GBDe 2006 Issue Group

Consumer Confidence
"Privacy, Trust Mark and ADR"

Issue Group Leader: *Toshiro Kawamura, Executive Advisor, NEC Corporation*

Issue Group Members: *Tomokazu Hamaguchi, President & CEO, NTT DATA Corporation*
Ing. Badlisham Ghazali, CEO, Multimedia Development Corporation (MDeC)
Shigemi Tamura, Chairman, TEPCO

1. Introduction

Since its foundation in 1999, the GBDe has analyzed the elements to eliminate the anxiety and risk on the part of consumers and to build trust for the growth of e-commerce. This effort to the past recommendations for governments and non-govenmental organizations to represent consumer interests.

The GBDe argues that five elements are essential to win consumer confidence:

1. Trustmark
2. Alternative Dispute Resolution (ADR)
3. Privacy Protection
4. Secure Payment, and
5. Reliable Network.

Among these five, the Consumer Confidence Issue Group has focused on the first three elements and issued combined recommendations at the GBDe's Tokyo Summit in 2001. After this Summit, the GBDe concentrated on advocating the recommendations through dialogue with various parties involved in consumer confidence. However, taking recent development in this area into account, it has been agreed that it would be timely to issue additional recommendations.

2. Privacy

The GBDe has adopted two basic positions in recommending policies related to e-commerce. First, to facilitate the growth of e-commerce, the GBDe has been seeking a uniform regulatory and competitive environment. Second, to avoid the burden of unnecessary regulations, it has been seeking a self-regulatory framework with emphasis on "best practice".

In protecting personal information, the GBDe has been consistent with these two basic positions. In the 2001 Tokyo Recommendations, the GBDe set its own guidelines for personal information protection with reference to the OECD Guidelines. The GBDe guidelines were then promoted, especially within APEC, which awarded GBDe guest status in 2004. APEC launched its own "APEC Privacy Framework" in 2005. Before that, in 1995, the EU issued its "EU Directive". This has influenced legislative efforts not only among EU member countries but also those outside of the EU. Even though uniformity of regulation has not been achieved, the GBDe assesses the current situation as satisfactory and far better than the regulatory patchwork approach the GBDe has sought to avoid since its foundation.

The next step in protecting privacy is to evaluate the regulatory efforts so far put into practice. For this purpose, it is important for governments who have implemented privacy protection regulations to share their experience with other governments who have not yet fully taken this step. In essence, they should seek the "best practice in regulation". This will lead to better regulations and improved privacy protection.

As to self-regulation, two developments have come to our attention: Privacy Mark in Japan and Generally Accepted Privacy Principles (GAPP) in Canada and the United States.

Privacy Mark in Japan started as a self-regulatory effort in 1997. The Japanese government enacted the Personal Information Protection Law in 2004. This legislation attracted huge interest, and as a result, more than five thousand businesses have been certified for the Privacy Mark.

GAPP was co-developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

It should be noted that both Privacy Mark and GAPP extend beyond online e-commerce to cover all types of business transactions involving personal information. Also in terms of scope and structure, both present striking similarities, which might be an encouraging sign that businesses can adapt very similar approaches even when operating under different regulatory frameworks.

Best practice gets its power from third-party audit and certification, which are similar in function to ISO certification and the audit of financial data. Businesses face risk in choosing a vendor to process customers' personal information. But using a vendor that

has undergone third party audit and certification reduces the risk of that choice. Also, this enhances the security for consumers.
In addition, governments could promote these measures by awarding contracts to companies who practice third party audits and certification for personal privacy protection.

But self-regulatory efforts face a challenge: the shortage of well-trained specialists. This is more the case for small to medium sized enterprises, since their training costs are relatively higher than for larger enterprises. One possible solution for this shortage is a standardized training program for professional qualification. The qualification itself and the employment opportunities that should come with it will be good incentives for training. Also, a formal training program is not only more cost effective but also provides justification for governments or other authorities to subsidize training for SMEs.

Thus, the GBDe has observed significant progress in the development of a uniform regulatory framework and a self-regulatory mechanism. However, we see still one more hurdle: cross-border activity. As business processes become global, there will be more need for cross-border processing of personal information. However, government efforts have so far focused on domestic operations. The GBDe believes that consumers are entitled to the same level of privacy protection in cross-border transactions.

Fortunately, some international forums have begun to take up this issue. The GBDe welcomes this move and will seek to contribute.

3. Trustmark

The GBDe established it basic position on trustmarks in 2001 with the publication of its Guideline on Trustmark (TM). To facilitate this Guideline, the GBDe has assisted efforts for cooperation among TM programs of each country in various ways. A uniform environment has not yet been achieved globally; however, through voluntary efforts by the private sector, various TM program organizations were established and developed with their own style in many countries and sectors to promote best practices.

3.1. Current Status

This year, the GBDe conducted a global survey to find out how TM service providers have actually worked, based on the information colleted from their websites. An overview of 27 TM providers was obtained. Of these 27, 13 are in North America, 7 in Europe, and 7 in the Asia/Pacific region.

(1) Management Base
When categorizing these TM providers in terms of organizational form and management base, there are 2 main groups as follows:
A. Non-Profit Organization (+ Government Assistance) Model
In Europe and the Asia/Pacific, most TM programs are based upon the Non-Profit Organization (+ Government Assistance) model. Meanwhile in North America, most organizations, except BBB Online and TRUSTe, are managed on a commercial basis.

Most bodies in the non-profit model have a close connection with their governments. However, their assistance is provided in different ways and in varying degrees. Some organizations are covered by public funds for the considerable portion of their management expenses, and other organizations just share the data.

B. Private Profit-Making Model

In North America, eight organizations were established by investment of venture capital, etc. and now provide TM service as a venture business. Two are operated by a security business and by a major online advertising business. In Europe, one TM service is provided in the United Kingdom only for offline advertisement. In Japan, a TM service will soon be provided by a subsidiary of a major Internet advertising agency.

(1) Guarantee

The most common standard for certifying a TM, or what is guaranteed by a TM, is to follow certain Code of Conduct. Most of those of the Model A mentioned above apply this standard and offer an Alternative Dispute Resolution (ADR) service for consumer disputes.

Organizations categorized in Model B have their own certification standard in line with their specialized service. Some bodies are specialized for personal data protection. Some identify and guarantee a site itself as a secured one. Some provide their TM services only to those who agree to ADR settlement in advance. Others provide their TM services to a business which clears financial health criteria.

(2) Other Information Services

Member stores of a major shopping mall and of a credit card company fulfill the required criteria and receive certification from a third party. This is not what is called a "trustmark", but this mechanism can provide some level of confidence to consumers and should be focused on. This service has played a similar role to TM in a broad sense and has contributed to market expansion.

One of major roles of TM is to show business data to consumers plainly and to provide an indication of a proper business. Some TM program bodies provide a rating service for a business' customer service, etc. These efforts can provide an indication for making consumers' own judgment and promote best practices by using a business' reputation. This type of service is expected to grow further.

3.2. Assessment and Issues

It is heartening that independent efforts have developed, in both profit-making and non-profit organizations, in each country and each area. Meanwhile, some new issues as well as remaining problems are emerging.

(1) Assessment of Trustmarks and Information Provision to Consumers

Because of the variety of TMs in the market an investigation is needed to determine whether consumers can identify correctly what each TM certifies.

In addition, the GBDe believes now is a right time to give an assessment of TMs' roles for promoting e-commerce and expanding its market base, from viewpoints of consumers as well as small-and-medium sized businesses (SMBs), considering the actual situation of each nation and area. With regard to these efforts, consumer organizations are expected to take initiative.

(2) Release of Leading Practices

In more countries, TM will be introduced as an e-commerce promotion measure. Releasing what is to be learned from the developed service practices, management problems, etc., makes it possible to accelerate progress towards developing similar global environments for competition and regulation.

(3) Measures for Cross-Border Transactions

In this survey, most of TM services, especially the ones provided by Model A, are confined to a single country or area. The first step for cross-border business growth is, as GBDe has recommended so far, to facilitate the certification partnership between local TM program organizations.

In order to facilitate this effort, TM programs organized by bodies such as direct marketing associations, chambers of commerce, and industry of each country should fully utilize their linkages with overseas partnership bodies.

As for the partnership among TM service providers, the Asia Trustmark Alliance (ATA), founded by four Asian countries, works very actively. A conference has been held annually since the adoption of a Memorandum of Understanding (MOU) in 2003. The GBDe has provided as much support as possible to their activities. As for cooperation at a global level, after some years of discussion, a Global Trustmark Alliance (GTA) is expected to be formed in the near future.

Meanwhile, some services managed in Model B are provided for the entire world. The providers use the English language, which is an advantage when targeting a global audience. In addition, overseas development can be achieved by a base at home, which is a significant advantage for online business. VeriSign and TRUSTe have developed their services globally by establishing bases in each country and localizing each of them.

As cross-border e-commerce has been facilitated, the GBDe has continued to pay attention to such movements and make efforts in obtaining the cooperation of governments and related organizations in order to consolidate the framework for building confidence of consumers.

4. ADR

The GBDe has focused on the potential of ADR as an easy and prompt settlement option for e-commerce disputes between countries with different legal systems, without going to court. For this reason, the GBDe created the Guideline on ADR in 2003. This guideline was issued in the form of recommendations to each of e-commerce businesses; ADR service providers, and governments. The GBDe conducted a direct dialogue with Consumers International for over three years before reaching an agreement. Since then, the guideline has served as a standard when introducing or assessing ADR services.

4.1. Current Status

1. ADR associated with Trustmark

In the GBDe survey on TM service providers, it was asked whether an ADR program is offered or not. Out of 27 organizations mentioned above, 18 bodies provide an ADR service. Most of them have created organized linkages between their Code of Conduct, TM, and ADR programs.

2. ADR other than Trustmark

The survey also asked about ADR services provided independently, and categorized the services into two models as follows.

A. ADR programs provided at the initiative of government agencies or consumer organizations as an extension of a complaint handling program
B. Online ADR (ODR) offering a partially automated dispute resolution system (software) on a website

As for Model B, the survey conducted by the International Conflict Resolution Center, University of Melbourne (2003) shows that there are 115 websites on ODR in the world. B2C e-commerce disputes are handled on 24 of these 115 websites.

Efforts for Cross-Border Transactions

ADR program cooperation has been discussed in the global alliance of TM program organizations. As for bilateral cooperation, two cases are found: North America (BBB Online) and Japan (ECOM) started in 2001 plus North America (BBB Online), and the United Kingdom (TrustUK) started in 2005. Especially in the latter case, the global ADR mechanism will be built effectively by using the technology of the ODR platform.

4.2. Assessment and Issues

(1) Roles of ADR

The combination of Code of Conduct, TM, and ADR is the best practice model, and appears to be an ideal model for promoting e-commerce. This is expected to continue to be introduced in many countries.

In analysing the performance of ADR services introduced after the issue of the GBDe Recommendation on ADR in 2003, the following significant developments can be observed:

1. The best practice is spread in the market by educating the businesses involved through settlement of each dispute.
2. Self-regulation by other businesses is enhanced by publishing complaint-handling cases.
3. Resolution of new complaints leads to the creation a new code of conduct. Rules are flexibly modified without regulation and control.

(2) Dispute Handling and Information-Gathering Function

Under present circumstances, many "ordinary" businesses are located laterally to "good" businesses certified with TM and have active transactions with consumers. Most complaints handled from consumers are about these "ordinary" businesses.

A mission of an ADR program other than TM, especially in Model A mentioned above, is to respond to such actual needs and to bring relief to consumers. This means that ADR service providers may receive a complaint from a victim of a fraudulent transaction. In this case, it is difficult for private ADR providers with no legal force to reach a settlement. However, the information received by ADR service providers is very useful for government agencies and law enforcement bodies. A mechanism for forwarding information promptly from ADR service providers to the related agencies and bodies is recommended so authorities can take action if required.

(3) Issues in Cross-Border Transactions

An immediate problem is to promote ADR program cooperation among multiple nations as an extension of bilateral cooperation.

The ideal mechanism is that a complaint handling and/or ADR is available as a "one-stop" service to consumers without constraints like different languages and legal systems. A discussion of the related issues, from a long-term perspective, is required.

In cross-border transactions, the efforts to detect a fraudulent transaction are more important. It is very difficult to detect fraud targeting an overseas consumer, even if it is a rudimentary trick, because of the jurisdiction barrier. It is also difficult to take measures to prevent the damage from spreading such as shutdown of a website. Some immediate measures, involving the relevant governments and law enforcement agencies, should be implemented for this situation.

(4) Sustainability

In case of Model A, assistance from a business is difficult to provide because business incomes such as a TM fee cannot be expected and because incentives for a business are poor. Therefore, providing a management base, or financial resources, to keep providing ADR services becomes the biggest problem.

There are many cases where a complaint-handling program is covered by public funds for the purpose of consumer protection. However, there are very few cases where governments provide assistance for ADR services and cross-border business issues. It is

necessary to discuss how these services can be offered continuously by governments, businesses and consumer organizations.

Meanwhile, in Model B, the service for handling a large number of disputes semi-automatically has been implemented successfully by a business linked to a large-scale auction site. Thus, a business idea, technology, flexibility, and maneuverability brought by the private sector can be utilized to solve cross-border disputes. The GBDe should continue to focus on the possibility and do something for partnership projects.

5. Other Service for Confidence-Building

Another purpose of this survey is to examine other services related to consumer confidence other than TM and ADR.

5.1. Escrow Service

The basic mechanism of an escrow service is to receive money for payment from a buyer and to wait for a seller to send out an article to the buyer. The seller cannot receive the money until it is confirmed that the buyer received the goods. It is a service to reduce a risk that a seller cannot receive the payment at the same time to avoid the situation "that a buyer does not receive an item even though he/she paid the price": the greatest risk of a prepayment method.

Recently in Japan, an escrow company was established by joint investment of some major businesses, which was triggered by the success of auctions via mobile phone. There are other cases where an operating company of an auction site and a distribution company offer an escrow service. In the United States, an independent escrow company (escrow.com) has offered this service since 1999.

5.2. Insurance and Transaction Guarantee

The paid money is refunded to a consumer only when certain terms are fulfilled. This service is effective as an "ex-post" relief to reduce the risks of a prepayment method. The most common condition among "certain terms" is, as mentioned above, the case where "an item has not been sent even though payment has been completed". The typical service is "compensation" offered in auction sites. This is a similar service to "insurance" that a user bears widely and at a limited level. In some cases, an auction site provides the service internally; in other cases, the service is offered by a tie-up with an insurance company.

"The transaction guarantee" service that is combined with TM and ADR services has also been established. Some of these services are not limited to fraud cases. The pioneers are Guardian e-Commerce and Web Assured in the United States, and Trusted Shops in Germany. Recently Buysafe, which tied-up with an auction site, is growing and, using their service, a consumer can apply for a guarantee by item unit. A similar service (TradeSafe) will be started in Japan in future. These services are designed and provided through the creativity of the private sector. The beneficiaries or users pay the service fee.

From a viewpoint of confidence building in the market, in addition to TM and ADR, the services provided by such businesses should also be focused on. Especially when providing cross-border service, the GBDe hopes that a difference of legal systems among countries will not hamper the competitive development of business especially when providing cross-border service.

6. Recommendations

6.1. Privacy

1. Governments, who have adopted a regulatory framework for protection of personal information, whether by legislation or other means, should share their experiences with other governments. Studying the outcomes of these policies, particularly the unintended effects, will be of great value in developing measures to protect personal information.

2. Results so far show that self-regulation based on best practice is more effective when combined with audit and certification by an independent third party. Government can promote this type of self-regulation by giving preferred status to certified businesses in awarding contracts.

3. Governments and businesses should work together to harmonize rules and regulations for cross-border transfer of personal information.

6.2. Trustmark

1. As for the Trustmark programs which have been started and developed within the past five years, every government should promote establishment and offer developmental support on best practices and management issues for those countries planning to introduce such programs.

2. Trustmark service providers and consumer organizations should share experiences and seek to foster improved information provision of their services to enable consumers to easily understand the differences between providers.

6.3. ADR (Alternative Dispute Resolution)

1. Every government should develop a mechanism for law enforcement bodies to effectively use the information ADR and complaint-handling organizations collect. Furthermore, law enforcement bodies in every country should make an effort to cooperate with each other effectively on a global basis.

2. ADR service providers must also continue to pursue ongoing global cooperation and contribute to carrying out seamless cooperation amongst various nations. Governments should discuss ways in which to provide cooperation of law enforcement bodies and ADR providers and should assist them to promote these efforts.

3. In order for countries to reference other country ADR systems, governments should publish the statistics and case studies of ADR services, especially concerning best practices and management issues.

4. Every government should take care not to hamper the development of private confidence-building businesses offering global services because of the differences of legal systems from one country to another.

In order to carry out these recommendations firmly and effectively, the GBDe will continue to offer opportunities for discussion to trustmark service providers, ADR service providers, governments, consumer organizations and other related organizations.

The GBDe strongly hopes that this discussion will increase the importance and awareness of a global network for building trust in the e-commerce market.

GBDe 2006 Issue Group

Cyber Security
"Threats and Countermeasures"

Issue Chair: *Buheita Fujiwara, Chairman, Information-technology Promotion Agency (IPA), Japan*

1. Overview

Cyber security is expanding its scope within the cyber and real economy. Cyber threats continue to escalate in variation and frequency. Efforts to fight cyber threats have involved a growing number of participants including governments, non-government public sectors, non-profit organizations and private organizations. Activities vary from legislation, public-private cooperation, commercial services and offerings as well as civil voluntary networking. International organizations provide treaties, recommendations and guidelines.

This report gives an overview of some of those activities and efforts, with references reported by some of the survey participants. Based on findings of the case studies, some recommendations are provided to make a better and safer cyber space.

2. Trends of Emerging Threats

Every country within the GBDe survey experiences some sort of threats. Typically, they are categorized into malicious codes, network attacks and network abuses. Malicious codes include computer viruses, worms, Trojan horses, spyware, key loggers, and BOTs. Network attacks typically include intrusions, DoS (Denial of Service) attacks and web defacement. Network abuse includes SPAM, phishing, pharming and network-related forgery.

There are two cases of attacking vulnerabilities. Software developers (e.g. Microsoft) release security updates to patch vulnerabilities for users. An attacker, then, analyzes this vulnerability and develops malicious programs to attack servers or client PCs which are

not yet updated. Usually, the period between the release of security update and the appearance of such attack is more than a month. However, recently, it is gradually becoming shorter and there are many examples with a very brief lead time such as a few days.

The other case is called the "Zero-day attack". An attacker finds a new vulnerability and attacks it before the security update has been released. Such "Zero-day attacks" have been observed many times recently. Information on new vulnerabilities is not disclosed at the time of attack and hence the measure to rectify such vulnerability is not available. The cyber world faces an ever larger danger of software vulnerabilities.

The other point to be observed is monetary damages. Computer attacks are used to disturb the normal usage of computers, networks and data, and compromised web sites are used to send political messages or for propagation purposes. BOT net sometimes causes DoS attacks which result in network choking. Websites are sometimes compromised to show political messages or geopolitical harassment.

Now, offenders work to get real money. Last year the US experienced theft of credit card information in millions. In Japan a man sent spyware with a disguised complaint e-mail to a mail-order house to successfully get the customers' credit numbers. Offenders attack any place where individual information could be available. Tools to intrude can be easily obtained from the Internet, and they are good at inventing social engineering and fraud methods. Threats are next to an innocent citizen's door.

3. Statistics on Threats

Malaysian incident reporting includes "Monthly Abuse Statistics", "Quarterly Summary of Incidents reported to NISER[1] " and "Yearly Report". Taiwan has an "Intrusion Alert and Advisory for Government Agencies". IPA (Information-technology Promotion Agency of Japan) provides monthly and annual computer virus and malicious access statistics, associated with warnings and recommendations. US-CERT [2] publishes monthly bulletin handling vulnerability information. It also provides quarterly report on incidents. These are not specifically statistics on viruses and incidents. Virus statistics are typically provided monthly by anti-virus software vendors. Incident statistics come out from security information services providers.

The other statistical information is network monitoring reports. The IPA and a few other Japanese agencies including the National Police Agency periodically announce findings from network monitoring. Several private players, typically, security information service providers offer network monitoring information and early warning services as a commercial service.

---

[1] NISER: National ICT Security and emergency Response Centre, Ministry of Science, Technology and Innovation, Malaysia

[2] US-CERT: United Stats - Computer Emergency Response Team

4. Countermeasure Efforts against Threats

A type of Public-Private Partnership (PPP) to counter online security threats is active in Taiwan. Taiwan has also established a National CERT called ICST (Information & Communication Security Technology Center), which plays a key role in various activities to fight against Threats.

ICST has formed a network of 13,000 government officials to share and distribute computer emergency alerts and advisory information. ICST has also established a National Security Operation Center (NSOC) and this serves as a key organization in the Security Incident Data Exchange (SIDEx) consisting of government Security Operation Centers (SOCs) and commercial managed security services providers. ICST is also active in training and education, including "Cyber Security Drills," e-learning curriculums and CISSP training to the Government.

While serving mainly government sectors, ICST collaborates with private sectors in terms of SOC, early warning information sharing and security education.

In Malaysia, the National ICT Security and Emergency Response Centre (NISER) has been formed by the Malaysian Government to support the nation's cyber security initiatives. Through collaborations between private and public sector organizations, NISER continuously identifies possible gaps that could be detrimental to national cyber security. MyCERT, a division under NISER is a national CERT for Malaysia that provides incident response services. They have established a National Cyber Early Warning Centre that provides monitoring and detection of potential cyber threats in Malaysia. For information sharing, they have successfully organized ICT Security forums, conferences and exhibitions. NISER, in collaboration with (ISC)2, provides CISSP education and examinations. NISER is also active in cooperation with APCERT and other neighboring countries in combating cyber threats.

In Japan, various public and private entities work jointly and separately. The IPA and NICT (National Institute of Information and Communication Technology) together with AIST (National Institute of Advanced Industrial Science Technology) are the major government-sponsored agencies. All of these agencies are active in ICT security research and development. The IPA is responsible for the IT Engineers Examination, which is the largest examination in Japan.

Besides these government agencies, JIPDEC (Japan Information Processing Development Corporation) is active as the operator of ISMS certification and Privacy Mark authorization. Various industry associations, including JNSA (Japan Network Security Association), JASA (Japan Association of Security Audit) and NRA (Network Risk Management Association) are actively promoting network security and security management.

The IPA and JPCERT/CC jointly operates JVN (Japan Vendor Status Note), which is a website to share software vulnerabilities and solution information as a part of vulnerability information handling and coordination effort. (ISC)2 Japan collaborates with JNSA to promote CISSP.

As seen above, and can be observed from the case of US-CERT and NISCC of UK, there is a distinctive commitment from the Government to information and network security. This indicates that cyber security deeply relates to national and social security. It also affects industry and consumers. Thus, the private sector is also active. An important and interesting point is that the public and private sectors work together in many countries. This is a natural tendency because cyber security is seamless over public and private entities.

5. Cyber-specific Laws against Threats

Cyber specific laws fall into three categories; enabling, prohibition and investigation.

Enabling typically gives legal effect to electronic documents and storage. For example, digital signatures can legally work as real signatures only when legislation provides such judicial capability. Evidence for tax or other purposes can be effective when a specific law defines electronic exchange and storage to be sufficient as evidence. The Digital Signature Act 1997 of Malaysia is a typical example.

Prohibition typically prohibits and punishes computer related crimes. In several countries, electronic data destruction cannot be criminalized under the general law, because it does not destroy any physical matter. Similarly, intrusion itself does not constitute a crime as it does no physical harm. Thus, a specific law is required. The Unauthorized Access Prohibition Law of Japan is a typical example of this type of law. The Computer Crimes Act 1997 of Malaysia is another example. These are the most typical law enforcement against threats.

For investigation purposes Internet services providers are typically required to reserve communication logs for a certain period of time and submit such records to national investigative agencies. As communication services providers are prohibited from divulging communications secrets, specific legislation is required to give exemption. Eavesdropping and network monitoring for specific communication also should be allowed under a jury court's order judged in line with a law allowing special investigation. The Communications Protection and Surveillance Act of Taiwan is a typical example of this type of legislation. These types of laws are prepared to indirectly fight against threats.

6. Non-cyber-specific Laws and Enforcement against Threats

A typical example of non-cyber-specific laws against threats would be the specific articles of penal laws. Penal laws usually handle only material crimes and damages. As

cybercrimes often destroy no physical material but electronic data, no physical damage is generated. However, economically, certain damage may occur.

The Malaysian Penal Code provides such effect with reference to Computer Crimes Act 1997. Article 234-2 of the Japanese Penal Code is another example. Computer operation disturbance itself constitutes a crime even when there is no physical damage. Criminal Code, Chapter 36 of Taiwan is also a similar example.

Besides specific cybercrime legislation, personal data or privacy protection laws also provide some protection. This does not necessarily relate to cyber threats, but cybercrime can often infringe privacy information. Therefore, privacy protection can also be deemed as non-cyber-specific law against threats.

7. Non-Government Regulations or Collaboration to Control Threats

Not many activities other than CSIRT collaboration were reported. Some Internet service providers in Japan control SPAM mail to protect their service bandwidth. SPAM mail control requires mail content monitoring, and it might constitute an infringement of the secrecy obligation of carriers. Yet, protection of network from abuse is a very important issue which every player should seriously think over.

8. Criminalization in Relation to the Cybercrime Convention

The Cybercrime Convention of the Council of Europe calls for eight offenses to be criminalized:

1. Illegal interception
2. Data interference
3. System interference
4. Misuse of devices
5. Computer-related forgery
6. Computer-related fraud
7. Offenses related to child pornography, and
8. Offenses related to infringement of copyright and related rights.

Japan and Malaysia provide legislation for all of these offenses. These offenses are typically regulated by the Criminal Code or cyber-specific laws such as the Communications and Multimedia Act 1988 and Cyber Crime Act 1997 of Malaysia.

The Convention also calls for legislation of six legal procedures:

1. Preservation of computer data
2. Preservation and partial disclosure of traffic data
3. Production order
4. Search and seizure of stored computer data
5. Real-time collection of traffic data, and

6. Interception of content data.

Japan legally provides all of the six procedures. Malaysia is the same, yet some are not officially provided, or on the way.

9. OECD Initiatives to Fight SPAM

The trouble with SPAM grows day by day. On April 19, 2006, the OECD announced a recommendation which urges government and industry to fight against SPAM in international harmonization and public-private partnership. Japan has some laws to restrict SPAM. Efforts from tool vendors and communication carriers take place, but are not really effective. Malaysia reported a detailed domestic and international collaboration to fight SPAM. SPAM continues to be an ever expanding headache among the Internet citizens.

10. Other Civil and Industrial Efforts

Malaysia provided information about a cyber early warning initiative, CEWS (Cyber Early Warning Service), which monitors and detects cyber attacks in the early stage. Malaysia has also held international CERT Workshops and Cryptology Conferences. For information sharing amongst the members, Special Interest Groups and a Mailing List have been established.

Japan reported early warning-related civil activities and Telecom-ISAC (Information Sharing and Analysis Center), and other civil collaborations aimed to share and distribute information among member firms and industry stake holders.

11. Overall View

Countries/economies participating in the survey reported active efforts against threats from both governmental side and private sector side. The public sector side includes legislation and administrative initiatives while the private sector side contains various activities. The most typical activity is CSIRT, and CSIRT has established an international collaboration network. Cyber space is borderless, so the efforts against cyber threats should be international. The social framework, though, is based on each country. Thus, governmental efforts including legislation, administrative actions and national funding are important.

12. Recommendations

Based on findings and observations made following the 2006 survey and related study by the Cyber Security Issue Group, the GBDe would like to give the following recommendations for cyber space participants to fight against threats.

A. Better Awareness of Users

Individual users do not have enough information about the danger of cyber threats. As cyber attacks tend to aim at money, they face a bigger risk of fraud and financial damages. Many Internet users are easily lured by unknown mails and web site buttons, falling victim to spyware and phishing.

Education of users is most important. Japan's METI, the IPA, and Chamber of Commerce run security seminars for corporate users every year all over the country. METI and JNSA also offer Internet literacy classes for citizens in towns across Japan to lecture about the danger in a simple, easy and friendly manner (e.g. using comics and short videos).
This is a typical area where public-private collaboration can work well. It is recommended that every country should have such educational program or activities to improve civil awareness of cyber threats.

B. Law Enforcement

The GBDe has observed that many countries now have legislation against cybercrime. Legislation is not a simple solution. There are areas of conflicts involving human rights and communication secrecy, and a trade off of between deregulation and industrial order.

The other difficulty is that cybercrime can take place regardless of borders, but legislations and jurisdictions are based on a nation-by-nation framework. So, international collaboration and coordination are very important. If an international, seamless restriction and regulation network could be established, it would provide a great boost to efforts to suppress cyber threats.

Information technology evolves day-by-day. Cybercrime technology is also constantly evolving. Hackers invent IT and social engineering methods to commit cybercrime. The important thing to prevent cybercrime is, therefore, to cover any security holes. It is also necessary to ensure better quality through improved software engineering development. An early warning partnership to eliminate vulnerabilities is another potential area of major benefit. The final point is to fill the legislation gaps and holes among countries. Do not create a hacker haven.

C. Damage Control

Completely exterminating cybercrime is impossible, just as real crime cannot be completely suppressed. The next best alternative is to prepare for unexpected attacks and damages.

Prevention is one way. Precautions, protections, detections and preventions should be properly implemented. Tools and services are available. Employ appropriate and effective prevention measures.

Mitigation is the next step. In order to minimize the impact of attacks, it is important to prepare for incidents. Measures to limit the extent of damage include the creation of a

backup to enable rapid recovery. This helps businesses resume with limited loss and system down time. Business continuity planning should also include damage mitigation strategies.

D. Collaborative Fight against Threats

CSIRTs play a key role in the defense against cyber threats in many countries and regions. These include both government and non-governmental CSIRTS. Although they have formed an effective international network, the GBDe would like to see collaboration expand between participants. What the international community and respective national governments should do is to reinforce support for CSIRTS so that they can be more active.

GBDe 2006 Issue Group

e-Government Issue Group
"Summaries of Previous Recommendations"

Issue Group Leader: *Manabu Shinomoto, Senior Vice President & Executive Officer, President & CEO, Information & Telecommunication Systems, Hitachi, Ltd.*

1. Introduction

The GBDe e-Government Issue Group was founded in 2001 and has made the following recommendations:

- 2001: On the adequate conditions of e-Government from the perspective of the relationship between governments and the private sector.
- 2002: On the adequate conditions of e-Government from the perspective of the relationship between governments and citizens.
- 2004: On the development of businesses/citizen-participation systems.
- 2005: On challenges and responses for Open Source Software (OSS) utilization in order to achieve e-Government at lower cost.

After five years, the GBDe considers it timely to summarize the pertinent points of these previous recommendations with the addition of some further external comments and opinions.

Central and local governments are among the most important providers, consumers and content owners in any country. Therefore, governments' progress in moving their operations and services online will help accelerate IT infrastructure development, as well as promote and expand domestic e-commerce.

2. Summary of 2001 Recommendations

In 2001 the GBDe provided recommendations on e-Government from a private-sector perspective.

2.1. Role of Government

The GBDe stated that a government has the following six roles:

1. Provider of public services (the 'vendor' in business sense).
2. Purchaser of materials needed for its operations (the 'buyer' in business sense).
3. Supervisor of law and institution (i.e. 'enabler' for IT society).
4. Collector of taxes, duties and tariff needed for operation of government services.
5. Facilitator of transparency in government processes.
6. Contents holder of large information including valuable statistical information.

2. e-Government Implementation

The GBDe recommendations also listed five key points to clarify the scope of e-Government. These were:

1. Governments achieve public services of higher effectiveness, speed and quality.
   Examples:
   - New type of services may be created as a result of IT utilization.
   - Increased efficiency in a current operation may lead to cost reduction, which create surplus in the original budget (tax revenue), and this surplus may be utilized for further improvement in the operation.
   - Speedier communication between the government and a company may be achieved.
2. e-Government as a showcase of good IT utilization.
   Private companies can deepen their understanding on the advantages of IT utilization by looking at the successful use of IT in the government. In other words, e-Government can function as a showcase for IT utilization that private companies can refer to.
3. Governments promote measures to overcome obstacles to IT society
   Through the process of e-Government construction, governments will become more aware of different problems that need to be solved for successful IT utilization. Hence governments will set out effective measures to solve such problems.
4. e-Government may facilitate IT utilization in private sector
   When the government is digitized, private companies may also promote further investment to, and utilization of, IT in order to enjoy the benefits of e-Government.
5. e-Government construction may nurture IT-related industries and lead R&D
   Since private companies actively join e-Government development projects, IT-related industries should flourish.

2. Conditions for e-Government

Based on above, the GBDe recommended the following 23 points as conditions for e-Government:

1. Establish institutions/systems that allow Government to process private company project requests electronically.

2. Disclose and publicize e-Government information systems except those require limitation to disclosure (e.g. national security matters).
3. Express milestones/roadmap for e-Government construction.
   Governments should clearly state the objectives, substance and the roadmap of any e-Government implementation projects. Governments should incorporate the private sector's opinions when setting such milestones.
4. Establish measures/structures to appropriately evaluate governments' digitization progress. Publicize the results of this evaluation and allow private companies to join the process.
5. Specify "feedback merits" of digitization of procedures.
   Governments should identify what kind of merits private companies can receive from e-Government. For instance, governments may quantify and publicize "reduction in time required for a transaction", or "lowering of commission charge", that occurred as a result of digitization.
6. Utilize private outsourcing.

Requirements to realize e-Government objectives within the public sector include measures to:

1. Enable all administrative procedures to be 100% online, and achieve one-stop service provision, with favorable law establishment.
2. Conduct administrative reform and establish the favorable law institutions to make it efficient.
   Current operations within government agencies should be revised, more integrated and more simplified.
3. Standardize operational forms of central and local governments.
   Enhance simultaneous digitization process in central and local governments.
4. Ensure a secure environment.
   The e-Government system must be securely protected so that private companies can have appropriate access.
5. Carry out measures to facilitate SMEs' utilization of e-Government services.
6. Disclose more information on government services. Speed up the process of information disclosure. The government information should be released on the Internet as quickly as conventional publishing.
7. Create an environment to diversify the means to utilize services.
   e-Government services should be accessible not only from personal computers but also from a range of network-connected devices.
8. Establish methods of speedy resolution of conflicts in transactions between business and Government.
9. Help provide and disclose any information that private companies need in formats that are easy for them to use.
10. Establish a system that assures management of high transparency in any kind of procedure.

To respond to the internationalization governments should:

1. Prepare material in as many languages as practically possible including their own language.

2. Adopt international neutral standard access methods/protocols/specifications/ technologies.
3. Promote adoption of an international (global) standards.
   Methods/specifications used in transactions and procedures should meet a certain international standard.
4. Collaborate with foreign governments to strive for global digitization and international networking.
5. Notify necessary qualifications/standards for bidding, as well as appropriate reasons for setting them.
6. Government operations related to international e-commerce must go online with high priority (e.g. trade/import and export operations).
7. Arrive at an agreement of conflict resolution in international e-commerce transactions.

2.4. Comments

These recommendations generated the following comments, among others, after the presentation.

1. It is important to set appropriate benchmarks for evaluation of e-Government from the point of view of private companies. For instance, the private sector can cite turn-around time for applications or registrations.
2. In some countries, e-Government has not been promoted. The GBDe needs to analyze the causes and the factors, and develop plans to overcome the obstacles from the point of view of the private companies.

3. Summary of 2002 Recommendations

In 2002 the GBDe focused on the promotion of e-Government to citizens, based on the view that the greater e-Government utilization by citizens has a beneficial flow on effect for private-sector e-commerce.

1. Enable 100% of administrative procedures online, and achieve one stop service provision.

Currently, users of administrative services often have to follow separate procedures with different agencies in order to complete one single transaction. e-Government should offer one-stop seamless services that allow users to complete these procedures (e.g. document submission and fee payments) at the same time via an integrated front office window. Partial digitization of current administrative services does not provide a big improvement in user relations with the administration. Additionally, the benefits of digitization for the private sector can be limited if business transactions with governments remain partially manual and offline.

2. Conduct administrative reforms and establish the favorable legal framework.

Operations within government agencies should be integrated and simplified. Mere digitization of current administrative services without business process re-engineering may not provide sufficient results in enhancing the effectiveness of the public sector.

Furthermore, laws and institutions should be adapted to make these reforms possible and insure interoperability across the Government agencies. One of the most important issues here is the legal acceptance of the electronic signatures. Corresponding regulations are required in order to make remote delivery of services to citizens possible.

3. Ensure privacy, confidentiality and reliability for services rendered to the citizens through the Internet.

The e-Government system must be securely protected so that citizens can access, provide and exchange information (personal and transactional data) at ease. We suggest posting clear statements on security measures being taken by governments should be outlined on the web sites in order to reassure the citizens of their privacy and give them confidence in e-Government usage. This will also serve to promote e-services in general.

4. Support the development of the telecommunications infrastructures.

The telecommunications infrastructure needs to be expanded and enhanced, in particular in the "first-mile" with broadband access, and broadband connectivity between Government agencies. State-of-the art solutions should be tested. Provision of broadband and high-quality network security, should be incorporated to encourage development of media rich content.

5. Sponsor the digital literacy of the citizens.

ICT, although a potentially valuable tool, can divide those who own it and use it, and those who do not. In order to make the benefits of e-Government fully available to the citizens, governments should familiarize their citizens with the Internet.

6. Support the establishment of Internet access points.

An increase in number of public Internet access points will contribute to a corresponding increase in number of potential service requesters ("customers") and lower the risk of the exclusion for those citizens who are not connected at home.

7. To create an environment to diversify the means to access services.

e-Government services should be accessible not only from personal computers but also from other technological platforms, e.g. mobile terminals, digital TVs, etc. This is necessary in order to expand the merits of e-Government. Additionally, the provision of network services varies in different countries. Therefore, e-Government should be accessible via various types of user devices.

8. To apply new technologies in the participation and electoral processes to promote e-Democracy.

With the help of online participation, citizens are able to express their views directly to Government. For example, electronic voting facilitates such processes as elections and referendums make it easier for citizens to exercise their democratic rights. This also allows major savings, both in time and money.

4. Summary of 2004 Recommendations

The focus on online access and participation for citizens was further developed in the GBDe's 2004 e-Government Recommendations. From the private-sector perspective increased Government dialogue and interaction with citizens through online means encourages more familiarity and confidence in the Internet. In this sense, e-participation can become an important catalyst for e-commerce in many countries.

In this respect, the GBDe recommended that the public sector:

1. Create a culture of consultation and dialogue.

Improve communication, to bridge the citizen to Government divide. e-Participation should not be viewed as a substitute for existing methods of involvement but should add value to them. The development of e-participation tools should be viewed as an evolving process linked to the confidence and assessment of citizens, representatives and governments.

2. Start with Local Government.

Local Government plays a key role in this process and is the best candidate to drive it forward, since it is really the nearest to citizens real life problems. This is the level of Government that more directly represent citizens' interests.

3. Provide a Citizen Space for consultations and a public forum for discussion,

This space must include a register of Central Government consultations. Citizens can be notified in different ways: e-mail, SMS, etc.

4. Produce e-participation guidelines.

Experiences in e-consultations show that in general, governments do not have clear guidance on making the best use of electronic media in consultations. To tackle with this, it is recommended that a toolkit and mandatory guidance be developed for departments in charge of coordinating these kinds of initiatives.

5. Bring the citizenship closer to the new technologies, through adequate training, support and guidance.

6. Drive pilots, share and analyze experiences, develop policies on the basis of best practices.

7. Pay attention to change management among public servants, since they may feel that decisions in which they were concerned previously are now taken by people who does not have the skills and experience to do so.

8. Security and confidentiality – Reliability and trust are key issues in e-participation.

4.1. Comments on the Recommendations

Following the publication of the 2004 Recommendations it was noted that the public network established for e-participation should have a high standard of security to enable it to be used by the public for private business, especially service payments.

5. Summary of the 2005 Recommendations

As shown in surveys by UN and others, realization of e-Government has been set as national policy in many countries. It is true that it is being realized on national-central level, but it is also pointed that it has not been promoted on local level. One of the causes is lack of financial resources.

In 2005, the GBDe evaluated the application of Open Source Software (OSS) as a solution for improved e-Government. The GBDe identified challenges and proposed measures to encourage further development, with research on the status GBDe-member counties.

5.1. Definition and Features of OSS

OSS is a generic term for software that is allowed to be used and distributed under license agreements which have some common features. The features of license agreements are:

- OSS is free to be distributed and redistributed.
- OSS is licensed for free.
- There is no limit to the objects and uses of OSS.
- Source code must be disclosed and distributed.
- Source code is allowed to be modified.

It is important to note that license-conditions are different for each OSS license in the same way that commercial software is sold under various agreements. In addition, OSS is NOT free software. It is licensed for free, but there are usually charges for additional services such as maintenance, technical support and distribution. Linux is the best-known OSS software.

5.2. Summary of the recommendation

The following challenges have been frequently pointed out; however, the GBDe would like also to offer some solutions:

Challenge 1: Due to the lack of precedents of OSS adoption, the effects offered by OSS have yet to be fully recognized.
Solutions:

- Develop and publish policies at central and local government level to support the adoption of OSS into information systems.
- Establish pilot OSS projects and then evaluate and publish the results of these projects.

Challenge 2: A lack of competitive growth among OSS vendors means benefits of OSS adoption have sometimes been difficult to identify.
Solution:
- Implement a software engineering development policy through industry-academia-government collaboration.

Challenge 3: A lack of investment in personnel training and education, which results from IT vendors' concerns about the negative effects on business activities such as shrinking of the market size, is hampering development of OSS.
Solution:
- Governments should apply savings gained by OSS adoption to IT vendors' services to build the advanced systems.

Challenge 4: The standards necessary to ensure interoperability between OSS systems at a global level have not yet been specified.
Solution:
- Consider the establishment of organizations and develop conferences to encourage cooperation between countries to create the appropriate standards in proper sequence.

OSS is not, of itself, a panacea which will enable the realization of e-Government. As representatives of private enterprise, the GBDe will endeavour to support the efficient and widespread adoption of OSS.

5.3. Comments on the recommendation

Simply changing to OSS will not promote its utilization without establishment of a mechanism in which middle software and application software can be used as OSS. Government must support not only the application of OSS, but also development and circulation of middle software and application software.

The following list contains useful URLs for further e-Government reference material:
United Nations
http://www.unpan.org/egovernment4.asp
OECD
http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/$FILE/index.htm
Global Cities Dialogue
http://www.globalcitiesdialogue.org/default.htm
Brown University
http://www.brown.edu/Administration/News_Bureau/2006-07/06-007.html
Waseda University
http://www.obi.giti.waseda.ac.jp/e_gov/2nd_rankings_en.pdf
Accenture
http://www.accenture.com/NR/rdonlyres/D7206199-C3D4-4CB4-A7D8-846C94287890/0/gove_egov_value.pdf

---

Major presentations or statements of the GBDe e-Government Issue Group:

- Sep.2001 GCD GAM (Melbourne, Australia)
- Oct.2001 INFOS (Ljubljana, Slovenia)
- Nov.2001 e-EU e-Gov. Forum (Brussels, Belgium)
- Mar.2002 OECD e-Gov. Project Meeting (Paris, France)
- Mar.2002 APEC TEL (Hanoi, Vietnam)
- Apr.2002 DOTFORCE Global Forum (Naples, Italy)
- Jul.2002 APEC e-Gov. Forum (Seoul, South Korea)
- Aug.2002 APEC e-Gov. Forum (Acapulco, Mexico)
- Nov.2002 CICC AFIT (Vientiane, Laos)
- Apr.2004 G8 e-Gov. Forum (Palermo, Italy)
- Jun.2004 ADB e-Gov. WS (Bangkok, Thailand)
- Mar.2005 GCD Sherpa Meeting (Prague, Czech Republic)
- Sep.2005 CICC OSS Forum (Colombo, Sri Lanka)
- Mar.2006 GCD Sherpa Meeting (Milan, Italy)

GBDe 2006 Issue Group

"International Micropayment"

Issue Chair: *Chunghwa Telecom Co., Ltd., Taiwan*
Issue Group Members: *Institute for Information Industry, Taiwan*
MDeC, Malaysia
Nihon Unisys, Japan
NEC Corporation, Japan
NTT Data, Japan

1. Introduction

With the rapid growth of the e-commerce market, the demand for micropayment is now rising rapidly. Due to the very nature of micropayment, namely small amounts in each payment and high frequency of transactions, the processing cost and efficiency become key success factors, especially for cross border transactions. In the past year, the credit card companies have started to consider handling micro transactions and, at the same time, e-wallet for micro prepayment is developing relatively fast. A micropayment method called Near Field Communication (NFC) mobile payment has been established in Asia. Nevertheless, for NFC or phone bill-based micropayment systems, set-up costs and high efficiency are still their common issues, particularly for extending transaction services across borders.

The set-up cost issue means that the incurred added fee can not be too much with respect to price of the merchandise. Here the added fee includes tax, agency fee of each service provider, cash transfer charge, and other added cost caused by cross border transaction including copyright license of content and withholding tax. Actually, the cost is always a relative, rather than absolute, amount for merchants or consumers. For instance, if the transaction is profitable and sale amount is huge then the merchants would not think the cost is too high even if the total cost takes up a rather high percentage of each transaction. Similarly, whether the transaction cost is high or not is closely associated with the perceived value and the demand of the consumers.

Generally, the transaction efficiency depends very much on overall transaction flow. As both the number of transaction nodes and connected systems increase, the transaction efficiency for international micropayment (IMP) becomes even more critical.

The current status of IMP in the world was investigated and summarized as below.

- Credit cards are still the most popular payment mechanism.
- There are still excessive payment tools, but their integration is not yet in the picture.
- The European payment landscape is heterogeneous. Money transfer and direct debit dominate in some countries.
- Similar situation is also true in Taiwan. Credit card payment is more popular for general transactions of tangible goods; however, it is not well trusted for transactions in the cyberspace.
- The prepaid and credit card based micro-payments still dominate in the United States.
- The growth of contactless card based payment is significant in Japan.
- Most payment types are still strictly regulated for domestic transaction.
- An integrated monthly phone bill as a payment mechanism is a favorable solution for digital content.
- For cross border transactions, a system integrating various micropayments of the same type is expected to run first.
- In addition to monthly phone bill solution, other micropayments should also be included as part of the integration issue.

2. Study Issues in IMP

To further explore the important elements of IMP, some key issues such as market size of IMP, multiple system integration, ADR, taxation and legal issues are addressed in this report. At the same time, the GBDe has developed some policy recommendations for government and industry to help to create a better IMP environment. For the purposes of this investigation, we investigated the importance of a range of issues in the context of an IMP commercial trial run. The study issues include:

1. System integration
2. Taxation
3. Content and IPR
4. Settlement
5. Consumer dispute handling
6. Risk management.

3. Different payment approaches to IMP--Case study

The payment models can be divided into two kinds according to their payment access method, namely, the remote server model and proximity model respectively. The GBDe studied the phone bill-based IMP for remote server model and NFC IC card based IMP for proximity model. The reasons to focus on phone bill and IC card based are outlined below:

1. Market and technical trend
2. Customer base and need
3. Minimal extra cost for Content Providers
   - Well established billing mechanism
   - Forecast infrastructure developing in the world
   - Low extra handling cost
4. Ease of System Integration
   - Making use of roaming & international settlement
   - Support the international technical standard
5. Ease of use for Customers
   - Simple payment method
   - Convenient and fast
6. Security
   - Well recognized AAA mechanism
   - Chip level security

3.1. Phone bill-based IMP

The cases investigated in this section include Japan, Korea, Taiwan, China and Europe. The phone bill or virtual account based micropayment is quite popular in the Asian region, particularly in Taiwan, China and Korea. All of the IMP issues concerning Taiwan, Korea and China have also been fully investigated through a real commercial trial run.

Europe

Daopay is one of the typical IMP methods in Europe that use a monthly phone bill. Basically, all the customers having a phone can use the payment service. Daopay claims that their service is available in over 250 countries, with most of the linked websites concentrated in Europe and North America. None of the taxes are included in the list price and these vary in different countries. There are two reasons for that - one is that the rate of international phone calls for different countries is not the same and the other is that the tax rate in each country is different. This is a simple system integration issue because all the interfacing systems follow internet protocol and the 128 bits SSL encryption standard. The settlement is processed once each month except for the initial transaction, which is completed within 60 days.

Japan

Until now, there is still no real case for phone bill based IMP in Japan. However, there are phone billbased micropayments such as @pay, PayOn and CoDen which, due to user preference and payment trends in Japan, are limited to domestic transactions. PayOn is for OCN Users (NTT Communications). CoDen is for NTT Communications Users including OCN (an Internet Service Provider). NTT Communications provides not only ISP, but also phone, e-money and several services.

Taiwan, Korea and China
An IMP commercial trial run between Taiwan and Korea is underway, and was scheduled to be launched in October 2006 with the support of the GBDe. Similar trials with China and Taiwan are also in progress and are expected to be set up before December 2006. The issues and policies associated with these commercial trials are summarized below.

System integration
Because all of the existing operating payment systems in the project are following the same protocol, system integration is quite smooth between the Taiwanese IMPC and Korean IMPC or between individual IMPCs and corresponding payment systems. The communication protocol Taiwan, Korea and CNC adopted is https protocol with 128 bits SSL and the data structure is XML. Major concerns during the system integration stage have been the overall user's flow and the responsibility for authentication and authorization. For China trial, the CNC plays both IMPC and CP role. For this reason, they have had to modify their system slightly to meet the common user's flow. On the other hand, the SSL certificate adopted is also one point to concern for system integration. Currently, there are three options. They are:

1. International SSL certificate issued by VeriSign
2. Private SSL certificate issued by individual institute
3. Negotiated proprietary SSL certificate.

On analysis, the international SSL certificates issued by VeriSign are recommended in order to provide the greatest opportunity to extend IMP to other countries.

Taxation
Basically, all taxes are charged additionally, including the withholding tax, and commission fee for each IMPC, except VAT (value added tax). This means that the withholding tax and commission fee for each IMPC are not included in the list price of the goods. Although this is likely to bring about disputes during the transaction flow, it can be solved by clear declaration and notification during critical charging nodes. With regard to VAT and withholding tax, generally, these two taxes are not fixed and depend on the regulation of each country. Fortunately, most countries in Asia impose the same percentage of VAT, i.e. 5%. However, withholding tax is not homogeneous among different countries and IMPCs operated by different institutes.

Content Policy and IPR
Content issues can be divided into two major themes. One is the nature of content and the other one is the issue of extending copyright licenses to foreign countries. According to the GBDe survey, the major content in IMP commercial trial runs are music, games, drama and the content about celebrities in the entertainment business. Popular dramas with local culture features as well as music and the content by superstars are always the most favorite items. Due to variation of regulation/policy in different countries, the content allowed for sale is quite different. For example, the content allowed to be sold in Taiwan might not be allowed for sale in China. Therefore it was agreed to adopt a common policy which requires that any kind of content sold via the IMP website has to be verified and approved in advance by each country. Furthermore, the selling parties

have to comply with related IPR regulation and ensure that all the content is legal for usage in specific countries, even if it might increase the cost of content.

Settlement
The settlement method and its period are closely related to the operational cost and management risk. To ensure the correctness of each transaction, a daily batch check between transaction systems should be carried out. However, to reduce the cash transfer cost incurred by any bank, longer settlement periods such as three months have been suggested. The US dollar is being used as the common currency on the pricing list among the bill settlement for all IMPCs except for RMD in the case of China. The cash transfer rate is referred as the last day of the transaction date.

Consumer dispute handling
Consumer disputes can be divided to two types based on the transaction flow. One type of dispute happens during online transaction and the other type occurs after receiving the bill. Generally, the first type of dispute has to be solved immediately. Therefore a customer service center needs to be set up and work online. The first type of dispute can be further divided into two categories by handling responsibility: one is handled by the content provider and the other by the payment service provider. The former generally has to be solved through cooperation with the foreign IMPC. The latter may be solved by domestic payment service provider. The observation is that most of disputes can be solved through the handling process via the mechanism mentioned above. Additionally, disputes can be still solved through the organization of national dispute handling association such as SOSA, ECOM and BBBOnline.

Risk management
The major risk is caused by the bad debt. Phone bill based IMP belongs to the category of post-payment. The payment risk may be taken by payment service providers and merchants. Although the actual rate of bad debt in each country is quite different, a common policy is still needed. The risk of bad debt is taken by merchants in Taiwan and Korea. However, the risks of bad debt, which can not be verified to be from illegal methods, are still taken by payment service providers and merchants in China. To find a common ground for a consistent policy, the payment service providers will be required to manage the risk and probably will need to reflect it in the commission fee.

3.2. NFC IC card-based IMP

In past years, most IC card based payments were based on the financial debit card. However, because of the growth and promotion of NFC technology, the prepaid e-wallet embedded in the IC card is becoming more widespread. An NFC credit card that supports micropayment is also combined with an NFC chip to extend the applications of the IC card. Basically, the NFC payment solution is similar to the IC card type but it is contactless and can use card readers. So, developing applications combining the IC card and NFC has become a market trend. Integrating the NFC function embedded smart IC card with mobile phone has also become a new fashion. Although the applications with NFC micropayment have been developed internationally, the IC card based IMP with NFC function is still not available except in domestic applications. The big issue of

"International" MP with an IC prepaid type card is currency settlement. A prepaid IC card is an immediate transaction, so it is very difficult to exchange from foreign currency to domestic. (The currency market is also moving dynamically. It is hard to choose the correct currency rate.)

Japan

The typical example is NTT DoCoMo Felica payment service. KDDI also has a similar micropayment solution. The characteristics are summarized below. The typical example is IC prepaid type card service (or chip embedded on mobile phone) on Felica standard such as "Edy" or "Suica".

- Technical Standard: proprietary and called ISO 14443 type C.
- Physical body: embedded in the operator's handset and IC card.
- Scalability: 20 million users at least, about 370,000 merchants as of Aug. 2006
- Tax: 5% VAT
- Commission: charged from merchant.
- Payment method: prepaid e-wallet and contactless credit card.
- Application: e-ticket for train (not only JR), vending machine, corporate ID card or student ID, point accumulation, physical shopping and check in for airline.
- Available area: Japan only and NTT DoCoMo/Au (KDDI) handset and several type of IC card such as corporate ID card, airline mileage card.

Felica uses IC card technology which was developed by SONY. This NFC communication protocol was standardized in December, 2003 as ISO 18092. For example, applications which run on Felica are "Edy", "Suica", "Pitapa" and some other IC cards. Mobile phone service providers such as NTT DoCoMo or Au (by KDDI), embedded this Felica IC chip on their mobile phones. SONY and NTT DoCoMo have agreed to establish a joint venture company of new mobile Felica service. Octopus card in Hong Kong uses the same Felica technology.

Korea

SKT announced an NFC mobile payment field trial through cooperation with Philips on May 17, 2006. The field trial system will provide 400 SKT employees and visitors with NFC-enabled mobile phones to access a variety of NFC applications by simply swiping a mobile phone. The initial applications of the trial include:

- Active Posters, which are smart objects and labels that offer access to embedded content such as ticket information, ring-tones and wallpaper for mobile phones. Users will be able to download ring tone and wall paper by swiping their NFC phones to the poster.
- To pay and access public transportation system by their NFC phones or download schedule of public transportation.

USA

Since December 2005, Visa and Philips have been working together on a major NFC trial which provides services at the Philips Arena stadium in Atlanta, Georgia, allowing sports fans to easily buy goods at concession stands and apparel stores. Additionally they are able to access and download mobile content such as ring tones, wall papers, screen

savers, and clips from favorite players and artists by holding their NFC-enabled phone in front of a poster embedded with an NFC tag. Other partners include Nokia, Cingular, Visa, Atlanta Spirit, Chase, and VivoTech.

Germany
On April 19, 2006, Philips, Nokia, Vodafone and the Rhein-Main-Verkehrsverbund (RMV), the regional public transport authority for the Region Frankfurt Rhine-Main in Germany, announced that, following a successful 10-month field trial, NFC technology would be deployed in a commercial environment. Nokia 3220 mobile phones with integrated NFC technology can now be used as electronic bus tickets and act as loyalty cards for discounts at local retail outlets and attractions. Every one of the approximately 95,000 residents in the city of Hanau can use NFC for mobile ticketing in public transportation, simply with the swipe of their compatible phones.

France
In October 2005, Philips, in collaboration with France Telecom, Orange, Samsung, retailer Group LaSer and Vinci Park, commenced a major multi-application NFC trial in Caen in Normandy, France. During the six month trial, 200 Caen residents will use Samsung D500 mobile phones with an embedded Philips NFC chip as a means of secure payment in selected retail stores, parking facilities and to download information about famous tourist sites, movie trailers and bus schedules.

Taiwan
In Taiwan, the typical example is Taipei EasyCard. The original application was only for metro bus e-tickets. Now, its application has been extended to the parking and bus toll system. In the near future it is proposed to combine Taipei EasyCard with mobile phones. System characteristics are listed below:
- Technical Standard: proprietary and called Mifare contactless protocol.
- Physical body: card
- Scalability: 1.5 million cards at least.
- Tax: 5% VAT included in ticket price.
- Commission: got from bank.
- Payment method: prepaid e-wallet.
- Application: Taipei city metro, parking on metro state and Taipei public bus.
- Available area: Taipei city only.

Other examples are Taiwan money card and contactless credit card issued by Chinatrust bank. Taiwan money card adopts Mifare protocol and ISO 14443 type B (T=CL), a protocol which is adopted for all of contactless credit cards issued by bank in Taiwan.

Malaysia
Designed for multi-purpose application, the MyKad card is highly promoted and enforced by local government. Currently, the multi-purpose card does not yet support a contactless function yet. The related information is listed below.
- Technical Standard: contact card protocol.
- Physical body: card

- Scalability: all citizens of Malaysia should be applied.
- Application: personal ID card, passport, driver license, personal health.
- Available area: Malaysia and Brunei.

The first problem encountered when extending NFC IC card based micropayment to cross border transaction, is the interoperability of technical standards. The solution is either to follow a common technical standard or to support NFC technical standards for all of the client devices and card readers. Additionally, there are still the following issues for NFC IC card based IMP:

- Support of financial organization
- Support of payment service/platform provider
- Support of mobile operator and manufacture vendor
- Support of NFC chip supplier
- Participation of merchants
- Taxation issue for payment of prepaid e-cash

The support of each player depends on potential benefit. The support issue will not be a problem as soon NFC IMP can deliver benefit to all players. Hence, both the technical interoperability and commercial client device ready should be the first issues in the initial stage of promotion.

4. Conclusions of the Case Study

Heterogeneous in technical protocol

The case study of phone bill-based IMP shows that the communication protocol as well as secure process being followed are almost the same, with secure http protocol in 128 bits SSL and XML data interfacing being commonly adopted, although some differences do exist in particular micropayment systems. This situation will facilitate the integration of systems in each country.

Heterogeneous in adding the rising cost from MP to IMP to the beneficiary

All of the costs of MP to IMP will be imposed on the “beneficiaries” in order to keep the consistence in domestic payment operation. The “beneficiaries” here may include the consumer and/or merchant. Furthermore, the taxation rate is not uniform for each country. The GBDe believes that adding tax and processing cost of IMP to the list price of goods is acceptable.

Content access policies for IMP are not unified among countries

The case studies indicate that some differences exist in content access policy among countries. That is, the regulation on access to foreign content and content provision to the foreign people are different. Fortunately, content access for the entertainment field is almost the same.

Future of NFC micropayment, even of NFC IMP, is promising
In spite of existing differences among NFC technical standards, the case study shows that the business of NFC micropayment is growing fast. It is reasonable to be optimistic about IC card-based IMP if an NFC technical solution is clear and more successful business models are realized.

5. Recommendations

Encouragement in taxation policy
High frequency and small amount per transaction are the characteristics of micropayments. The situation is also similar for IMP. High tax imposed on cross border transactions will be a barrier for IMP in the initial stages. To encourage and promote the growth of cross border e-commerce, governments should create an incentive-based taxation environment in which unequal tax is eliminated or reduced.

Creating a more open financial policy
With the advance of e-commerce, more and more players are joining because of the multiform nature of e-business. Besides the financial industry, which deals with real cash transfer, governments should make a more open operational policy for IMP business. Governments should lift restrictive regulations and allow non-banks to enter the micro-payment arena.

Active and effective preventing the cyber crime
Cyber crime not only discourages the willingness to purchase via the Internet, but also increases the operational costs of merchant and payment service providers. In order to speed up the growth of cross-border business, an effective preventive action for cyber crime is very important. Governments should take an active role in fighting rapid and growing cyber crime to ensure privacy online and to protect payment and transaction information.

Unification in technical standard
Some differences still exist in NFC IC card-based micropayment systems in spite of the fact that most of phone bill based micropayment systems follow almost unified technical protocol. To enlarge the market and to speed up the growth of NFC IC card based IMP, the chip and client device should be compatible with all of the NFC forum standards such as ISO 14443 type A, B or C. Additionally, the technical specification of commercialized combi SIM chip should be ready and open as early as possible. The differences among payment systems in technical flow should be negotiated to reach consensus for phone bill-based IMP. To aid the development of mobile NFC IMP, governments should encourage and enable the dialogue and negotiation among vendors, banks and solution providers.

GBDe 2006 Issue Group

Ubiquitous Network Society
"Emerging e-Business Opportunities"

Issue Chair: *Dr. Teruyasu Murakami, Chief Corporate Counselor, Nomura Research Institute, Ltd., Japan*

Issue Group Member: *Dr. Jyh-Sheng Ke, President, Institute for Information Industry, Taiwan*

1. Introduction

The wide spread of the "Ubiquitous Network Society" (UNS) concept is well underway throughout the Internet. This is more prevalent in the Asian region with Japan, Taiwan and Korea all actively developing Ubiquitous Network Society policies. In order for this kind of concept to be successfully implemented, there needs to a framework of support provided by National IT Strategies.

Last year, the GBDe studied the Ubiquitous Network Society from the aspect of future use, services, and potential applications. This year, selected National IT Strategies are re-examined and, with the maturing of the UNS concept, a new business opportunity is discussed. Also, further recommendations are made to enhance the rapid implementation of the "Ubiquitous Network Society" throughout the world. The most productive approach is co-regulation where business seeks to adapt and grow while the Government provides a supporting environment through an effective National IT Strategy.

2. National Strategies and Worldwide Activities Update

2.1. u-Japan

In Japan, the initial framework for the current "u-Japan" strategy was created as "e-Japan", started on January of 2001. At first the aim was to create the world's most advanced IT nation. During the first stage targeted for 2005, the plan was to support the rapid development of a reasonable broadband infrastructure.

In July of 2003, infrastructure building was well ahead of the initial projection and the IT strategy changed course. In July of 2003, the "e-Japan II" strategy was announced, and an increase in usage by everyone was to be the new focus. This shift in Japan's National IT Strategy was one of the first of its kind, where strategy is innovative and dynamic, adapting to changing economic environments. At the end of 2004, with many of the goals of "e-Japan II" achieved, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) announced a new 10-year National IT Strategy was to be launched called "u-Japan".

For "u-Japan", the theme was "Whenever, Wherever, Whatever and Whoever are connected to the Network" and, "Using ICT to Establish a Richness of Ubiquitous Network Society".

In January of 2006, the next 5-year National IT Strategy was created. This time, the plan was to enhance the ICT usage not only through network infrastructure building, but by creating new applications, content as well as usable devices and instruments. This is to be the primary R&D effort between now and 2010. Examples maybe seen in "non-contact RFID IC tag technology-based electronic cash", and "Blog and SNS – Social Networking Service-based information provision"; both well established ubiquitous instruments in Japan.

Japan's IT Strategies are based on the belief that the establishment of advanced ICT mechanisms will enhance the daily life of each citizen and unlock individual creativity. However, in addition to the positive impact of new technology, there are also possible negative societal impacts which should also be considered.

2.2. United States of America

As far as the U.S.A. in general, there is no visible official IT Strategy for the Ubiquitous Network Society. However, as the Internet was born in the U.S.A., new trends and applications continue to create a dynamic market. One recent initiative from the private sector is the concept of "WEB 2.0". Another influential trend may be the increasing use of digital technology in the implementation of anti-terrorism and National Security strategy.

The Internet was originally created to provide communication between the U.S. Government's defense project and associated academic institutions. Because of that, many of the new Internet technologies emerged from the universities. In the U.S., the word "Ubiquitous" is not often heard, but the original use of the word comes from trying to solve the complex computer network connections. One U.S. Academic Researcher noted the following: "Recent years have witnessed a dramatic trend towards ubiquitous computing, whereby very large numbers of casually accessible, mobile or embedded computing devices are connected to an increasingly ubiquitous networking infrastructure."

In principle, the US National IT Strategy may be described as one which seeks to follow a twin path of technological development for National Security combined with fostering

an environment in which business innovation can thrive. In this way the U.S.A. continues to act as an incubator for new ICT companies with cross-border ambitions.

2.3. Korea

Korea has placed a high priority on the establishment of the Ubiquitous Network Society and is one of the most advanced nations in terms of implementation of this concept. In order to promote "Ubiquitous" readiness, Korea's first National IT strategy was called "IT839". The initial base for IT839 was called "e-Korea vision 2006". The term "839" comes from "8 Services", "3 Infrastructures", and "9 Growth Engines".

In 2006, IT839 was transformed into a new IT National Strategy called "u-IT839". This strategy is based on "8" main services. These are:

1. WiBro Service with 2.3Ghz mobile Internet
2. DMB – Digital Multimedia Broadcasting on Satellite and Terrestrial Broadcast Network
3. Home Network – Network within any given home
4. Telematics
5. RFID related Application and Services
6. W-CDMA
7. Terrestrial Digital TV
8. Internet Telephony (VoIP).

In conjunction with these 8 main services, for the infrastructure, there are "3" infrastructure expansions:

1. Broadband Convergence Network
2. U-Sensor Network
3. IP v6 based Internet.

Lastly, there are "9" specific new markets:

1. Next Generation Mobile Network
2. Digital TV
3. Home Network
4. IT System on Chip (SoC)
5. Next Generation PCs
6. Embedded Software
7. Digital Content
8. Telematics devices
9. Intelligent Robots.

Like Japan, Korea has been dynamic in changing its IT strategies to accommodate new trends. The Korean Government predicts if the u-IT839 is successful, then by the year 2010, growth in ubiquitous related businesses will be 14.2% within 5 years time, equivalent to 576 trillion Korean Won in directly related industries, and 266 trillion Korean Won in adjacent industries.

2.4. u-Taiwan

During the past years Taiwan's government has devoted significant efforts to developing competitive ICT infrastructure and industry. As a result, the World Competitiveness Report 2005-2006 of World Economic Forum (WEF) rated Taiwan in fifth position among the 117 countries worldwide. For the past 20 years, Taiwan's IT industry has evolved from an OEM to ODM model, and has migrated to providing the global supply chain management services. Currently, Taiwan's IT industry has obtained the 4th largest market share in hardware manufacturing and OEM business. However, within the IT value chain, the profit margin of manufacturing and packaging has been reduced significantly. Taiwan's IT industry is therefore facing a critical challenge of paradigm shift from a manufacturing-oriented focus to a high value-added services and products focus.

With the convergence trend of consumer electronics as well as information, wireless communication and service technologies, the Ubiquitous Network Society environment has become more apparent. The Executive Yuan (Cabinet) of Taiwan Government incorporated "the development of Taiwan's UNS society" into its major IT policy and designated it as the next stage of the e-Taiwan project. After the planned mission and tasks of the current e-Taiwan project are accomplished by the end of 2007, Taiwan's government will start from users' point of view to develop innovative key UNS services, to strengthen the competitiveness of Taiwan's IT infrastructure and industry.

The key action items of the e-Taiwan project are establishing broadband environment for over 6 million households, as well as developing the services of e-Government, e-business, e-life, e-transport, as well as bridging the digital divide. The goal of the M-Taiwan project is to resolve issues associated with the last mile, and to develop Taiwan's wireless communication industry. For the u-Taiwan project, the key concept is to develop Taiwan as a secure and convenient society, where users will be able to share knowledge and information to achieve their full potential in promoting sustainable development and improving the quality of life. It will also support the design and realization of a people-centered information society, where the secure and reliable flow of information will be ensured.

The Taiwan government planned the following strategic goals and directions for the u-Taiwan project:

1. Plan and develop a Ubiquitous Network Society infrastructure, to make Taiwan one of the 5 leading countries in the network readiness index (NRI) of the WEF. The strategic directions consist of focusing on the human needs as well as technology trends, encouraging social experts and citizens to be involved in the UNS development.
2. Provide 80% of national households with 30 Mbps broadband infrastructure, to enable a diversified class of services such as entertainment, video, conference, monitoring, and context aware services. The strategic directions consist of developing a competitive next generation high-speed broadband network

infrastructure, as well as to leverage industrial resources to develop a u-City for experimenting and demonstrating prototype UNS services.

3. Promote the idea of "Ubiquitous Network Society basic law", and related policies, to strengthen the UNS environment. The strategic directions consist of establishing policy law, enhancing information security, developing citizens' trust, providing fair digital opportunity, and training experts for the next generation networks.
4. Develop key UNS services that fulfill users' requirement as well as to make Taiwan as a leading UNS service demonstration country. The strategic directions consist of developing various life enhancing UNS applications such as applications in food, medicine, accommodation, transportation, as well as education. For instance, Taiwan plans to develop a series of intelligent living space applications. The key idea is to incorporate the IT and the architecture related domain knows how to assist the IT industries providing integrated intelligent living space products or services. In addition, the developed intelligent living space applications and services should improve the life quality and convenience for user users.

2.5. China

China is one of the fastest growing economies in the world. Like many other sectors of its economy, rapid expansion has resulted in China leap-frogging technological generations and emerging as an increasingly important IT market.

This leap-frogging phenomenon is also true in some areas of China's National IT policy. Earlier in 2006 China enacted one of the world's most strict SPAM laws (effective on March 30th). Although, Chinese per capita Internet usage ranks it below the world's top 30, the total number of users is far above that of Japan for example. As the benefits of economic growth are spread inland, the potential for e-commerce will grow exponentially.

Aware of this potential explosive growth, the Chinese Government is working on many different aspects of the law to govern and protect the Internet usage. In early summer of 2006, China held a Government-sponsored symposium discussing the creation of privacy law in China. The most notable aspect of this symposium was that domestic and foreign industry representatives were invited and encouraged to voice their opinions. The willingness to support continuing dialogue and the establishment of a "Privacy Law" may herald a significant attempt to begin a process to establish a comprehensive National IT Strategy.

Another major development in 2006 was the news that the Chinese Government would not allow any manufacturing or sale of PC equipment without a pre-installed operating system. This was seen as an important development in attempts to reduce the number of illegal copies of PC software.

2.6. Europe

In Europe, the overarching IT Strategy for the European Union is known as "i2010".

The focus of "i2010" is based on the convergence of industries to support the EU's emergence into the Ubiquitous Network Society. These are:

1. Telecommunications industry
2. Internet service providers
3. Media and content providers
4. Internet user communities.

The convergence of these four industries is expected to create further technological innovation, employment and emergence of new markets. i2010 is also known as "A European Information Society for Growth and Employment" with a key aim being tho create more employment and e-business opportunities.

Recently, there was an "i2010" conference among EU members entitled "Towards a Ubiquitous European Information Society". This marked one of the first times the term "Ubiquitous" had been used in this way in a European context.

3. Emerging e-Business in Ubiquitous Network Society

Many of the impacts of the UNS on society are not yet known. However, much of the initial focus has been finding a balance between a nation's desire to protect its citizens by electronic monitoring and the rights of individuals to a degree of privacy. This debate is still in its initial stages but it is likely to become one of the defining issues surrounding the implementation of the Ubiquitous Network Society.

One of the technologies which has generated significant discussion to date is RFID (Radio Frequency Identification), sometimes known as Smart Cards or Contactless Cards. The GBDe has noted some current cases involving RFID applications and also new devices and the possible impact on business.

3.1. RFID IC Tag Use For Child Safety

Protection for children is unfortunately becoming a growing concern in many parts of the world. Concerns include accidents travelling to and from school, and even include the possibility of kidnapping. There are a number of instances where schools have begun using RFID Tags for the purpose of locating and tracking pupils.

In Japan, there is a cell phone called "Kids' Cell" which is used to locate a child's position using the phone itself and GPS when the signal is receivable. Parents may use an Internet application available from the cell phone carrier to browse the web for the location information. This phone is specifically designed, that the unit cannot be powered off, unless a supervisory password is entered.

In 2006, the mechanism to locate child activity was further expanded with visual sensor networks (VSNs) and ubiquitous devices. In this example, a child is equipped with an active and passive type RFID IC Tag. A sensor at the school's entrance gate, for example, will electronically monitor entrance and exit and transmit this information to parents. Alarms may be triggered if any child is overdue.

By October 2006, there were some 219 examples child safety mechanisms using UNS technology in Japan. Some have been initiated and driven by the P.T.A. – Parents and Teachers Association, and some by the town and city level local government. Also, some universities and colleges with engineering or technology laboratories are providing the service as a part of their research and development expenditure.

3.2. Mobile Ubiquitous Devices – Cell Phones

Japanese cell phones have already becoming ubiquitous devices. These phones have changed their shape several times since being introduced as a simple mobile phone.

In February 1999, NTT Docomo introduced the "i-Mode" Cell Phone service, where web browser and internet e-mail were incorporated into the cell phone. Two months later another Japanese carrier – now called KDDI - introduced a similar service called "EZ-Web", which did the same.

i-Mode and the mobile phone services it inspired created a distinct monetary collection and exchange service. It was seen that content access could be charged to the phone carrier and added to the cell phone subscriber charges. This in turn transformed the mobile telecommunications provider into a micro-payment collection service.

The next major cell phone development related to the UNS was the rapid evolution into a key personal entertainment device featuring:

1. Incorporation of the digital camera capability
2. Promotion as a music and video playing device with networked download capability.

The natural evolution was to embed a credit card onto the same device. Soon, the cell phone became:

1. Voice communications device
2. Internet browser
3. e-mail terminal
4. Digital camera
5. Video and audio content display terminal
6. e-Cash and Credit Card.

This qualifies the cell phone as a fully ubiquitous-capable device with "Wherever", "Whenever", and "Whoever" capacity.

New developments include the addition of biometrics devices such as finger print recognition. The IC chip's spare memory region is being used for purposes such as e-Key

to open electronic locks for building access. Functions such as the incorporation of e-Pass and e-Ticket for transportation are also practiced widely throughout the world.

One of the most recent additions is a digital TV Broadcast receiver. This function has nothing to do with either the cell phone network or the Internet, but the digital receiver was added to show the digital TV content. With these additional ubiquitous functionalities, one person's everyday life maybe compacted into this ubiquitous cell phone.

3.3 Music and Emerging Businesses

Electronic delivery of legitimate music content was hampered during the Internet's first phase of commercial development by cost and download speed issues.

However, Apple Computer's iPod and linked iTunes service was based on a reasonable fee, and music-listening device was able to establish a successful business model.

One new marketing development involving the iPod involves the ability to read data collected by sensors embedded in running shoes for those with active lifestyles. The availability of this feature requires a combination of ubiquitous network technologies:

1. Sensor device
2. Intermediate data collection device
3. Data gathering and transport interface to the Internet
4. e-Business server at sporting goods company.

With the spread of the ubiquitous network, a combination of network-enabled devices and applications are able to gather information directly from specific sets of consumers. By incorporating these ubiquitous network technologies, marketing research firms can undertake increasingly sophisticated consumer purchasing and product studies.

3.4 Social Networking Service – SNS and Blog

During the past two years the terms SNS - Social Networking Service, WEB Log – Blog, and Web 2.0 have become popular to describe new user-based Internet activities.

With the use of SNS and Blog, an individual can easily create their own sub space on the Internet and share content with others. The basic difference between SNS and Blog could be said, as Blog is an individual journal with only one person responsible for content. However, an SNS is a community of users all contributing to the development of content. Business may benefit from establishing links to some specialized or particularly influential SNS.

An illustration of this concept is "Google Map", where the Search Engine site is providing APIs (Application Program Interface) so that anyone on the Internet may access and manipulate the original Map Data for other subsequent usage, which could be public, semi-public, or private.

Web 2.0, refers to second-generation of Internet-based services — such as social networking sites — that let people collaborate and share information online in previously unavailable ways. It differs from early web development in that it moves away from static websites, the use of search engines, and surfing from one website to the next, towards a more dynamic and interactive World Wide Web.

Potentially with Web 2.0-type concepts, along with the growth of SNS and Blogs, new e-business opportunities may arise.

3.5. RFID Impact – Bank Loan Example

In Japan, the economy is believed to be in an upward shift. With positive economic signs, financial institutions are seeking to expand commercial loans.

In the past, traditional collateral in the form of property has been a limiting factor for financial institutions seeking to extend commercial loans to small and medium enterprises. However, one bank in Japan has overcome this problem with the help of ubiquitous technology.

The specific case involved a pig farming business which was seeking to obtain a loan from a local bank but was unable to meet normal collateral criteria. Instead, the farm sought to provide the pigs as collateral but for this purpose it was important for the bank to establish exact numbers and the health of the stock. The solution was to provide each of some 10,000 pigs with a unique IC Tag on their ear. IC Tags are scanned every month to identify every pig. In this way the business was able to both secure a 200,000 Japanese Yen loan and also improve production with the application of accurate and up-to-date livestock data.

3.6. Other RFID Initiatives

Market forecasts indicate RFID will likely enter common usage within the next 10 years. Therefore, the challenge now is how to make RFID indispensable for a wide range of automated data collection and identification applications, especially when the ROI from RFID implementation is not yet apparent.

In line with the UNS Strategy for next generation development, the Taiwan Government has committed to the advent of RFID applications. The aim is to make Taiwan the powerhouse of RFID industry worldwide, and to revolutionize the convenience and security in the living environment.

The significant advantage of RFID systems is the non-contact nature of the technology. RFID tags can be read in challenging circumstances at remarkable speeds, in most cases responding in less than 100 milliseconds. Developments in RFID technology also continue to yield larger memory capacities, wider reading ranges, and faster processing. The read/write capability of an active RFID system is another advantage in interactive applications such as work-in-process or maintenance tracking.

In the last few years, there have been a number of initiatives involving RFID applications in Taiwan, such as RFID for Emergency Medicare, SARS Alert via RFID/Location-Based Medicare Service, RFID-enabled Outpatient Clinic System. The advances in RFID applications are set to close the technology gap, to improve safety, and to support better decision-making in the coming Ubiquitous Network Society. A major SOA project in Taiwan, iCare, is also expected to deliver an innovative model later this year, seeking to become a blueprint for service to senior citizens and those with disabilities.

In order to drive adoption and bring RFID down to the individual item level in Taiwan, at least two comprehensive projects of RFID applications in the public domain (i.e. food, agriculture, pharmaceutical and healthcare industry) will be scheduled for implementation by 2013. The plan is to use 3 billion tags for agriculture/produce (NT$12 billion) by 2013; 1.5 billion tags for food (NT$6 billion); and 0.5 billion tags (NT$2 billion) for healthcare industry. By 2013, public domain initiatives in Taiwan are expected to drive RFID demand to NT$20 billion.

Pilot studies in the private sector are expected to create another NT$5 billion market value in RFID applications. Extensive research centered around RFID technologies will also help industries gain competitive edge and are expected to create another NT$45 billion market value. By 2013, Taiwan is aiming for 10% of the global RFID market share, with at least two among the top five global RFID products/services developed in Taiwan. The total of RFID market value in Taiwan is expected to reach NT$70 billion.

One of the core initiatives launched in 2006 is a 3-year action plan to develop an RFID Enabling Application Platform (REAP) by 2008. The project is making progress to address issues in RFID development, including data collection/filter, standards, event management, device management, real-time process management, security and infrastructure. The platform is expected to help drive cost reductions and increased RFID adoption across vertical markets.

4. Conclusion

The term Ubiquitous Network Society is becoming widely accepted world wide as a means to describe the next phase of the commercial development of the Internet and growth of e-Business. As the infrastructure required for the UNS is installed, particularly in Asia, new business opportunities are being actively identified. The GBDe will continue to monitor and promote three major themes in future:

1. National IT Strategy

First of all, a national IT strategy must be shared and understood which defines the UNS for a particular economy and develops a coherent framework for its implementation and goals to be achieved. National IT strategies which explicitly refer to the UNS at present include “u-Japan”, Korea’s “u-IT839”and“u-Taiwan”.

2. Exponential Growth in User Interaction

Secondly, the establishment of the UNS promises to exponentially increase the amount of communication and information flow over networks. In this way consumers will be able to identify and purchase products in a range of new ways aided by almost real-time information. This provides a tremendous opportunity for business as well as placing greater demands on manufactures and retailers to improve customer service.

3. New Frontiers

Third, as has been seen in Asia, the deployment of UNS technologies is only the beginning of the emergence of a new e-commerce paradigm. The convergence of digital technologies and the incorporation of new data collection capabilities within networks will create new opportunities which are only now starting to emerge.

The GBDe has been seeking to generate increased discussion worldwide about the concept and potential impact of the Ubiquitous Network Society for three years. During that time the concept has started to become a talking point in Europe and the US as well as in Asia (where it originated).

The GBDe believes it is important to continue to discuss the societal issues and business opportunities arising from the establishment of the UNS. This discussion will be instrumental in determining the future international environment for e-business.

** ** ** **