*. http://news.bbc.co.uk/1/hi/uk/7736405.stm Accessed on November 18 2008.

[9] S. Spiekermann, J. Grosslags and B. Berendt. E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior. Proceedings of the 3rd ACM conference on Electronic Commerce, p.38-47, October 14-17, 2001, Tampa, Florida, USA

[10] Berendt, B., Günther, O., and Spiekermann, S. Privacy in e-commerce: stated preferences vs.

actual behavior. *Communications of the ACM* 48, 4 (Apr. 2005), 101-106

[11] J. Grossklags and A. Acquisti *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, Sixth Workshop on the Economics of Information Security (WEIS 2007), Pittsburgh, PA, June 7- 8, 2007.

[12] B. Huberman, E. Adar and L. R. Fine. Valuating Privacy. *IEEE Security and Privacy* 3, 5 (Sep. 2005), 22-25.

[13] ZHAO Qing song, SONG Ru shun, Network Privacy Protection in WAP. *Application Research of Computers*, No.6. 2004

[14] Zhang Jie. For whom Designing the Water Wall, *China Computer Users*, No.17. 2004.

[15] S. Rogerson and T. W. Bynum. Reflections from China. *Originally published as ETHIcol in the IMIS Journal*, Vol. 17, No. 3, 2007 http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/ecv17no3.html Accessed on November 29 2008.

[16] BCS Code of Conduct. http://www.bcs.org/server.php?show=nav.6030. Accessed on November 22 2008.

[17] J. P. Li, S. P. Shin and G. L. Sanders. Prediction of Information Sharing Behavior in China: Under standing the Cultural and Social Determinants. *Proceedings of the 40th Hawaii International Conference on System Sciences*, 2007.

[18] A. C. Lorents, J. C. Maris, J. N. Morgan and G. L. Neal. Ethics of Computer Use: a Survey of Student Attitudes. *Academy of Information and Management Sciences Journal, Volume 9, Number 2, 2006.*

[19] E. Oz. Ethical Standards for Information Systems Professionals: A Case for a Unified Code. *MIS Quarterly*, December 1992.

[20] N. Negroponte, *Being Digital*, Vintage Books, Random House Inc., 1995

[21] http://www.spamrazor.net/news.htm

[22] Charles Fried, Privacy(A moral Analysis), reprinted in *Philosophical Dimensions of Privacy*, edited by Ferdinard D. Schoeman, 1984

[23] Tiantian Zhang. Probe into the Protection of Personal Information in the Opening of Archives' Utilization. *Archives Management, Number 3*,2007.

[24] Detang Zhou. The Protection and Opening of Personal Information.*Scientific and Technological Informatiom*，2007.