Analyzing Privacy and Security Issues in the Information Age

JI-XUAN FENG
School of Computer and Information Science
Zhejiang Wanli University
8 South Qianhu Road, Ningbo, Zhejiang
PRC
http://www.zwu.edu.cn

JANET HUGHES
School of Computing
University of Dundee
Dundee DD1 4HN, Scotland
UK
http://www.computing.dundee.ac.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 a case study 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 Technology (IT) Age, that is to say, the information and communication technology --ICT is involved in our daily life every day, and it is expected that it will be much more deeply blended with our life. Meanwhile, Internet makes us living in a global village. Everyone could meet anyone who is online at anywhere, and at any time.

Does the ICT bring us all good effects, and always have a positive side? Clearly, the answer is “No”. Actually, associated with expanding of use of ICT, there are much potential physical and mental health risks to human being, including negative effects on our life environment such as heavy metal contamination caused by the manufacture of the ICT-related products. Among the negative effects are the world-wide concerns about privacy issues. 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’

2.1 Historical Difference
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. Yet, as ICT continues to develop, the threats to the privacy of personal data and information keep increasing too. 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 to the safety of personal details.

2.2 Cultural Differences
Mirroring historical differences in the understanding of privacy is the fact that younger generations hold the different views about privacy [2]. The ETHICOMP survey of professional practice in 2006 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, 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, 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 disease 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 date is stored in IS systems [3].

2.3 Features of 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 past it back to other 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.

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.

Another feature of personal information in the information age is it keeping expanding and variety, and hard to control. It is so easy to copy information from the Web and past it back to other website again, thus any news can broadcast immediately all over the world. Simultaneously, new ICT achievements make people have more personal facts and more ICT tools to violate other’s privacy.

3 Survey
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 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 personal records.

4 Case Studies
4.1 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. (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.

4.2 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.

4.3 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.

5 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 characters; 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.

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Age</th>
<th>Order</th>
<th>Entry Date</th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>何英</td>
<td>3</td>
<td>虎</td>
<td>Oct/21/07</td>
<td>肺气肿</td>
</tr>
</tbody>
</table>

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.

6 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. 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: