



Global Business Dialogue on Electronic Commerce

GBDe 2007 Issue Group

**Consumer Confidence
“Reflection of Alternative Dispute Resolution,
Trustmark and Privacy Activities”**

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

*Issue Group Members: Tomokazu Hamaguchi, Senior Vice President and Counselor, NTT Data Corporation
Shigemi Tamura, Chairman, TEPCO
Ing. Badlisham Ghazali, CEO, Multimedia Development Corporation
Dennis McGuire, Chairman, TPI*

GBDe’s Consumer Confidence Issue Group has released various recommendations over the last nine years, with many recommendations adopted by governments and related organizations, including APEC, OECD, and ATA. In the era of WebCommerce2.0, however, a new perspective is needed. This year we have focused on a reflection paper that highlights new issues to be discussed in the coming years rather than a rough-and-ready recommendation. In particular, considering the issues from an outsourcing point of view is new and will add depth to future discussions.

1. Alternative Dispute Resolution (ADR)

This chapter discusses “International Consumer Advisory Network,” which will be the first step to realizing cross-border ADR in the future. We will initiate a global dialogue on this and evolve it into a recommendation after the summit.

1.1. Background

GBDe has consistently highlighted how significant dispute resolution is in e-commerce. In 2006, GBDe surveyed how ADR in each country has developed and learned that in addition to the financial burden of ADR, one difficult issue remains. That issue is the response to dispute resolution arising from cross-border transactions.

This year, GBDe considered what it takes to build market confidence by focusing particularly on the global cooperation among ADR providers and analyzing the current status.

1.2. Current Status of Global Collaboration in ADR

ADR global collaboration started with the creation of bilateral partnership agreements. The first bilateral cooperation was formed in 2001 between BBB (U.S., Canada) and ECOM (Japan), and now EC Network has taken over as BBB's partner. In 2005, BBB (U.S., Canada) concluded a partnership agreement with TrustUK (U.K.) as well. Although these joint activities provide complaint handling services rather than ADR services, they have provided a certain level of effective resolution to cross-border problems for consumers.

Only a limited number of nations have concluded such bilateral agreements at present. Nevertheless, the need for collaboration is expected to increase. For example, about 20% of the complaints filed to EC Network from Japanese consumers are related to cross-border transactions. And cross-border purchasing is likely to continue expanding from the U.S. to Europe and Asia.

Recently, online complaint handling has been promoted as a way of providing more effective services. With the web-based Online Dispute Resolution (ODR) Platform, after a consumer files a complaint, a message is sent to the other party by an automated email system. BBB developed this system with the support of the United States government and uses it with TrustUK. The online system helps to eliminate the time and effort involved in conveying complaints to another party. More focus on responding to fraudulent cases, which make up the largest number of filed complaints, and on automatic translation of different languages would make the system more effective.

ADR collaboration has also been considered within the Trustmark Alliance. In general, however, the ADR program provided by trustmark certification bodies is available only to businesses holding a trustmark, which means that the programs do not always cover all complaints and disputes arising from cross-border consumer transactions.

Econsumer.gov, a joint project by law enforcement agencies of 21 different countries, has a complaint report form available on its website (<http://www.econsumer.gov/>) that can be used by consumers living anywhere in the world. At present the form is available in seven languages, and anyone who can read and write in one of these languages can submit a complaint via the website. The complaints posted on this site become shared data among the participating countries' law enforcement agencies, but they do not provide redress to individual cases. Cooperation with ADR services was considered and executed as a pilot project in 2003 and 2004 and is still in the testing phase. At this point, the site's main involvement with ADR is publication of an international directory of ADR providers.

The most-watched initiative is the regional network known as European Consumer Centers Network (ECC-Net), to which 26 European nations have joined. In 2005,

European Consumer Centers (ECC) were established in each country with funding from the European Commission as well as its member countries. For cross-border consumer transactions, the ECCs systematically provide a complaint handling service and related information upon request to consumers. ECC-Net is designed as a flexible and effective scheme, offering services by phone and email as well as in translation.

1.3. OECD Recommendation on Consumer Dispute and Redress

Recommendations issued by OECD in July 2007 propose that each economy “provide domestic frameworks for dispute resolution and redress.” As for cross-border complaints, the OECD recommendations propose to “provide clear information,” to “expand the awareness of justice system participants,” and to “minimize legal barriers to applicants from other countries.” The recommendations also point out the necessity of “private sector cooperation” and “collection and analysis of complaints filed from overseas consumers.”

GBDe is trying to devise a practical framework to realize the OECD recommendations.

1.4. Framework: International Consumer Advisory Network (tentative)

The new framework proposes that governments designate consumer advisory service providers, to be called Consumer Advisory Liaison Offices (CALO), and that CALOs around the world build a loose network. This is abbreviated as “ICA-Net” here.

The primary role of CALOs is to receive inquiries on cross-border disputes from domestic consumers and to provide information and advice to those consumers. In addition, if necessary, a CALO may contact the CALO in the country where the supplying business is located, and both CALOs will work jointly to handle the complaint. When it is difficult to handle a complaint in a consumer’s own language, the CALO in the consumer’s country will translate the complaint into English and convey it the other CALO.

Another role of CALOs is to receive complaints related to domestic companies from overseas consumers via the CALO in the country where those consumers live, and to provide support to settle issues and disputes effectively. For this purpose, CALOs are expected to collaborate with relevant organizations in their respective countries, such as ADR service providers, business associations, consumer groups, trustmark service providers, and law enforcement entities.

The basic framework is the same as what has been developed under bilateral collaborations, such as between the U.S. and Japan. The objective of the new framework is to extend the same activities to multilateral collaboration. Another aim is to approximate a solution through cooperation between domestic organizations for cases that could not be resolved through complaint handling and ADR providers. These purposes and activities are exactly the same as those of ECC-Net.

In order to participate in the ICA-Net, commitment from each country’s respective government will be required. This is because past experience with global

collaboration shows that many complaints from overseas consumers cannot be solved without involving organizations that have compelling force. According to the circumstances of each country, different organizational forms are expected to participate in the network as CALOs, including government agencies, private consumer associations, and ADR providers. An important role of each government, however, will be to organize a system in which effective investigations can be conducted and adequate support provided for the settlement of complaints posted from foreign countries. It is each government's responsibility not to let their country become criminal or the den of illegal business enterprises.

Multilateral operation will present some challenges. For instance, standardizing the CALO certification and protocol of complaint transactions might be a barrier to participation in the ICA-Net for countries still new to e-commerce. It could also raise the management costs of the network. Moreover, management costs and issues of privacy and data protection will grow significantly when consultation/complaint data are consolidated into a single database. It is therefore preferable that ICA-Net be created as a loose network in which voluntary participation is possible from anywhere in the world, and that it be decentralized so as not to generate high management costs.

The following chart depicts the basic concept of a troublesome case between a consumer in country A and a business in country B as handled by ICA-Net.

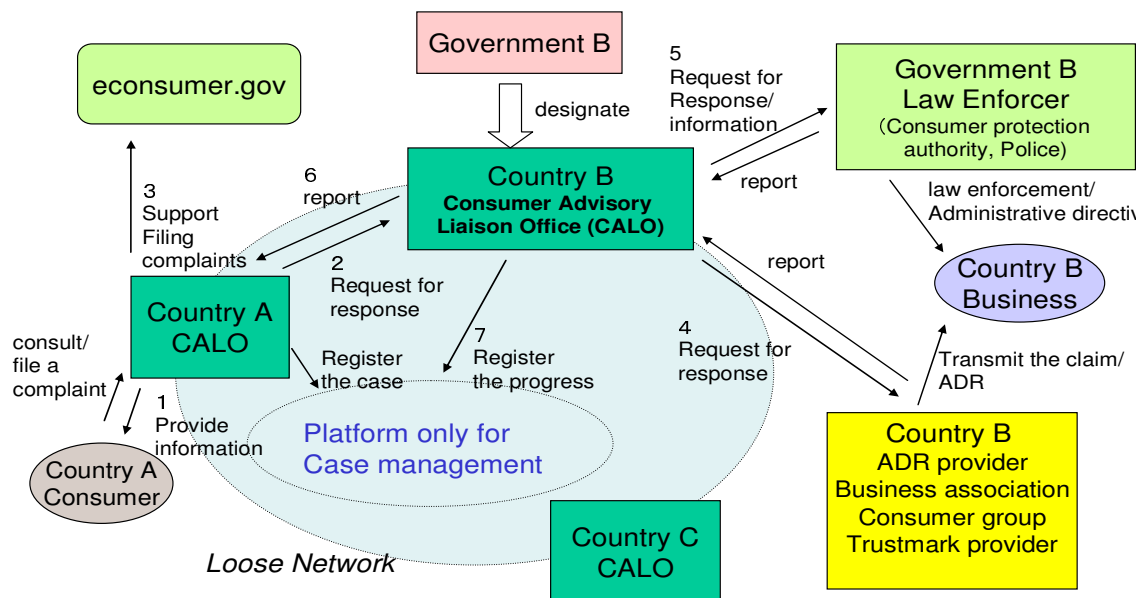


Figure 1 - International Consumers Advisory Network

The role of CALO in country A: support to the consumer in country A:

- CALO receives inquiries from its domestic consumers, and provides advice on legal matters, ways of trouble settlement, and system or agencies available for dispute settlement.

- When a consumer files a complaint to the said business, CALO translates his/her complaint into English, reports it to the business, and gives feedback to the consumer.
- For complaints other than transactions, such as lottery, gambling, Spam, or identity theft, as well as cases where the location (country) cannot be identified, CALO recommends reporting them through the site of e-consumer.gov.

The role of CALO in country B: correspondence to the business in country B:

- When a complaint is filed to a domestic business through an overseas contact point, CALO asks for a response, depending on the nature of the trouble, to an industry group, a self-regulatory scheme (trustmark, etc.) or the shopping mall where the said business belongs. Or CALO might make direct contact with the said business.
- Cooperation by law enforcement institutions is called for when the contact information of the business is not known, when there is no responses from the business, or when there seems to be breach of law.
- CALO reports the result to the CALO in the consumer's country.

Information management:

- The platform for case management is used to manage only the progress of a complaint settlement exchanged between CALOs, not the content. By allowing the progress report to be seen by CALO of a third country, it is expected that peer pressure will accelerate prompt action for complaint settlement.
- The data stored by the CALO in each country should be analyzed based on its responsibility and used to gain awareness of marketplace trends and provide information to prevent consumers from becoming involved in trouble.
- Universal standards are necessary for handling of personal information and trade secrets.

1.5. Recommendations

In 2007, GBDe Consumer Confidence Issue Group discussed the cross-border ADR issue several times at a workshop with several Japanese experts and drafted the above framework.

GBDe makes the following recommendations for country governments regarding the framework:

- For the protection and redress of domestic consumers in global e-commerce transactions, the current status should be checked and systems organized.
- Following OECD 2007 Recommendations, domestic systems to provide redress for overseas consumers should also be organized. Before doing so, complaint data filed from overseas consumers should be collected and analyzed in cooperation with the private sector.
- To build overseas consumer confidence in the domestic e-business environment, the creation of an International Consumer Advisory Network

(tentative name) should be discussed at global intergovernmental conferences, such as OECD, APEC, and ICPEN. The U.S., Japan, and the European Commission, which are ahead of other countries in the development of e-commerce, are expected to play a leading role in this discussion.

2. Trustmark (TM)

This chapter reports the results of investigation and analysis of existing trustmark organization in Europe, which follows the previous investigation in the Americas in 2006. In addition, this chapter covers the current status of the Asian Trustmark Alliance and countries in the Asia-Pacific region.

2.1. Common Criteria of TM Accreditation

GBDe has been recommending the necessity of common criteria for TM accreditation since its beginning. The Asia Trustmark Alliance (ATA) aims to accredit TM based on common criteria, while also considering and comparing each member country's existing TM accreditation criteria. As a result, they decided to adopt GBDe's guideline for the future mutual recognition this year.

It is recognized that the countries which start TM accreditation should refer to this guideline, ATA Guideline for Trustmark Operator (GTO). Without adopting one particular member country's common criteria, adopting the GBDe's common criteria for TM accreditation established from a neutral perspective apparently helped lower hurdles for new member countries of ATA mentioned below. The GBDe TM accreditation guidelines can be found in Appendix B.

2.2. Expansion of ATA

ATA was originally formed by Singapore, Korea, Taiwan, and Japan, but this year the United States, Thailand and Mexico also joined. The Malaysian government is considering establishing a TM accrediting organization as well.

Although previously ATA only accepted non-profit organizations as its members, it is notable that TradeSafe, a Japanese TM accreditation company, has now joined ATA. This means that the company's operation will be performed justly and that it shows its intentions to the ATA common criteria of TM accreditation. It also means that opportunities exist for other commercial TM accreditation enterprises (particularly from the U.S.) to join the alliance.

2.3. Research on Online Trustmark Programs in Europe

As a consequence of ATA, trustmark collaboration has mainly focused in Asian countries. Nevertheless, a large number of trustmark schemes are already operating around the world. It seems that websites are flooded with so many trustmarks that consumers may find it difficult or impossible to understand their meaning.

GBDe concluded that a better understanding of the current situation was needed in order to evaluate trustmark schemes and to understand how these schemes contribute to consumer confidence. In 2006, GBDe examined the performance of existing trustmark programs in North America and Asia. In 2007, GBDe focused the scope of examination on European trustmark organizations and created the list shown for each country in the Appendix C.

Following on the study report, “E-Commerce Trustmarks in Europe,”¹ which was presented at a trustmark conference in Denmark by Jan Trzaskowski, an associate professor at Copenhagen Business School, GBDe conducted further web-based research and gathered information via e-mail questionnaires about trustmark schemes in Europe.

Based on this research, GBDe learned the situation of trustmark schemes in Europe as follows:

- 1) Examined organizations and administering organizations
 - GBDe examined 33 trustmark schemes in 17 countries in Europe. According to the study report, about two thirds of European countries have trustmark schemes and the concept of trustmark is widely recognized.² However, the number of online shops that are trustmark accredited is still small compared with the United States.
 - In terms of the number of accredited businesses, the most successful certification organization is the German-based Trusted Shops (approx. 2,000), one of the oldest trustmark scheme organizations, followed by SafeBuy in the U.K. (1,200 sites). Italy and Portugal have approved only a single-digit number of businesses.
 - A great number of examined trustmark organizations, twenty two of them, seem to be administered by non-profit organizations such as IT companies associations, direct marketing associations and chamber of commerce, with cooperation from governments and consumer organizations. E-commerce ILiM Crtyfikat of Poland and IQUA of Spain are operated by respective governments.
 - There are not many trustmark schemes operated by private companies. Besides SafeBuy in the U.K. is administered by a private research company, there is a trustmark called Ebtrust in Norway operated by multinational risk management corporations. Launched in 1999, Trusted Shops not only issues trustmarks but also offers a compensation system cooperatively with an insurance company for non-delivery of goods, non-refund after returning goods, and credit card fraud.
- 2) Criteria for certification
 - Each trustmark scheme aiming at general consumers’ trust accredits its trustmark based on its own code of conduct. We will discuss later, but trustmarks of Euro-Label has common criteria called European Code

¹<http://www.trustmarkconference.dk/download/trustmarks-report.pdf>

² The same as the report above.

of Conduct. Trusted Shops has been operating in accordance with the trustmark guidelines established by InitiativeD21, a public- private partnership aimed at promoting ICT.

- SafeBuy’s code of conduct was approved by the Office of Fair Trading (OFT). Trustmark schemes are often supported by public organizations from an early stage of establishing their code of conducts. The standards of quality of W-Mark of EIQA in Ireland have been playing a role as criteria for accreditation.
 - However, many of code of conducts are displayed only in local languages. Unfortunately, we cannot read some of them in English. According to the report presented by Trzaskowski, the standards are similar to EU legislation and do not exceed it much.
- 3) Relations with ADR service
- Some trustmark organizations only accept complaints and do not provide ADR service, such as BeCommerce of Belgium and PACE of Portugal. However, about half of the examined organizations has ADR mechanism internally or work together with external ADR organizations.
 - e-mark of Denmark has in-house consumer complaints board. Euro-Label cooperates with ombudsman scheme through the European Consumer Center Network.
 - WebtraderUK accepts consumer complaints regardless of trustmark-holders if the complaints are not fraudulent cases. In Czech Republic, there are no ADR organizations at present, but the government is considering creating ADR cooperating with ECC in Czech.
 - Trusted Shops has an in-house customer service center which handles all disputes between its member shops and their customers as well as offers amicable solution through its mediation service. According to the response of the questionnaire, going to court has not been occurred in any of the disputes they have dealt with. Cases which are not related to the Trusted Shops quality criteria are forwarded to its co-operation partner, ombudsman.
 - SafeBuy offers a similar service. If its mediation fails, SafeBuy will refer to the Chartered Institute of Arbitrators. Thuiswinkel Waarborg of the Netherlands has a complaint committee outsourcing to an organization which handles complaints with about 40 branch associations.
 - Based on these results, GBDe should conduct further research with regard to whether these ADR services have binding force to businesses.
- 4) International cooperation and handling of cross-border transactions
- Some trustmark schemes are offered in more than one country, such as Trusted Shops of Germany and Euro-Label. In 2000, a Trusted Shops representative attended at the “Dialogue with Trustmarks and ADRs Organisations”, held by the GBDe. The European Commission financially supports Euro-Label. Current member countries of Euro-Label are Austria, France, Germany, Italy, Malta, Poland, and Spain. Euro-Label has awarded its trustmark to nearly 700 businesses. E-Commerce Trust Mark of a non-profit organization in Australia is a founder of Euro-Label. Consumer and business associations

- participated in drawing of its code of conduct. Cross-border complaints are currently handled with Euro-Label partners in the respective country. Euro-Label Austria responded that it is interested in global cooperation.
- Asked about the same questions, members of W-Mark, EIQA in Ireland are from different countries; therefore it answered that it accepts cross-border complaints and looks for partners in different countries.
 - SafeBuy also responds that it has strong interest in joining a global trustmark alliance but concerns that other trustmark schemes should have a code of conduct that is supported by the government or the third party and provide a completely independent ADR mechanism. Unless otherwise matched, it would be difficult to collaborate with other trustmark schemes.
 - TrustUK in the U.K., which had a partnership agreement with BBB in North America, seems to have stopped its operation³.
- 5) Collaboration with law enforcement organizations
- The Code of Practice is performance monitoring of SafeBuy in the U.K. by the OFT. Trusted Shops in Germany also responded that it has collaborated with several government organizations and participated in a project by the European Commission called “Consumer Protection Seal: Assurance and Money-back-guarantee (COSEAG).

Based on this research and that of 2006, GBDe concludes the following with regards to existing trustmarks:

- Despite the fact that a variety of trustmark schemes are available worldwide, information regarding trustmark schemes is not necessarily presented in an easy-to-understand manner. In the context of promoting international cooperation, a general understanding of what trustmark schemes exist in each country is necessary, in addition to considering how to address the issue of international cooperation.
- In addition, we were able to gain a better understanding of the situation of trustmark schemes in Europe. We learned from the questionnaire that some trustmark organizations, such as Euro-Label and SafeBuy, are willing to cooperate internationally. While more in-depth research is required, this initial research enabled us to take an important first step toward extending cooperation not only with other countries in the Asia-Pacific region, but also with Europe. It is a step toward enhancing consumer confidence globally.
- Harmonization of codes of conduct is a prerequisite for international cooperation. This research revealed that trustmark schemes in Europe adopt a certain level of unified accreditation criteria. Generally, as a high level of consumer protection is legally assured in the region, it is assumed that their accreditation criteria are sufficient. As ATA is assessed in terms of GBDe’s Guidelines, the same efforts will be required for each European trustmark organization’s code of conduct.

³ As of November in 2007, its website has been closed

- With the numbers of cross-border transactions growing, it is indispensable to provide information to consumers. For examples, with regard to transactions, consumers should know what the trustmarks on foreign websites mean and what rights they provide. This will help consumers to choose trustworthy websites.
- Given this view, information disclosure by trustmark organizations in each country is still insufficient, except for the schemes in the United States. It is inevitable for trustmark organizations to provide websites in multiple languages given the growth of international trade, yet few trustmark organizations have done so.
- Furthermore, accessibility for consumers may be enhanced if they can access comparisons and evaluations of these sites by a third party. With this as a turning point, sharing and disclosure of information may be accelerated among trustmark organizations. Having links from consumer organization sites to the above-mentioned third-party sites would increase awareness and dissemination of information.

3. Privacy

This chapter looks at some privacy protection activities and tries to extract and analyze some of the underlying issues. Outsourcing issues are discussed in the next chapter.

3.1. Privacy in the Age of WebCommerce2.0

In 1999 when GBDe was formed, the potential privacy risk of “e-commerce” was already apparent. Once personal information is transmitted across a border, it is outside the jurisdiction of the country where the consumer resides. In short, the “cross-border” nature of e-commerce cuts across and to a degree nullifies existing regulatory frameworks.

In response to this situation, GBDe made two proposals. As e-commerce was in its infancy and heavy regulations could have choked its growth, the first proposal was that any regulations, if necessary, should be simple, minimal, and easy to comply with. The second, given that it would take considerable time and effort for governments to develop a regulatory framework to effectively cope with the cross-border nature of e-commerce, was that the business community should regulate itself so as not to leave consumers in a vacuum while waiting for effective governmental regulations.

Nine years later, the landscape of personal information protection has changed in many ways. Two of them are noted here. The first change was brought about by the pervasive business use of information technology. The second is the change of the context in which privacy is at risk. Today, privacy data is transferred among business organizations along a value chain, and the globalization of business activities means that value chains now almost always cross borders. Outsourcing and off-shoring are typical examples, to which we will come back later in Chapter 4.

These changes, in turn, caused several movements. Three of them are mentioned below.

3.2. Self-Regulation in the Context of B2B

GBDe advocated self-regulation and emphasized the importance of best practices in its 2006 recommendation. We cite here the Privacy Mark system in Japan is an example of best practice.

In Japan, business organizations can be certified for having implemented personal information protection management systems in conformance with “Japan Industry Standard Q15001,” which set forth personal information protection management systems requirements. Certified business organizations can highlight their capabilities by displaying the Privacy mark on their Web-site, business cards, marketing materials, and so on. Such a privacy mark system achieves two objectives:

- It raises awareness on the part of general consumers of the importance of the protection of their personal information.
- It gives incentives for business organizations to win social trust by implementing a personal information protection management system.

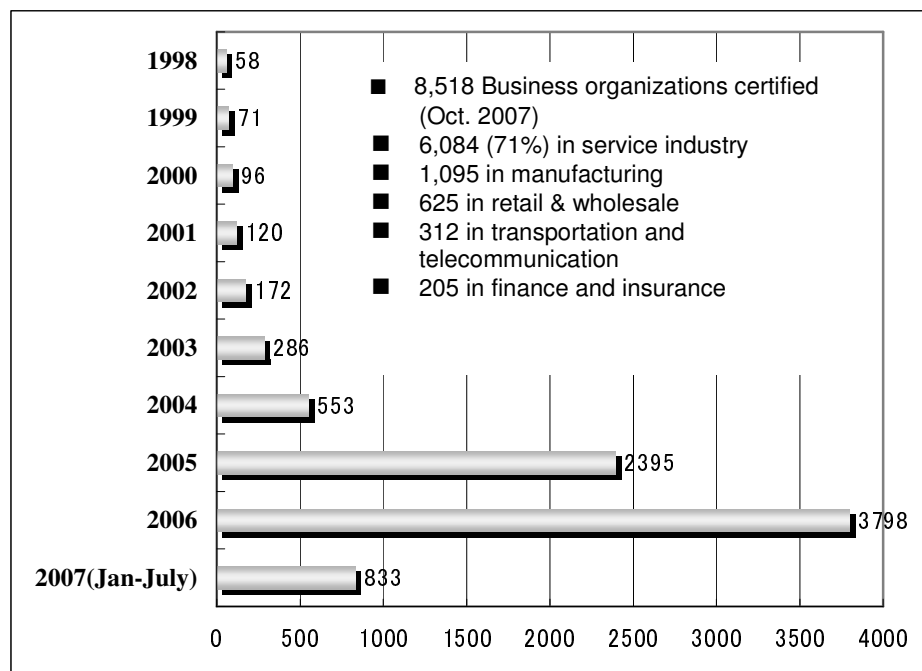


Figure 2 - Increasing P-Mark Owners

The number of certified organizations in Japan has been growing rapidly (see Figure 2). A survey in 2005 suggests one reason for the growth. It found that businesses that outsource processing of customer personal information more often select outsourcing companies that are Privacy mark certified.

3.3. Cross-Border Privacy Rules

Asia-Pacific Economic Cooperation (APEC) issued the APEC Privacy Framework in 2004 and is now working on Cross-Boarder Privacy Rules (CBPR). It covers cooperation of various forms, including cooperation between or among regulatory authorities and cooperation among trustmark operators, and provides a region-wide code of conduct for trustmark operations. In short, CBPR tries to combine existing systems and rules, including self-regulations, to enhance the level of privacy protection throughout the Asia-Pacific region.

GBDe not only supports this effort but also welcomes APEC's move to open its discussions to other international forums, such as OECD. This is exactly the direction GBDe has hoped for since its early days.

3.4. Changing Role of Network Operators

The third change is in the role of network operators and service providers. For instance, the use of mobile phones to access the Internet has exploded in recent years. Standard models are now capable of storing more than 1000 individuals' personal information, which include their name, address, telephone number, zip code, birth date, blood type and digital photos. If a mobile phone set is lost or stolen, this stored private data might be used in an unintended way. This poses a new type of risk in the sense that consumers could easily lose a substantial amount of privacy data simply by misplacing or losing their phones.

In response to this concern, mobile telephone companies now offer services of various kinds. For example, users can set biometric authentication on their phones or purchase plans that allow them to lock their mobile phones simply by notifying a call center when the phone is lost. In sum, "privacy services" are emerging.

The other change is coming from the deployment of new technologies. The Next Generation Network (NGN) allows network operators to provide a package of basic services for e-commerce, such as authentication for identity as well as payments. As such, NGN could become a trust management focal point, including for privacy protection. Although NGN technologies are still in the field testing stage, their deployment could change the role of network operators and thus the focal point of e-commerce related policies, just as happened to Internet service providers in the early days.

3.5. A New Approach to Privacy Issues

Even when e-commerce was just emerging, GBDe noted that the landscape of privacy protection would change. What has developed in the past nine years, however, is far beyond what we had envisioned. Nevertheless, GBDe is still confident that its basic approach – to raise important issues from the frontlines of business and to promote dialogue with all interested parties – is valid. This approach has produced many useful outcomes, and GBDe will continue its course.

4. Cross-Border Sourcing and Data Privacy

This chapter reflects on some facts and trends related to the intersection of cross-border outsourcing and personal information protection, then extracts some issues for the further discussion.

4.1. Current Trends and Issues

The potential collision between two global trends, increasing cross-border flows of information and increased concern over data privacy, could have significant implications for global economic growth. In the extreme, data privacy could become a significant barrier to trade across national boundaries and reduce global economic growth.

Businesses today operate in a climate where:

- Global demographic changes are driving an increase in cross-border trade and information flows.
 - Reduced communication costs increase the opportunity to cost-effectively decompose work into chunks that can be performed across a variety of locations and time zones.
 - The ability to effectively map and track these revised processes and data flows has not kept pace with the development of the processes.
 - The potential for large-scale, rapid breaches of privacy increases with the growing volume of data stored and transferred electronically.
- Increased individual concern regarding privacy of their personal data is driving governments to adopt a variety of laws and regulations regarding data privacy.
 - The relatively new laws and regulations create uncertain implications regarding responsibility and liability.
 - The rapid change has resulted in potentially overlapping and contradictory laws and regulations further increasing uncertainty.
 - Uncertainty results in increased costs, such as for monitoring, understanding, and demonstrating compliance.

These are not new topics. Paper-based data can be copied or discarded inappropriately. Shared service groups, located in other countries, are common in multinational corporations. Inconsistencies and clashes of laws have and will continue to exist between countries and regions.

Rather, what has changed is the degree to which these areas are interacting and business models are changing. The potential to effectively take data from one location, store it in a second, and process it in both of those locations as well as a few others is something that is only recently available to a broad range of organizations.

This change in degree is important because an event that happens once a year affecting only 10 people has a different risk profile than one that happens every day affecting 10 million people. Appropriate risk mitigation strategies also differ.

Simplification and harmonization of legal and regulatory frameworks continues to be an ongoing goal in this area as well as others. This paper examines the topics of cross-border sourcing and data privacy from a business context and considers the steps

involved in implementing cross-border sourcing and the approaches often adopted by businesses to manage the associated risks and costs.

The reflections in this paper were informed by discussions between TPI, the largest global sourcing advisory firm, and a number of outsourcing service providers covering IT outsourcing, application outsourcing, and business process outsourcing. These companies span the globe with operations in all major areas, including North and South America (Brazil, Canada, USA, etc.), Europe (Germany, U.K., etc.), and Asia (China, India, Japan, etc.) Respecting the wishes of many of the companies and individuals, names have not been included.

4.2. Implementation Steps

To deal with the issue of data privacy in a cross-border sourcing context, organizations typically have to address the following implementation steps:

- Understanding obligations.
- Negotiating a data transfer agreement.
- Implementing data transfers.
- Monitoring and compliance.

4.2.1. Understanding Obligations

The effort involved in understanding obligations is clearly higher:

- For new and rapidly changing areas than for established and stable ones;
- When dealing across multiple jurisdictions and with how those obligations inter-relate than for single jurisdictions; and
- For complex legislation than for straightforward legislation.

Unfortunately, cross-border sourcing and data privacy involve the more difficult side of all of the above points. This almost exponential increased level of effort to understand has an unfortunate side-effect. Widespread ignorance (lack of understanding) of data privacy legislation coupled with misunderstanding creates a fertile breeding ground for fear and uncertainty.

How this fear and uncertainty get managed, especially in the political sphere, will significantly influence the ongoing degree of effort and will have a significant bearing on whether the costs to acquire such understanding stabilize then decline or continue to increase.

4.2.2. Negotiating a Data Transfer Agreement

Negotiating a data transfer agreement extends well beyond, and in fact does not even need to involve, an external service provider. It includes employees, unions, regulators, and even customers. For example, in many European situations, regulatory as well as employee approval is required before personal data can be transferred to another country for storage or processing.

Multi-party negotiations are complex and costly, with the cost increasing dramatically when the negotiations involve poorly understood areas, such as data privacy. For example:

- Data privacy protection may be cited when an underlying issue is job protection.
- Before any data is allowed to be transferred, it can take months of socializing data transfer arrangements with country regulators to gain understanding and acceptance of what data is transferred, how it is transferred and what is done with the data after it is transferred.

Organizations need to factor time and cost for this into their plans for cross-border sourcing involving data transfers.

4.2.3. Implementing Data Transfers

Implementation of data transfer involves issues such as:

- Physical transfer of data.
- Encryption and encoding of data.
- Disaster recovery plans including customer and employee retention plans.

These are ongoing costs that would be factored into any business decision regarding cross-border sourcing that involves data transfers.

4.2.4. Monitoring and Compliance

To satisfy the demands of legislation, regulators, and employees, as well as for good corporate governance, appropriate monitoring regimes and compliance verification approaches need to be established for cross-border data flows.

An interesting observation is that more complex schemes (partitioned data, multiple and varying processes, and information security requirements) are perceived as more likely to fail because the ability to effectively map and track these processes and data flows has not kept pace with the development of the processes.

As such, it is common for regulators in particular to question such schemes and scrutinize the associated monitoring in more detail, which inevitably results in increased costs and timeframes for implementation.

4.3. Business Approaches

To deal with the challenges posed in the implementation steps, organizations tend to adopt four different approaches:

- Avoid cross-border transfers.
- Pass the challenges to someone else.

- Adopt the highest common denominator.
- Implement detailed data and process tracking.

4.3.1. Avoid Cross-Border Transfers

This is certainly a simple approach to avoiding the issue. It avoids the costs associated with all of the implementation steps but at the same time loses the opportunities associated with cross-border sourcing.

While such an approach may be appropriate for some organizations, widespread adoption would result in a slowdown or even potentially a decrease in trade across national boundaries.

Just as individual, corporate, and national policies have and continue to evolve over time with regards to the transfer of goods across borders and the movement of people (work visas, immigration), it can be expected that the same will be true for the movement of data across borders. Some will be more protective and some will be less; some will stagnate and some will prosper.

Studies on the correlation between cross-border movement of goods and people and economic growth should be extended to the cross-border flow of data.

4.3.2. Pass the Challenges to Someone Else

A second approach is to attempt to make someone else responsible for the challenges. Outsourcing is a thriving industry, and without a doubt, leveraging a third party's "pre-approved" implementation, including monitoring, is attractive for many organizations.

A challenge with this approach relates to the boundary between service delivery and insurance. Service providers will take responsibility and liability for their actions; however, they do not insure their customers. Customers still need to understand their obligations and accountability.

Much like the experience with SOX obligations, it will take some time, even after the total set of obligations are well understood, to clarify the appropriate division of responsibility and liability between customers and service providers.

In the interim, there is potential for data privacy regimes to make data "radioactive" such that no party wants to be responsible for storing or processing it unless significant controls, at significant cost, are in place and liability is clarified.

4.3.3. Adopt the Highest Common Denominator

Another approach is to adopt the most stringent of all requirements for all situations. This type of approach is often seen in accounting and more recently, in SOX.

This approach has a number of implementation benefits compared to tailored approaches including:

- Easier to explain (e.g., to regulators);
- Easier to manage and govern a consistent set of policies and processes than a multitude of policies and processes around the world;
- Avoids challenges such as deciding how to partition data and policies; and
- Less likely to create “islands” that may restrict future flexibility.

This approach, however, also has some challenges:

- Determining the “highest standard” can have a significant cost. And that presumes that there is a “highest standard” and that there are no inconsistencies between various regions that prevent adoption of a single “highest standard.”
- Negotiation costs can actually increase as there can be a perception that a “standard” solution does not address unique needs, perceived or real. Unfortunately in evolving areas, the belief that tailored solutions are required can be strong.

It is often assumed that this approach avoids the need to understand the data transfers that will actually occur. In the long term, however, this looks unlikely, especially when the data not only move across borders but also shift between companies.

4.3.4. Implement Detailed Data and Process Tracking

Another approach, often only possible for large organizations and for major service providers, is to invest in the ability to map, track and audit processes and the associated data flows.

While this approach can have a high initial cost, there are some strategic businesses that have evolved over time to leverage similar principles and, therefore, it should not be discounted.

While the rationale was driven primarily by cost, mainframe processing is one area where the recognition that data about “what happened and when” is considered just as important as what actually happened. This clearly comes at a cost, but the auditability and confidence that it brings provides benefits in the right context.

In a similar manner, the redefinition of logistics such that information about the delivery became just as important as the delivery itself was an industry turning point.

Will those who invest in managing the information about who did what, where and when with respect to data similarly redefine the industry with respect to cross-border sourcing?

4.4. Summary

The interaction between cross-border sourcing and data privacy continues to evolve. Legislation is evolving. Political and social reactions are changing. Implementation

steps are becoming clearer. A variety of business approaches are being adopted.

This shifting landscape could result in significant impediments to global economic growth or it could result in opportunities for companies to create new business models. The outcome is uncertain and further study should be undertaken in order to reduce the potential for the interaction between cross-border sourcing and data privacy to become a collision that impedes global economic growth.

5. Conclusion

GBDe continues those activities noted below in order to improve consumer confidence in the era of WebCommerce2.0 and looks forward to the positive cooperation of businesses, governments, and related organizations in each country. GBDe aims to:

- (1) Start a global investigation and dialogue of the necessity, effectiveness and possibility of an “International Consumer Advisory Network.”
- (2) Expand trustmark-related activities in Asian countries and deepen global dialogue on the possibility of European trustmark alliance.
- (3) Continue global dialogue on personal information protection issues.
- (4) Continue global investigation and dialogue on cross-border outsourcing and privacy issues.

Appendix A. Members of Japan ADR Study Group

Experts

Tsuneo Matsumoto, Professor of Law, Hitotsubashi University
Yoshihisa Hayakawa, Professor of Law, Rikkyo University
Kotaro Tsuru, Senior Fellow, Research Institute of Economy, Trade and Industry
Shino Uenuma, Attorney
Yoji Ochiai, Attorney

Observers

Ministry of Economy, Trade and Industry
Noriyuki Mita, Director, Americas Division
Junichi Iwasaki, Europe Division
Reiko Eda, Europe Division
Ryou Ikawa, Information Economy Division
Nobuyuki Hamanaka, Information Economy Division

GBDe Consumer Confidence Issue Group

Toshiro Kawamura, NEC Corp.
Takeo Koyama, NEC Corp.
Tatsuro Tanigami, NEC Corp.
Michikazu Chihara, NEC Corp.
Takaharu Nagata, NTT Data Corp.
Michael Rehkopf, TPI
Julian Wick, Sybase

Secretariat

EC Network
Toshiko Sawada
Yuko Tonomura

Appendix B. GBDe/ATA Common Criteria

GBDe Guidelines for Merchants		Proposed ATA Principles for Merchants	
No.	Principle	No.	Principle
1.	Accuracy and Accessibility of Information	1.	Information Disclosure
3.	Information about the Merchant		
4.	Information about the Goods and Services		
5.	Information about the Transaction		
6.	Cancellation/Return/Refund Policies		
2.	Marketing practices		
8.	Customer Service and/or Support	2.	Business & Marketing Practices - how to communicate - protection of minors and elderly
9.	Warranty		
11.	Unsolicited E-mail		
7.	Security	3.	Security
10.	Privacy	4.	Data Privacy (APEC Privacy rules)
12.	Dispute Resolution	5.	Dispute Resolution
		6.	Monitoring

Table 1- Proposed First Level ATA Principles for Merchants

GBDe Guidelines for Certifiers		Proposed ATA Principles for Certifiers	
No.	Principle	No.	Principle
1.	Accessibility	1.	Visibility and guidance to merchants
3.	Visibility		
2.	Enforcement Mechanisms	2.	Monitor compliance by merchants - frequency, mechanism (ie contract), etc
4.	Stakeholders Participation	3.	Independence - stakeholders participation
5.	Security	4.	Security
6.	Redress	5.	Redress
7.	Flexibility and Mutual Recognition	6.	Flexibility and Mutual Recognition
		7.	Information Disclosure

Table 2 - Proposed First Level ATA Principles for Certifiers

Appendix C: Trustmark Organizations in Americas and Europe

Country	Trustmark logo	Trustmarks	URL	Access to English sites	Name of Trustmark Operating organization	Type of organization	Approved businesses/ or websites	Does it have its own code of conduct?	Annual fees (EUR/USD)	What is the average minimum length of time to be accredited?	Renewal/extension	Sanctions for non-compliance	Is it required to comply with certain Alternative Dispute Resolution mechanisms?	Handling cover-tender cases or collaboration with other Trustmark operators	Cooperation with European Consumer Centres (ECC) or other international organizations	Others	
<p>Trustmark scheme in Europe</p> <p>This research is based on Euro-Label Management (www.euro-label.com) and Euro-Label (www.euro-label.com). Euro-Label is a partner of European Consumer Centre Network. Euro-Label website: http://www.euro-label.com. The European Code of Conduct is drafted in accordance with European legislation and the EU Directive on Distance Selling, Data Protection and on guarantees. There is no Trustmark scheme in Bulgaria, Cyprus, Estonia, Finland, Ireland, Latvia, Lithuania, Romania, Slovakia, Slovenia and Slovenia.</p>																	
Austria		DurachKocher	www.durachkocher.at	No	Austrian Institute for Applied Telecommunications (IACT) www.iact.at/index.php?seite=1	Developed in the framework of the Internet Consumer Law	240 websites	Yes. It is in accordance with the European Code of Conduct under the Euro-Label system	800 Euros in the first year for SMEs. Single companies pay according to work hours for the maintenance, 800 Euros the following years for all companies	None	annual	Non-compliance is covered by the withdrawal of the trustmark	Yes. ADR is done by www.durachkocher.at	ADR is handled by it or by Euro-Label partners in the respective country. It is involved in being active in cross-national and global trustmark schemes	Yes. consumer organizations participated in the drawing of the code of conduct and statute financing		
Belgium		BCommerce Label	www.bcommerce.be	No (Dutch & French)	Association for Electronic Commerce (Vereeniging voor Elektronische Handel)	Started operation by the Belgian Association of Direct Marketing (VABED) in 2006	400 companies	Yes. Code of the BCommerce (IMI, Belgian legislation), the code of ethics of the ABMD	500		annual	fine and withdrawal of the certificate	handles consumer complaints	As trustworthy sites, EILs (both Dutch, German and French) workshops, no workshops are posted as reliable marks			
Czech Republic		Certified shop	www.certifiedshop.cz	Top page only	Association for Electronic Commerce (Asociace e-shoppers)	Founded in 1998 as a non-governmental organization	35	Yes	35		annual						
Denmark		e-trustart	www.e-trustart.dk	partly English	Administrated by the e-Consumer Protection, a non-profit trust established by the Ministry of Science, Technology and Innovation, The Consumer Council, The Chamber of Commerce, etc.	371 shops and 159 under review (as of 2007)	Yes	Application fee: 200-1.000 Annual fee: 400-1.350			annual and random checks	withdrawal of the certification	Yes. Danish Consumer Complaint Board		Yes. ECC: the Ministry of Information, Ministry of Labour and Trade. Danish Marketing Association for Information Society		
France		Labelite	www.labelite.com	No	Created and developed by Publication of the companies Commercial and Distribution and the FEMAD (Federation of the Companies of France)	30	Yes. European code of Conduct (Euro-Label)							part of Euro-Label			
Germany		Partner	www.partner-label.com	No	Partner												
Germany		Trusted Shop	www.trustedshop.de	No	Trusted Shop	Founded in 1998 as a consumer protection and information service. Operating with a trustmark guarantee for consumers	2000	Yes. Code of conduct with micro-trust guarantee for consumers	19-99		annual and random checks	contractual penalty and withdrawal of certificate	Yes. Internal mediation system		part of Euro-Label		
Germany		Internet Privacy Shield	www.internet-privacy-shield.com	No	Internet Privacy Shield	Public and business organization	80	Yes	1.000-50.000		annual checks		No				
Germany		EIL (Int. Label)	www.eil-label.com	No	EIL (European Information Label)	Operating since 1999 supported by EIL as a research and advisory institute for the small business. Business of Informa EIL	213	Yes	per month 1000 EUR and/or 10000 EUR per year			withdrawal	Uses a Complaint form of Euro-Label	part of Euro-Label			
Hungary		Ekon	www.ekon.hu	No relevant information about Trustmark	Hungarian Association of IT Industries (Magyar Informatikai Szakmai Szövetség)	Association of IT industries	24										
Ireland		EDA W-Mark	www.eda-wmark.com	No	Evidence Based Quality Association	Approx. 50 businesses in Ireland and 3 in UK, USA & Australia	Developed in association with local media standards and Achievement Standards Board and endorsed by ASD & EDO	300		None	every 6 months	withdrawal					
Ireland		Stylez Trustmark	www.stylez.com	No	Stylez	A private organization	4	Yes	very		annual renewal	withdrawal					
Italy		Euro-Label Italia	www.euro-label.it	Only a top page and later sites are accessible	Confederazione, the General Committee of Trade, Tourism, Services and SMEs		4	Yes. European code of Conduct (Euro-Label)			annual	withdrawal		part of Euro-Label			
Luxembourg		e-commerce certified	www.ecertified.lu	No	Luxembourg e-commerce certified	Operated by The Chamber of Commerce, the State Chamber and COP (Consumer Protection) of the Ministry for the Economy and the Energy. Trust Certificate marks (e-commerce) a certificate with a compliance protocol since 2005	10	Yes	About 1.000		annual	withdrawal	No				
Republic of Malta		Euro-Label Malta	www.euro-label.com	No	Operated by Ministry for Investment, Industry and Information Technology and the Chamber of Commerce		4	Yes	The first year: 450. From the following year: 225		annual	withdrawal	Internal mediation system	part of Euro-Label			
The Netherlands		Trusted Webshop	www.trustedwebshop.nl	No. Only a pdf file is available. Otherwise not	Public and consumer organization	approx. 400	Yes	Assessment fee: 100-20.000. Trustmark fee: 450			annually (optional annual)	withdrawal					
Norway		Trust	www.trust.no	No. Only a pdf file is available. Otherwise not	Trust												
Norway		Ethnet	www.ethnet.no	Old website. Website is outdated by DNS	Ethnet	The year of launch in 2002, operated by DNS	24	Ethnet written E20 Standard	not posted	not posted	annually. Re-certification process after 3 years	withdrawal	not posted	not posted	not posted		
Country	Trustmark logo	Trustmarks	URL	Access to English sites	Name of Trustmark Operating organization	Type of organization	Approved businesses/ or websites	Does it have its own code of conduct?	Annual fees (EUR/USD)	What is the average minimum length of time to be accredited?	Renewal/extension	Sanctions for non-compliance	Is it required to comply with certain Alternative Dispute Resolution mechanisms?	Handling cover-tender cases or collaboration with other Trustmark operators	Cooperation with European Consumer Centres (ECC) or other international organizations	Others	
Poland		E-Commerce B.M. Certified	www.e-commerce-bm.com	No	E-Commerce B.M. Certified		4	Yes	80-450		annual	fine & withdrawal	Euro-Label/ADR				
Portugal		Trusted Shop	www.trustedshop.pt	No	Trusted Shop		7	Yes	membership fee is 500, application fee is 150		every 2 year	withdrawal					
Spain		Confianza Online	www.confianzaonline.com	No	Confianza Online	Created by advertising self-regulation organization in 2002. Launched Trustmark scheme in 2006.	290 shops with 165 members	Ethical Code on E-commerce EDO and Incentive Advertising	550-5.000								
Spain		ADR/CR	www.adr-cr.com	No	ADR/CR												
Spain		ADACE	www.adace.com	No	ADACE												
Spain		EDIA	www.edia.com	No	EDIA		over 140		114€ VAT								
Spain		EDIP	www.edip.com	No	EDIP												
Spain		Euro-Label Spain	www.euro-label.com	No	Euro-Label Spain		1										
Spain		TrustUK	www.trustuk.com	The website has been closed	TrustUK												
Spain		Webtrust UK	www.webtrust.com	No	Webtrust UK		approx. 200	Yes	375+VAT		annual and random checks	withdrawal					
Spain		Trustmark	www.trustmark.es	No	Trustmark	Supported by advertisement consumer groups and controlling agencies. Issuing marks to housing-related companies					annual						
The United Kingdom		SafeBuy	www.safebuy.co.uk	No	SafeBuy	Started Oct 2005. Initially a research company, not a trustmark organization	1.200 businesses with 500 websites	Code of Practice stage one approved by UK government through CPTI. Stage two is performance monitoring of SafeBuy by the CPTI which is happening now	65€ + VAT (€111.63 total) per 10 additional fees	None	annual	All given brief review on application. 20€ withdrawal in 48h if not approved. A different CPTI "truly accepted" annually	Non-compliance leads to the withdrawal of the trustmark with information on violation being reported to the CPTI	ADR (online) if SafeBuy mediation fails, by the Chartered Institute of Arbitration	The same as in temporary cases. SafeBuy is not involved in giving a Trustmark. ADR is not involved. If only SafeBuy Trustmark scheme is used, they have a Code of Practice agreed by an independent body (outside the national government). There is a scheme available to consumers and trust adds support from their national government	Not with ECC but with law enforcement in UK through CPTI/Trading Standards	

FINAL – SUBJECT TO BSC APPROVAL – November 8, 2007

Trustmark schemes in the US and other regions																
Country	Trustmark logo	Name of Trustmark	URL	Name of Trustmark Operating organization	Type of organization	Approved businesses / websites	Does it have its own code of conduct?	Annual fees	What is the maximum minimum length of time to be accredited?	re-examination	Sanctions for non-compliance	Is it required to comply with certain Alternative Dispute Resolution mechanisms?	Handling cross-border cases or collaboration with other Trustmark organizations	Cooperation with law enforcement organizations	Others	
U.S.A		Reliability Seal Program	http://reliabilityseal.com	BBB Online	Established in 1912. No single accrediting requirements for its Privacy Seal program. Prior to October 1, 2007, new BBB Accredited Businesses referred to themselves as BBB Sealers.	38017 websites	Yes	Fees vary based on the size of the company		Every accredited business is required for continuing adherence to its standards	withdrawal	Yes. Accepts complaints whether or not the business is its Accredited Business	Trusted OCR platform with TrustIn, in 2006. Signed MOU with SOA and ED Network. A member of (ITA/ATA)			
		buSAFE Seal	www.buSAFE.com	BuSAFE Inc.	A private company BuSAFE and TRUSTe firm strategic partners	over 770,000	Yes	Free of charge		monitors every transaction		Problem Transaction Resolution services	only in the US			
		Truste	www.truste.org	Truste	An independent, nonprofit organization which provides privacy seal programs. Founded by Electronic Privacy Foundation (EPF). Commerce met in 1997. BuSAFE and TRUSTe firm strategic partners.	2940	Yes	Base price differs based on business revenue. (\$840+) additional URL \$250+				License will be terminated/announced public and/or refer the matter to a relevant government agency	Yes. Webshop Dispute Resolution			
		VeriSign	www.verisign.com	VeriSign Inc.	Established in 1995. A private security solution provider. Handling as many as 31+ million website trust domains every day.	750000	Yes	offers depending on products. Trust 128-Bit SSL. VeriSign® 6 4950								
			www.safesite.com	Safesite Inc.	The largest independent warranty provider in the world. Provides OCR over trouble involving eBay transactions	30075		\$500/per month					OCR arising from eBay transactions with charge			
			Web Assured	www.webassured.com	Web Assured.com											
		Security Verification Seal	www.safesite.com	The Safety Search Inc.	Formed 2000. The seals only search engine that connects the world's largest retail shopping websites to over six million online shoppers each month.	Over 4500		Individual License - \$200, Unlimited Listing Package - \$898								
Canada		Guardian eCommerce Privacy Seal	www.guardiantrust.com	Guardian eCommerce Privacy Seal Program	An independent organization Administered through Web site monitoring, evaluation and seal certification of Web site and online consumer protection		Yes. Code of ethics and site requirements	One Year Privacy Seal is \$19.99 USD. Yearly renewal fee is \$25.00 USD	No			Accepts complaints on online				
New Zealand		eM&A Trustmark	www.marketing.com	The New Zealand Marketing Association	Initially established in 1974 as the New Zealand Direct Marketing Association and officially came into being in 2006. Original Offices in New Zealand Post.		Yes. Code of practice	members SAAS affiliates NZ\$ 1495-995. Non-members NZ\$495-995								
Australia		Paymate trustmark	www.paymate.com.au	Paymate Pty Ltd.	A privately-held company established in 2000. Paymate provides a secure, accurate and reliable Internet payment service. Used in 37 countries.			Differs from account type. NZ\$200-22 per month				Accepts complaints on online. If consumers fail to settle, they can file complaints to ombudsman.				
South Africa		thavp	www.thavp.co.za	thavp	A private organization within the VeriSign, Inc. launched in 1995.		Yes	offers depending on products \$198-\$399								
Taiwan		SOSA	www.sosatrading.com	Secure Shopping Online Association (SSOA)	Founded in 1999, a self-regulating e-commerce organization. Working closely with its government.	105 (as of 2006)	Yes	not mentioned on its sites					A member of ATA			
South Korea		e-Trust Mark	www.kbsa.or.kr	KBSA	Founded in 1998. Provides government-accredited marks		Yes	not mentioned on its sites				Handled by E-Commerce Mediation Center since 2000.	A member of ATA			
Singapore		TrustSG	www.trustsg.com.sg	National Trust Council (NTC)	Operated by National Trust Council. Work together with CASE and Commercial Arbitration Singapore (CAS)	1180	Yes	application fee is S\$50-100. S\$25-S\$100-250.00, annual license is S\$500-800. S\$100-1600, annual license is S\$800-900.	A month	annual	withdrawal of the certification		A member of ATA			
		ConsumerTrust	www.consumertrust.com.sg	CASE	A non-profit, non-governmental organization established in 1971. Facilitating membership system and receives subsidy from the government.		Yes. Aligns to the TrustSG core principles	application fee is S\$50, audit fee is S\$100-2000, annual license fee is S\$800-1000				Internal mediation center with charge.		A member of ATA		
Thailand			www.dpa.go.th	Department of Business Development, Ministry of Commerce												
Mexico			www.asociacion.com.mx	Mexicon Internet Association												
Japan		TrustSafe	www.trustsafe.co.jp	TrustSafe Inc.	Established in 2000 by GFT Inc., e-marketing companies and will provide services to guarantee e-commerce in 2008.		Yes	Accredited businesses to pay -x of payments				ADR will be done by ED Network.	A member of ATA			