Outline

Introduction

1. Definition of privacy

2. The manner of infringing Privacy

Personal behavior of infringing privacy

Live internet

Monitor of behavior

Personal communication of infringing privacy

Eavesdropping

To monitor e-mail

Personal information of infringing privacy

Collect personal data as commercial tool

Spread software which infringes Privacy

Cookie

Web bugs

Identity theft

Spamming

3. The way to protect Privacy

Self-Regular machanisms

TRUSTe

BBBOnline

Utilize high technology device

P3P

Anonymizer

4. Developing Act of protecting Internet Privacy

COPPA

GLBA

Safe Harbor Principles

5. Conclusion

Introduction

Along with need for information circulation, internet became necessary technology. Human being through internet to communication, business, entertainment and consume. Mass circulation of information has become irresistible trend. It became very easy to gather electronic documents of government, enterprise, and personal information through internet, in which they often relate to private information. Because of commercialized attempt, many people advanced process multi-information in order to enhance its value added and be benefited from selling information accordingly. This phenomenon became much easier because of overflow of information. For example, Marketing Company or advertising agent can gather personal data through credit card bill, medical case, phone registrations etc., and then resell them to relevant companies. Consequently, we should sincerely consider this negative development, and adopt appropriate methods to managing information collection and utilization in order to avoid harm of information overflow. Otherwise, we can expect that information overflow will trigger serious crisis of infringing privacy because tremendous demand of information exchange.

Definition of Privacy

Because of booming economy and fast expansion of internet utilization, human life is passing significant revolution in recent decades, which mainly resulted from different information, especially in personal information, are collected and utilized. After prevailing using of internet, it is much easier in collect, process, and utilize others' personal information. Undoubtedly, this trend strongly threat privacy of personal information. People's privacy and right has been infringed and invaded when personal

information is easier revealed by purposely manipulation of people who has evil intentions. Hence, the thought about privacy protection shifted focus to data protection. The concept of information privacy was generated accordingly.

Information Privacy not only means preventing evil intentions of grabbing personal information, but also should be expanded to level that we control utilization and circulation by ourselves. It means we have right to avoid that personal affairs are publicly interfered. Meanwhile, information collectors can't directly gather personal information, or even utilize gathered information in any purposes without notifying the person involved, and getting permission from him. We not only exclusively own the right of personal information, but also have right to examining integrity and accuracy of information, and deciding the scope of spreading personal information. Basically, we can divide information privacy into 4 dimensions,

Privacy of a person's persona

Such as name, identification, picture, voice etc. It directly involves to the first level of personal information and can means straight personal attribution, and should be primarily protected.

Privacy of Data about a person

Some information includes high personal attribution and enables the person are easier to be identified because it related to consumption habit, medical case, religion, finance statement, working experience, and crime record etc, which is unique and personalized.

Privacy of a person's communication

The expression of personal thought and emotions should not be monitored when people communicate with outside via electronic media. Hence, person should own privacy of communication content.

The manner of infringing Privacy

Infringing of Personal behavior privacy

- **Live internet**

To upload personal picture, action,vedio, and voice in internet and then forward them without notifying the person who involved.

- **Monitor of behavior**

We can monitor people behavior by using hidden camera which connecting to computer. That is also the way to find out suspect. This utilization is not only be used in prevent crime, but also in supervise employee's working attitude. Now, parents can even monitor their children's status in kindergarten via monitoring system connecting high speed cable and internet serve. There are more than thousands kindergarten had adopted this kind of systems. We can't deny the development of internet monitoring can significantly benefit people in short time, such as preventing crime, but it still causes controversy of infringing privacy in long time.

Infringing of Personal communication privacy

- **Internet eavesdropping**

Prevailing using of internet phone and Skype replaces traditional phone, and enables opportunity of crime through internet phone. Hence, to monitor internet is kind of skill of finding crime evidence, including duplicate and monitor the content of suspect's data package. Sometime it is necessary to decode for encoded package. Therefore, internet eavesdrop is through encoded package exchange system to get the targeting package. However, the transmitting of the internet is different from the traditional phone which uses point to point transmit ion. It should interrupt the information from big scope. Consequently, other people can monitor internet via system of exchanging data package.

- **To monitor e-mail**

Thousands million e-mail are circulating in internet every day, and they are highly possibly grabbed the communication via internet. Because these e-mails relate to commercial or private privacy, this infringement became topic that everyone concern. The invaders in e-mail possibly include employers, ISP companies, or even internet Hacker. I will focus my discussion in whether employers are appropriate in monitor employees' e-mails.

The intention of monitoring employees' e-mail results from different recognition to attribute of e-mail. Employer think employees are using company equipments. They should supervise quality of employees' duty. On the contrary, employees think the content of e-mail belongs to personal privacy. The monitoring of personal e-mail has infringed private right. "Electronic Communication Privacy Act" , ECPA, regulated that system administers can not interfere non-voice message sending unless they have preliminary agreement with internet users. However, system administers can examine data which has been saved, including saved in administers' computers and data is waiting for using, and private talking record between users. Hence, ECPA didn't grant privacy right to internet users regarding message which is in saving status, but system administers can't reveal information to the third party outside administers except law executor.

Infringing of Personal information Privacy

- **Collect personal information as commercial tool**

Site profiles

Many general information Websites and Web storefronts either encourage or require that their visitors register by filling out a form. These profiles generally include contact information, demographic data, and credit card information to make purchases

faster. For a frequent user, this is convenient. For the Website operator, profiles are a valuable source of marketing information, especially when combined with transaction histories built using cookies. These profiles make it possible to match the history with information that identifies a specific individual, like a name, an e-mail address, or a phone number. It is possible that these profiles can be sold repeatedly to third parties. Some sites publish their policies regarding how they use or sell customer data. Customers may have the option to submit their preferences as to how their data may be used. However, these preferences are subject to change without notice, as users of Yahoo found out in 2002. Their personal profiles were reset to allow their information to be used for solicitation by conventional mail, e-mail, and telephone. These new settings would take effect in 60days unless the “opt-out” setting were reset by the user.

- **Spread software which infringes Privacy**

A software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with Spyware. Once it is installed, the Spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers. Spyware is similar to a” Trojan horse” in that users unwittingly install the product when they install something else. A common way to become a victim of Spyware is to download certain peer-to-peer file swapping products that are available today. Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's

Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability. Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising purposes or sell the information to another party. Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers

Cookies

The most common method of collecting data about Internet users started when Netscape introduced cookies in the second release of its Navigator browser. Cookies are now a standard feature in all Web browsers. A cookie is a block of text sent from the Website to the browser on the user's PC, where it is stored. Information that the cookie collects can be sent to the originating Website at a later time. Cookies enable customized interactions between a repeat visitor and Websites. If a Web site stores information about user in a cookie that user doesn't know about, the cookie can be considered a form of Spyware.

Web Bug

A web bug is a hidden graphic on a Web page. Usually, they are used to log various data about the visitors of the page. Like cookies, they can be used to

track user's movements throughout the Web, but they are harder to spot. Usually, the ad banners that are easily visible could be called web bugs, since many use cookies to send information to the server sending the ad. However, web bug is generally used for those graphics that are designed to be as small as possible (1 pixel by 1 pixel). Therefore, the graphics are hidden from the surfer. These graphics are invisible to anyone without software that detects them or without reading the source code of the web page.

Advertisers may put HTML code alongside the URL leading to the product displayed in an ad. The web bug sends the user's IP address back to the advertiser, and this advertiser can recognize user on any site that it serves ads on. The spammers usually send out emails at random with the code from their web server. Therefore, when the people who are spammed open the email, their email client will connect to the internet to download the graphic. The email address is sent to the server, which logs it. This log is used by the spammer to find active addresses to send more spam too. For example, the graphics between these two arrows" ---> <--- "there's a web bug right there; a one pixel by one pixel transparent gif graphic that's impossible to see.

- **Identity Theft**

Identity theft occurs when an unscrupulous person obtains enough of personal information to be able to pretend someone and use identities to obtain financial gain. Internet identity theft is one of the fastest-growing crimes in the U.S. The FTC reported in its Consumer Fraud and Identity Theft Complaint Data that there were only 246,847 complaints filed in 2004. But a report released on April,2006 by the BJS says that 3.6 million households(about 3 %)of all US households had been the victim of at least one type of identity theft during a six-month period in the same year. Therefore, even computer bringing us the convenience, there are some methods use internet as the criminals.

Identity theft via Hacking

This is a direct method of identity theft. The perpetrator intrudes victim's system and steals files. Some of these may include personal information which be used as crime tool.

Identity theft via Phishing

Phishing usually attacks emails that are" spoofed." That is, they are made to appear to be coming from some trusted financial institution or commercial entity. The spoofed email usually asks the victim to go to a website to confirm or renew private account information. These emails offer a link that appears to take the victim to the website of the trusted institution. In fact the link takes the victim to a phony website that is visually identical to that of the trusted institution, but is in fact run by the criminal. When the victim takes the bait and sends their account information, the criminal uses it (just few minutes) to transfer the victim's funds or to make purchases. Phishers are the new con artists of cyberspace. Phishing is increase steeply. The Anti-Phishing Working Group reports that the number of new

phishing messages climbed at a monthly rate of 38 percent in the last six months of 2004. The number of new phishing websites has climbed 24 percent per month since August 2005. And phishing attacks are increasingly sophisticated. Early phishing attacks were by novices, but there is now evidence that some attacks are take by organized crime.

Identity theft via Pharming

The Internet faces the threat of "pharming." This insidious crime does not rely on email bait. On the other hand, it attacks web browsers and the Internet's addressing system. The effect is that even individuals who type a desired Internet destination into their web browser may be redirected to a phony web site, with the same disastrous result as clicking on the phony link in a phishing attack.

I**Spamming**

Recently, the rapid growth in spam had been a non-ignore issue. It creates important cost for industry as well as a annoying, time-consuming and money-consuming for users. The growth in spam had now significantly outpace growth in normal e-mail traffic. According to" MessageLabs" research indicates that companies of U.S lost productivity of $20n one year. This includes the time it takes people to delete the message, the cost of buying larger mail servers and storage system to cope with inboxes flooded with the messages and the cost of having staff unclog networks overloaded by spam. The "McAfee Americans and spam survey" in 2003 identified e-mail spam as the prime technology time waster(49%) by wide margins over other technical annoyances including automated voice response system(24%) and slow internet connections (19%).The survey revealed that 49% of Americans spend more than 40minutes per week deleting spam and 14% reporting they spend as much as three

and a half hours a week on this task

Spam Defense

In addition of the legislative and regulatory defenses, there are several ways individual and businesses can defend themselves against unsolicited e-mail.

Sever-base E-mail Filters

The e-mail filters can be installed at the e-mail gateway. There are several products on the market that can be used with an e-mail server to block suspected spam on its way to the addressee's inbox.

Client-bases E-mail Filters

Client-bases e-mail filters are designed to enhance users' e-mail clients, such as Outlook. Some of these filters work like AV programs in that they subscribe to a data-base of filtering rules that are constantly updated to adapt to new tactics of the spamming industry. Filters can be configured to automatically delete detected spam or divert it to a special folder for further review.

Possible methods to protecting privacy in internet

Self-Regulation mechanisms

***TR*USTe** TRUSTe Make Privacy Your Choice

TRUSTe is a non-profit, independent organization. The purpose is to build up trust and confidence of internet users to internet in order to urge development of internet business. The core business is to offer "Online Seal" which represent the brand is trustable, and is announced in homepage of e-shop. Consumers can understand that the website will limit public circulation of personal information in minimum scope, and know what kind of information was gathered too. The website will notify consumers the scope of information which will be gathered and circulated; enabling consumers

have option right to decide what kind of information is allowed to spread.

- **BBBOnline (Better Business Bureau Online)**

BBBOnline is a subsidiary of the Council of Better Business Bureaus. The program addresses a e-store's privacy practices and how a Website uses personal identifiable information collects from Web site visitors. The mission of the BBBonline is to promote trust and confidence in business transactions conducted over the Internet. The BBBOnLine issues two seals that certify that a Web site has met certain standards:

BBBOnLine Reliability Seal: 

indicates that the company behind the Web presence is a member of a local Better Business Bureau and has met truth in advertisement and reliability guidelines.

BBBOnLine Privacy Seal:

indicates that the company behind the Web presence conforms to baseline information privacy standards.

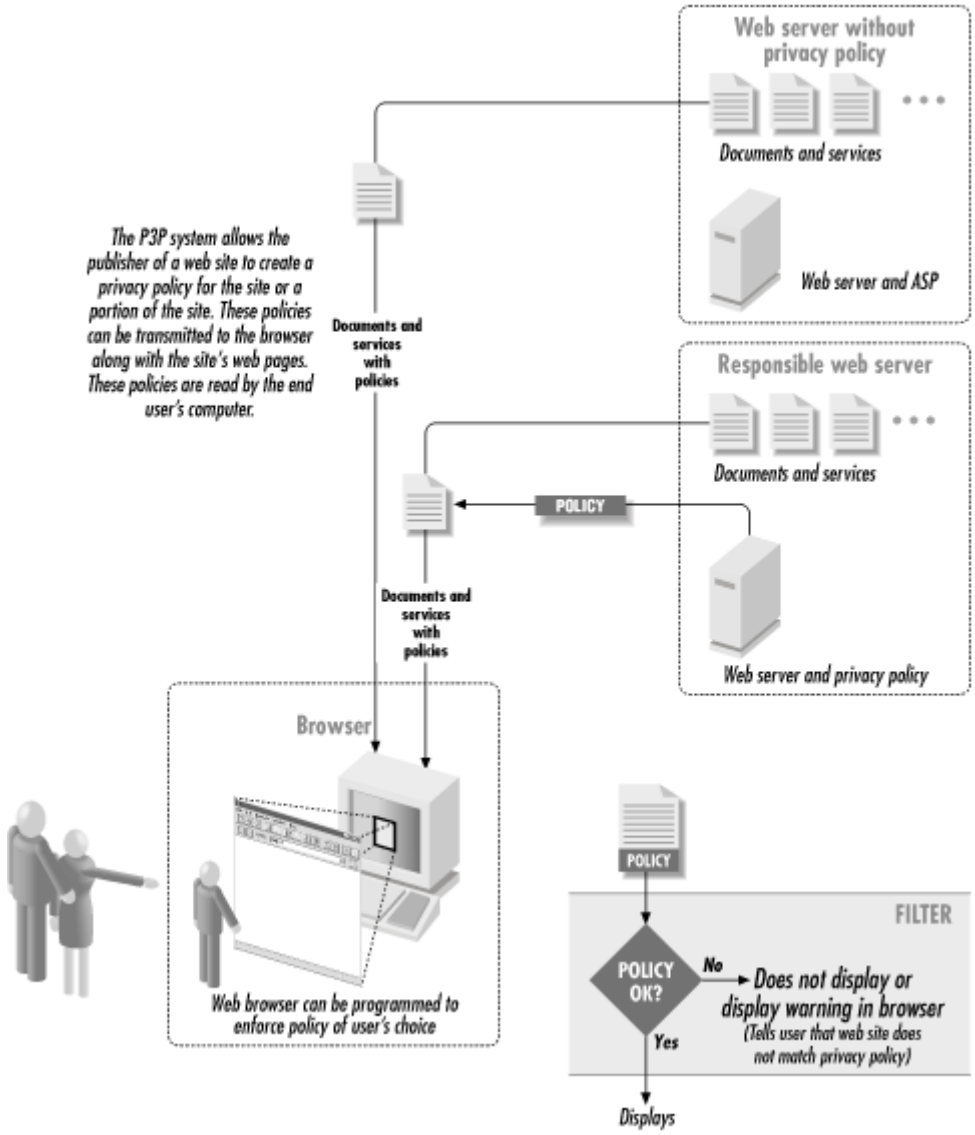
To Utilize high technology device

- **P3P**

The Platform for Privacy Preferences Project (P3P) provides a standard way for Web sites to communicate about their practices around the collection, use, and

distribution of personal information. It's a machine-readable privacy policy that can be automatically fetched and viewed by users, and it can be tailored to fit user company's specific policies. For example, it could reject any cookies from sites that do not have a policy that prohibits sharing of data with third parties.

Figure 1 : P3P process



Support for P3P in Internet Explorer 6.0

Internet Explorer 6.0 contains limited support for P3P. This support is limited to support for P3P's so-called *compact policies* that describe how a site uses information collected

through the cookies. IE6 uses this support to determine whether or not the user should accept a cookie from a given web site.

Internet Explorer's P3P implementation is controlled through the "Privacy" tab of the Internet Options control panel (Figure 2). Using this panel, the user can specify one of seven default policies to use all web sites. User can also modify these policies to suit his own individual desires. Finally, user can specify a list of web sites to be treated with specific rules.

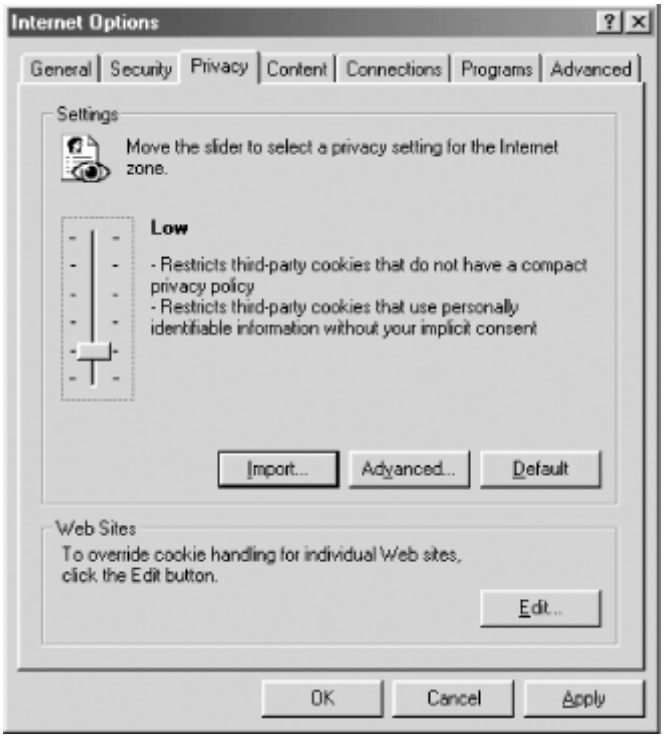


Figure 2: Internet Explorer 6.0 has limited support for P3P in the Privacy tab of the Internet Options control panel.

Internet Explorer 6.0's P3P implementation is concerned with the issue of cookies. The implementation distinguishes between first-party cookies and third-party cookies. The *first-party cookie* is used to refer to a cookie that is transmitted to user’s browser in the header of the HTML page that a browser is viewing. The *third-party cookie* is used to

refer to cookies that are transmitted in the header of included images or frames that come from web sites other than the web site of the base page. In both cases, the browser can be configured to accept or reject cookies depending on if a site has a P3P policy and how the policy says the site will handle personal identifiable information (PII).

Several of Microsoft's default policies are concerned the idea that use "without implicit consent" PII. Generally, it is used to determine if a web site operator collect personal information without asking user’s permission.

Internet Explorer 6.0 can "leash" cookies, so that they are only returned to the sites from which they originated. Cookies can also be "downgraded," so that they are automatically deleted when Internet Explorer is exited. The browser also explicitly makes reference to "session cookies;" that the cookies have been deleted at the end of sessions and are not stored on the computer's hard disk.

- Anonymizer

The Anonymizer provides a technological means for preserving a user's privacy when surfing the web. The basic idea is to set up a third-party web site (http://www.anonymizer.com) to act as a middleman between the user and the site to be visited. For example, when the user wants to view web pages at Apple Computer site, he does not ask his browser to establish a direct Internet connection to http://www.apple.com, but instead asks his browser to connect to http://www.anonymizer.com:8080/www.apple.com. The Anonymizer then makes the connection to apple.com without revealing any information about the user who requested the information, and finally forwards the information received from Apple to the user.

The basic principle of interposing a middleman server between user and web site is for a long time. Indeed, the Internet firewalls used by most companies rely on "proxy servers," which use similar technology to achieve their goal of eliminating direct connections between their employees and the outside net. The first version of the Anonymizer was based on the public-domain “CERN proxy server”, but with several modifications to preserve anonymity:

1. it does not forward the source IP address of the end-user;
2. it eliminates revealing information about the user's machine configuration from the "User-Agent" MIME header;
3. it eliminates the user's name from the "From" MIME header;
4. it eliminates the previously-visited site name from the "Referer" MIME header;
5. it does not forward the user's email address to serve as a password for FTP transactions;
6. it filters out Java applets and JavaScript scripts which may compromise anonymity;
7. it filters out all "magic cookies" which may compromise anonymity; and
8. it gives positive feedback to the user by displaying an Anonymizer header on the page and adding the word "[Anonymized]" to the page's title.

However, the Anonymizer cannot guarantee its users perfect anonymity. The reason is :first, anonymity can be violated through the use of "helper applications," such as RealAudio, which go around the proxy by establishing their own direct net connections. Further, the technical standards underlying the Web are constantly in flux; changes to the HTML language can potentially create new routes around the Anonymizer's automatic link-rewriting mechanism. Nevertheless, in the most of cases, users of the Anonymizer is secure in the Web sites .

To educate internet user

Clear memory cache after browsing:

After the user browse the Web, copies of all accessed pages and images are saved on computer's memory. While these copies make subsequent visits to the same sites faster, the browsing record has grave implications for personal privacy, particularly when the person share a computer or browse at work. Therefore, the user should delete most of online trail.

Keep e-mail private, use encryption:

E-mail is not as secure a medium as many people believe. E-mail can be easily rerouted and read by unintended third parties; messages are often saved for indefinite periods of time. Therefore, some technologies that allow user to encrypt the messages in order to protect their privacy. For example ,the PGP is a popular encryption software.

Opt-out of third party information sharing:

Many online companies provide the user with the option to opt out the list sharing their information. Some companies may enable users to easily opt out, however, more companies make opting out difficult or virtually impossible: addresses are buried or cannot opt-out online, etc. Therefore, the user should protect their information on these on-line companies.

Get a separate account for your personal e-mail:

Usually, the online users do not realize that the employer has a legal right to read all correspondence in their working e-mail account. Even if they send an e-mail from their home, a copy is often stored on their employer's main computer server. Therefore, to get a separate account at home allows the user to protect their personal messages.

Important protect privacy Act Legislated in U.S.A

Since the privacy issue is valued by population, there are some act be legislated which presents important meaning, I will discuss some as follow:

COPPA (Children's Online Privacy Protection Act of 1998)

Generally requires a Web site directed at children less than 13 years of age to obtain "verifiable parental consent" before collecting personal information online from children. The COPPA regulation defines the term" collects" to encompass providing a child with the ability to have an w-mail account or the ability to post to a chat room, bulletin board, or other online forum. COPPA also requires a covered Web site to disclose in a notice its online information collection and use practices with respect to children and provide parents with the opportunity to review the personal information collected online from their children. Also prohibits a governmental entity from obtaining personal subscriber data in a cable TV company's possession absent a court order reflecting a judicial finding that the data sought is likely to reveal criminal activity. Subscribers must be notified and provided with an opportunity to contest the government's claims.

GLBA(The Gramm-Leach Bliley Act in 1999)

The GLBA is the act to protect consumers' personal financial information held

by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions. The first two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. For example, the services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling. The “Financial Privacy Rule” governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies which are financial institutions that receive this information. The “Safeguards Rule” requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also from other financial institutions. For example, the credit reporting agencies receive customer information from other financial institutions. The “Pretexting provisions” of the GLB Act is to protect consumers from individuals or companies that obtain their personal financial information under false pretenses. It means to prohibit the use of false pretenses, including fraudulent statements and impersonation, to obtain consumers' personal financial information(such as bank balances). This law also prohibits the knowing solicitation of others to engage in pretexting. The purpose is cease the operations of companies and individuals that allegedly practice pretexting and sell consumers' financial information.

Safe Harbor Principles

The European Commission’s Directive on Data Protection went to effect in October, 1998, and would prohibit the transfer of personal data to non-European

Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. The European Union, however, relies on comprehensive legislation that requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin. As a result of these different privacy approaches, the Directive could have significantly interrupted the ability of U.S. companies to engage in many trans-Atlantic transactions.

In order to connect these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The safe harbor was legislated by the EU in 2000 which is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Therefore, the safe harbor will assure that EU organizations know that the company provides "adequate" privacy protection.

The safe harbor framework offers a simpler and cheaper means of complying with the adequacy requirements of the Directive, which should particularly benefit small and medium enterprises.

SAFE HARBOR BENEFITS

The safe harbor provides a number of important benefits to U.S. and EU firms.

1. All 25 Member States of the European Union will be bound by the European Commission's finding of adequacy

2. Companies participating in the safe harbor will be deemed adequate and data flows to those companies will continue;

3. Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted

4. Claims brought by European citizens against U.S. companies will be heard in the U.S. subject to limited exceptions.

The safe harbor framework offers a simpler and cheaper means of complying with the adequacy requirements of the Directive, which should benefit to small and medium enterprises.

An EU organization can ensure that it is sending information to a U.S. organization participating in the safe harbor by viewing the public list of safe harbor organizations posted on the Department of Commerce's website (http://export.gov/safeharbor). This list begun on November 2000. It will contain the names of all U.S. companies that have self-certified to the safe harbor framework.

Conclusion

Nowadays our life is deeply influenced by circulation of information. Because of development of technology, it is much easier to gather, process, and utilize personal information. However, when personal information is easily to be evilly infringed and manipulated, personal privacy has been serious threaten and harmed. Hence, the

demand to privacy has been transformed from no interference to that people has right to control, dominate information about their own.

The main infringement to privacy included monitoring e-mail and supervising internet. Because the using of internet is quite prevailing now, it probably is necessary to monitor employee's communication through internet. However, we should carefully consider how to manage the magnitude of monitoring in order to avoid invade employee's privacy.

On the other hand, we start to have some objective institute or organization to re-build people's trust in communication via internet. It enables people has more understanding about release of personal information, rather than purely resist it. Hence, the appearance of these institutes might be seen as that some regulations are gradually built in this simulated society, which orientates positive development of internet.

Reference:

Text book:Linda Volonino,Stephen R. Robinson.”PRINCIPLES AND PRACTICE OF INFORMATION SECURITY” Chapter11.

Textbook:Matt Bishop “Computer Security-art and science”

Slides from guest speak on 30th March

BBBOnline:
http://www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf
Spam: the evolution of a nuisance
http://www.compseconline.com/hottopics/hot_topic_Oct_03/Evolution.pdf

Spyware http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci214518,00.html

Spyware http://www.webopedia.com/TERM/S/spyware.html

P3P http://www.oreillynet.com/pub/a/network/excerpt/p3p/p3p.html?page=1

The Gramm-Leach Bliley Act
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Safe Harbor http://www.export.gov/safeHarbor/sh_overview.html

COPPA http://www.coppa.org/coppa.htm

Web bugs E:\SpywareInfo Web bugs.htm

Guest speaker recommend website:

http://www.privacyexchange.org/

http://www.privacyrights.org

http://www.epic.org

http://www.cdt.org

http://www.privacyassociation.org

http://www.securitypronews.com/news/securitynews/spn-45-20060410IdentityTheft20X

BiggerProblemThanReported.html