# Strategies for Trust and Confidence in B2C E-Commerce

**Pravir CHAWDHRY, Marcelo MASERA & Marc WILIKENS**

Institute for the Protection and Security of the Citizen
European Commission, Joint Research Centre, Ispra (Italy)

## ■ Introduction

Mass access to the Internet coupled with trends in globalisation of products and services have given birth to new e-commerce markets in recent years. There have been several optimistic projections of rapid growth for e-commerce, but the business-to-consumer (B2C) sector has failed to achieve its expected growth potential (CommerceNet, 2000). One of the main reasons for these disappointing results is thought to be the lack of consumer trust and confidence in e-commerce (SCRIBBENS, 2001). The European Commission, the Federal Trade Commission, the OECD and business sectors have all identified the establishment of T&C as being crucial for the future of B2C e-commerce (OECD, 1997, 2000, 2001). Although previous research has focused on the strategies deployed for the organisational growth of e-commerce as a whole (LYNCH, 2000), few efforts have been devoted to strategies for developing T&C in e-commerce.

Although trust and confidence have been cited as key enablers of the information society (GBDe, 2000), there is a lack of systematic studies on the precise relationship between technological, social, economic and policy fplayers. Earlier studies on the requirements and enablers of e-commerce do exist (JONES, WILIKENS, MORRIS & MASERA, 2000). Among the enablers, security, privacy and trust have been recognised as key while, among the other fplayers, we find new business models, awareness, critical mass, integration with traditional business processes, legal framework, enabling technology and infrastructure. The global dimension is also designated as a central feature of e-commerce, particularly in terms of its impact on operations and user confidence.

COMMUNICATIONS & STRATEGIES, no. 45, 1st quarter 2002, p. 81.

**Figure 1: Security and trust in electronic commerce (TEMMERMAN, 1999)**


More recently, factors related to security, trust, privacy and dispute resolution have been grouped under the term e-confidence. These are some of the fundamental fplayers that influence the consumer acceptance and use of e-commerce. The approach towards establishing e-confidence can be divided into two categories: legislation and self-regulation. The establishment of laws relating to e-commerce has been relatively slow, due in part to a lack of understanding of complex legal problems, and in part to the belief that existing legislation on traditional (offline) commerce can still be applied or adapted to e-commerce. A number of e-commerce trust schemes dealing with these fplayers have, nonetheless, been launched in the past few years, seeking to help establish e-confidence in a systematic manner within the self-regulatory framework.

On an e-market, a consumer will conduct a transaction when s/he has a sense of controlling the risks involved, having acquired an appropriate degree of trust and confidence. Trust and confidence do not occur by chance. They need to be systematically developed through a process of building, enhancing and maintaining. Trust and confidence evolve, they can grow or diminish, and are affected by the actions of the stakeholders.

The question put to consumers and traders is how to develop trust and confidence amongst them in light of the risks inherent in B2C e-commerce. In a market economy, it is often believed that market forces alone can achieve the desired results in the most efficient manner, within some unspecified time frame. To test these hypotheses we will analyse the four types of e-markets that derive from the balance between supply and demand of trust and confidence. These are characterised by the depth of relationship between the consumer and the trader, and the nature of the transaction.

**Key components of e-confidence**

There are various elements that contribute towards establishing consumers' trust and confidence in e-commerce. However, as shown in figure 2, these can be grouped into four categories, ranging from the business principles used to create trust relationships to the confidence in the overall business environment. These are summarised in table 1.

E-confidence measures must address consumers' T&C needs during various stages of their involvement: before, during and after a transaction. The pre-transaction measures, such as availability of insurance protection, use of reputed security mechanisms, and existence of codes of conduct inspire consumers' overall confidence in the e-marketplace.

The in-transaction measures adopted by the merchant such as trust seals, product warranties, secure transaction mechanisms, traceable delivery channels and customer feedback rating, help to increase consumers' trust in that particular merchant. In e-commerce, where new merchants often lack the advantage of an existing brand, such measures can act as a substitute for branding.

There are two types of post-transaction measures. First there are the measures used to deal with the direct concerns for redress in the event of a problem, and that help bring the transaction to a satisfactory conclusion. Second, there are the measures linked to the consumers' indirect concerns over the protection of their digital assets. These include fraud prevention and privacy protection.

**Figure 2: Trust & confidence: the consumer perspective**

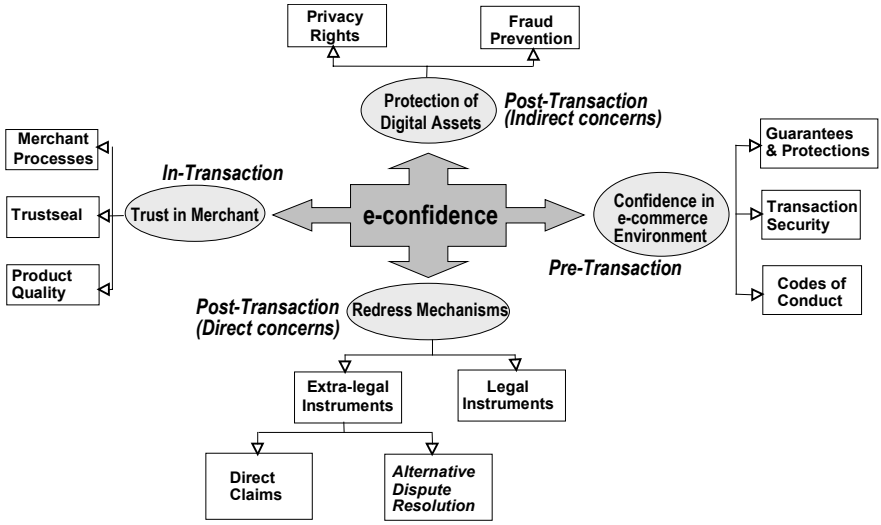



**Table 1: Key components of e-confidence**

| | |
|---|---|
| **Customers' digital rights** | - Privacy of personal information<br>- Existing norms for consumer rights<br>- Protection of digital identity<br>- Anti-fraud infrastructure<br>- Access to law and enforcement |
| **Merchant customer trust relationship** | - Identity of the e-tailer<br>- Identity of the customer<br>- Quality of information (product, process and company)<br>- Delivery of product/service<br>- Merchant's use of trust seal<br>- After sales customer care |
| **Customer confidence in the e -business environment** | - Industry norms for fair trade<br>- Legal framework for consumer protection<br>- Quality of product/service<br>- Security (and ease) of payment & delivery<br>- Protection against fraud (e.g. insurance, chargeback)<br>- Existence of codes of practice |
| **Confidence in redress mechanisms** | - Merchant's own procedures for handling claims (refunds, returns, exchange, replacement, repairs, …)<br>- Dispute resolution: legislation – self regulation – mixed regulation<br>- Practicality (accessibility, cost, time, etc.)<br>- Enforcement of decisions (legal vs. ADR)<br>- Power balance among stake holders in e commerce (before, during and after transactions)<br>- Scope of redress mechanisms (geographic, sectorial, etc.) |

## ■ Information Assets and E-Capabilities

We define an individual's information assets as any data that belongs to the individual or that enables only him to participate in the online environment.

The consumer involved in an e-commerce transaction interacts with another party (i.e. the e-commerce site) through two forms of data exchange:

**1.** Accessing the information presented by the other party; and

**2.** Sending own data to the other party.

The first type of transaction consists of digital data that is sent from the e-commerce site's computing system to the consumer's personal computer (e.g. product information containing text, images, forms, etc) via open networks (e.g. the Internet, wireless telephone networks, etc.).

The second type comprises the digital data that the consumer decides to send to the merchant through the same or another connection. This data could typically consists of commercial information (i.e. the goods or services that the consumer intends to purchase), and personal information (i.e. identity, address, credit card number, etc.).

Some of these exchanges of information can involve risks for the consumer:

- The data coming from the merchant can include malicious or erroneous software codes that could potentially compromise the security of the consumers' computer and the programs/data stored on it;
- The data transmitted by the consumer can be compromised: by a third party during its communication to the merchant over public networks (e.g. eavesdropping); by the merchant's neglect or misuse.

The security implications of such events depend on the value that the consumer attaches to the different information assets at stake. In an extreme case, if these assets have no perceived value, there is no actual risk. In other cases, several natures of risk are involved: economic, safety or relating to individual rights. These may arise during banking transactions, medical applications or social welfare applications. The value assigned by the consumer to a certain information asset can also take different forms: the value can derive from its confidentiality (e.g. credit card number), integrity

(e.g. authorised monetary value of the transaction), timeliness (e.g. data transmitted and received today and not tomorrow), etc.

The information assets can be classified from two main perspectives:

**1.** Their public or private character:

- Public information assets are available to all users without discrimination. Typically a public asset is displayed on a web site or broadcast in an undifferentiated way, i.e. it consists of data that anyone with the appropriate communication link can access. Naturally, this does not imply that the information's owner cannot ascribe some security attributes to a public asset; h/she will generally demand respect of the data's integrity, for instance.
- A private information asset is a set of data specifically sent by one party to another for a specific purpose, and on the condition that strict handling requirements are respected.

**2.** Their shared or non-shared character:

- A shared information asset is the data deliberately disclosed to specific users. The fact that the information asset is disclosed implies that there exists an understanding (unilaterally declared by the asset owner or agreed upon by all parties) of the rights and obligations deriving from its use. An example is the public key in an encryption mechanism that the user gives to intended third parties.
- Non-shared information utilised within an e-commerce transaction refers to any kind of data employed or communicated within the technical infrastructure, but without the need for it to be disclosed to humans. Examples of this are: identification codes, passwords, PINs, private encryption key. In certain circumstances it may be possible for authorised human agents to obtain access to this information.

The dependable management of information assets in e-commerce requires that all parties be able to make use of the appropriate technical means. They should, for instance, be able to:

- authenticate themselves and the information assets in an unequivocal way;
- express and negotiate their preferences and conditions, particularly with respect to integrity, confidentiality, availability and privacy requirements;
- process and transmit data while complying with those requirements;

- be accountable for their own actions, and avoid non-repudiation of the actions by commercial partners.

Thanks to the development of technologies and their subsequent deployment, consumers are generally able to implement a set of utilities for managing the information assets involved in an e-commerce transaction. We refer to these utilities as e-consumers' e-capabilities. E-capabilities include all the actions that an individual or an organisation can perform to achieve the desired effects in the e-commerce environment.

The e-capabilities can differ widely in terms of origin and quality: they could be part of the computing infrastructure, executed on either the e-commerce site or on consumers' computers, or via a third-party service (which is generally the case with Internet access or, more specifically, with of online payment systems).

A fraction of these e-capabilities correspond to the suite of available utilities for ensuring the risk-related attributes of the information assets. A crucial question at any moment is the correlation of e-consumers' needs and the e-capabilities available to them. Any disparity weakens the e-commerce link between the consumer and the merchant, as the former would feel unprotected.

Given that the decisive identifying feature of information assets is their value, the asset owner will try to prevent any potential damage. This situation would constitute an unwanted (and perhaps unacceptable) risk that should be adequately managed (SIEGRIST & CVETKOVICH, 2000). However the management of the information assets is not only in the hands of their owner, but is also shared with all the other players operating on the e-commerce virtual chain: e-merchants, organisations in charge of payment and logistics, identification and encryption service providers, communication network operators. E-consumers rely on all of these players and on their technical capabilities for risk management, and consequently expects that all of them will behave in such a way as to prevent damage to his information assets.

The conclusion is that consumers will unreservedly engage in e-market transactions only once they have accepted that the implied risks are being adequately managed. This can be summarised by the term Trust and Confidence in e-commerce.

## ■ Trust and Confidence in B2C E-Commerce

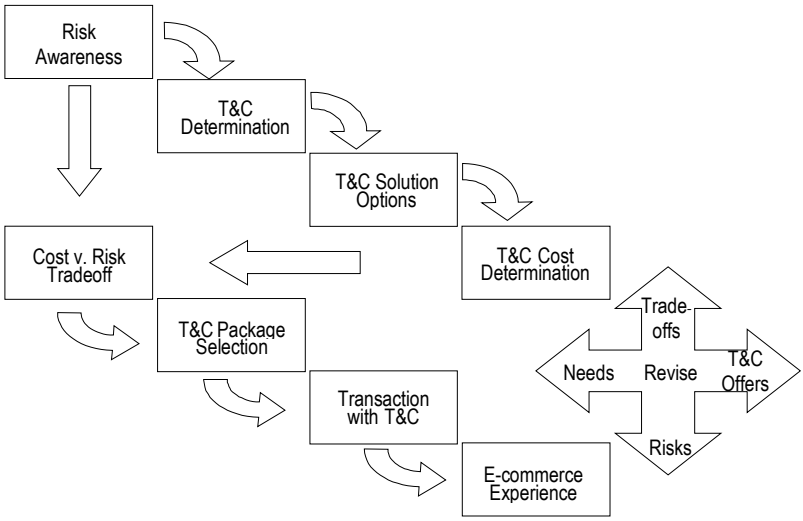
For any party, managing risk in an open network environment (such as the Internet) implies knowing and trusting all of the other players involved in the information's life-cycle. This requirement can be split into two main attributes: trust and confidence.

Trust in this context refers to the willingness to rely on the recognised players, organisations and systems with which the e-commerce interaction occurs. Trust between two parties evolves with the knowledge they might have about one other: their behaviour, their stated policies, technical solutions they deploy, etc. An example is the trust between a customer and his bank to carry out an online transaction accurately and confidentially.

E-markets exist within a broader social and technical realm, however. Who to trust? What is the sequence of steps in a typical e-commerce transaction? Which technologies are applied? These all constitute issues which are not always entirely transparent to the e-consumer. The information infrastructure hides most of its operations from the lay user, added to which, e-consumers and e-commerce sites are part of a much broader environment and therefore rely on its effectiveness: legislation, commercial codes of conduct, mechanisms for defending the rights of the citizen. This is the confidence dimension, which might equally affect the scope of e-commerce (CVETKOVICH & LÖFSTED, 1999). Thus, confidence refers to the perceived overall reliance that can be placed on an e-market as a whole. An example is the confidence of a consumer to start using online banking based on the protection offered by the banking industry, the security technology, and laws applying to the general security of such transactions, along with any redress mechanisms used in the event of a problem.

E-consumers require proof that they can trust their commercial partners, and that they can have confidence in the social and technical framework (FREWER, HOWARD & SHEPHERD, 1998). The more trust and confidence they are able to develop, the more frequent and valuable the transactions they will be willing to carry out. The process usually develops iteratively through interaction between the consumer and merchants, as shown in figure 3.

**Figure 3: A process model for transacting with trust and confidence**




The demand for trust and confidence (T&C) has certain key characteristics:

- T&C depend upon the perceived risks of a given commercial transaction. The perceived risk is a combination of its probability of occurrence and the potential negative effects or loss that might occur. If the potential loss is significant and its likelihood of occurrence is deemed substantial, the requirement for T&C will be greater than otherwise.

- T&C also depend upon the perceived benefits of a transaction. A commercial transaction implies that the customer is willing to acquire a good or service, and to benefit from its use. The greater the expected benefits, the more risks a consumer will be prepared to allow.

- Although trust and confidence develop on an independent basis, the extent of one may influence the demand for the other. For instance, when dealing with a well-known and trustworthy shop, a customer would be willing to accept less stringent confidence conditions. The relative weight of the trust and confidence components demanded when facing a particular deal should be complementary. A consumer might accept less trust evidence when his confidence in the e-market is sufficiently high. On the flip side, in a more unfamiliar market the e-consumer might accept to trade with only a merchant of proven trust value.

The demands for T&C and the ways in which they can be satisfied with technical and organisational systems thereby form a continuum. The degree of risk evolves along with developments made in technology and infrastructure: benefits might grow with the value of the goods traded online, and the introduction of new T&C solutions might even render some previous solutions ineffective.

## ■ A Risk-Based Analysis of T&C in the E-Marketplace

A central issue is the way in which the supply and demand of T&C solutions will be able to evolve in a balanced fashion within the changing reality of e-commerce. In a market economy it is often believed that market forces alone can achieve the desired results in the most efficient manner, in some unspecified time frame. Hence, there is a need to understand the driving forces behind the supply and demand for T&C, that will help in analysing the efficiency of different types of approaches to developing T&C in the information society.

Based on the what has been put forth in the previous sections, four types of e-markets can be identified according to the value and risk of e-transactions. Together, these two factors determine: 1) the need for trust (depth of relationship) between the consumer and the trader; and 2) the need for general confidence in the legal, commercial and technical assurance measures offered in the environment where the transaction is conducted.

From the consumer standpoint, the demand for T&C solutions depends a great deal on the perceived risks which are a function of the probability of an undesirable event occurring ($P^c$) and of the consequence of that event ($C^c$), which can be measured as the difference between the expected loss $L^c$ and the potential benefit $B^c$ for the consumer. Here, loss refers not just to the immediate negative effect of the event, but encompasses the whole transaction (and so includes the cost of eventual redress mechanisms, for instance). The risk for the consumer will be:

$$R^c = P^c * C^c = P^c * (L^c - B^c) = P^c * L^c - P^c * B^c$$

For a given level of benefit $B^c$, a T&C demand chart (as shown in figure 4) can then be developed using P and L as the axes, and on which set of constant-risk curves can be traced.

**Figure 4: Risk-based consumer demand for T&C**

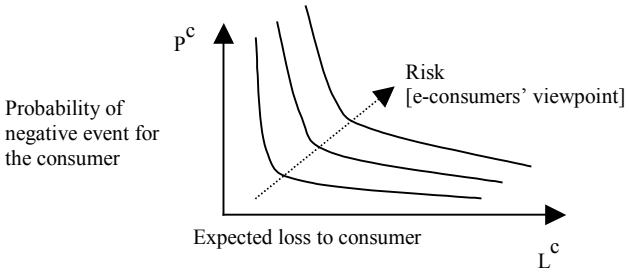



Figure 4 serves to indicate that consumers will demand greater T&C when a transaction seems to involve higher risk. The T&C solutions can act as preventive measures by diminishing the probability of adverse occurrences, or as response measures by diminishing the potential loss. As consumers will establish a limit of maximum admissible level of risk, there will be a maximum combination of adverse probability and loss that they will be willing to accept. A minimum level of T&C assurance would therefore be required for guaranteeing consumers' involvement in an online transaction of given benefit.

The supply of T&C solutions can be achieved by two types of actions: a) the individual actions taken by the single merchant, and b) the infrastructure-based actions that affect the e-market as a whole. The latter can also be called the T&C collective actions.

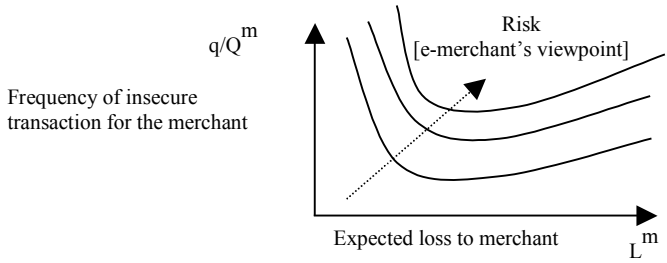
On the supply side of T&C, merchants take initiatives on an individual basis and seek to maximise their benefits by offering higher trust value to their customers. Their approach to e-commerce encompasses all of the transactions in which they could engage, rather than one transaction in particular. Within this aspect of T&C, a merchant's viability can be adversely affected by: 1) an excessive number of undesirable events that could undermine the trust of the potential customers, and 2) an excessive investment in T&C, that would lead to disproportionate costs when compared to resulting benefits, even though possibly attracting more customers. The risk for the merchant will be:

$R^m = q/Q * (L^m - B^m) = q/Q * L^m - q/Q * B^m$

Where q is the number of transactions that will affect the merchant's T&C requirements, out of a total of Q; and $L^m$ and $B^m$ are respectively the expected loss and benefits for the merchant. We will consider that the ratio q/Q is an inverse function of the investment in T&C made by the merchant (i.e., more negative events are likely to happen if fewer T&C measures are taken). $L^m$ includes the cost of those investments as well as the consequence of adverse events.

Figure 5 shows a family of T&C supply curves for a given level of benefit. For the merchant there is an optimum, albeit undetermined, level of investment in T&C solutions. Nevertheless, there is no guarantee that the merchant's optimum supply of trust will match the T&C demand from consumers. In this case, the motives of supply and demand are not necessarily complementary.

**Figure 5: Risk-based merchant demand for T&C**

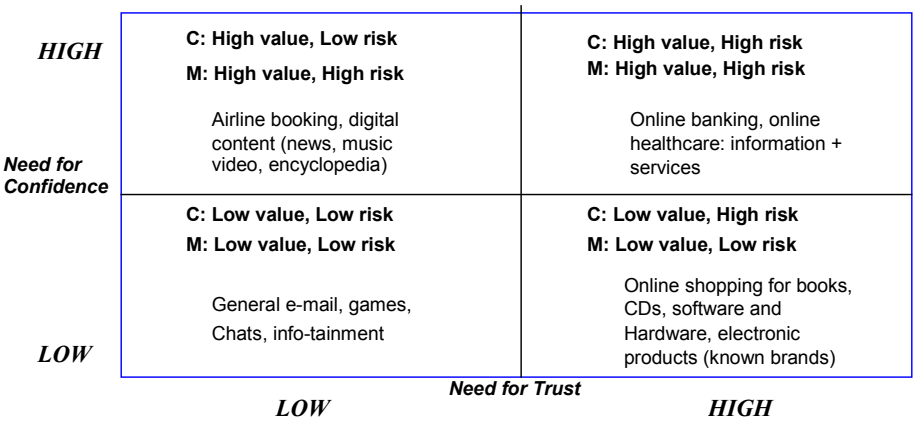



The development of infrastructure-based T&C initiatives derives primarily from the need to compensate for the disparity between consumer demand and the merchant's ability (or willingness) to adopt T&C measures, even in the absence of a full understanding of the type of collective initiatives that are required.

Figure 6 indicates levels of T&C in e-commerce transactions, and jointly examines the consumer and merchant perspectives for the same types of transaction, this in order to discern those areas T&C demand and supply coincide and where they diverge. In cases where they diverge, an initiative other than the existing market response needs to be taken. The vertical axis represents the consumers' need for confidence (i.e. their reliance on the B2C infrastructure), while the horizontal axis measures their need for trust (i.e. the required depth of relationship with the merchant). In the figure, the

consumers' perspective is preceded by the letter C:, and the merchants' perspective by the letter M:.

**Figure 6: Risk Management and segmentation of e-markets based on T&C demands**




A number of typical transactions in each quadrant of figure 6 are also presented. An analysis of these transactions suggests that the consumer and merchant perspectives differ in terms of perceived value and perceived risk of these transactions.

In the low-low segment (figure 6, bottom left) we have transactions characterized by small monetary value and potentially low negative consequences for both consumers and merchants, and therefore requiring little T&C support. Representative cases are: e-mail, messaging, online games and infotainment. Here the intervention of substantial T&C actions is not expected: both consumers and merchants might be willing to tolerate minor losses.

In the low-high segment (figure 6, bottom-right), there are low value transactions, but with potential losses that consumers might consider unacceptable. Hence merchants will be ready to invest – within certain limits – to meet the consumers' T&C demands within a competitive but profitable market. Representative cases are: online shopping of low-cost goods (books, CDs, software, hardware, electronic products). As the consumer usually pays in advance of the shipment of these goods, he incurs greater risk than the merchant. Consumers can suffer not only a monetary loss, but also leakage of their private information (credit card number, buying habits, e-mail address). The merchant is able to offer the required trust through a

combination of measures: co-branding, adoption of a trust seal, offering secure payment technology, establishing a privacy policy and commitment to a fair dispute resolution process. Building a strong brand is expensive and takes time, however. Display of customer feedback ratings and commitment to a fair dispute resolution process can be relatively cheaper while still effective in developing trust.

In the high-low segment (figure 6, top-left), there are perishable product of high value. Representative cases are: airline booking, online access to bank information, pre-paid digital content (news agencies. encyclopaedias, trade journals, video and music). The merchants suffer from the risk of losing their products by not selling them in time or through illegal re-distribution. For consumers this is a relatively low risk area since they can still obtain these products/services through traditional channels. Hence there is a discrepancy between the consumer and merchant viewpoints, opening up the opportunity for collective actions. Individual merchants have little incentive to invest in major T&C solutions, such as cryptography, since they involve costs that are very high when compared to the immediate benefit. Due to high costs required for individual merchants to establish trust, this area seems to require collective investment in an infrastructure of confidence-building mechanisms.

In the high-high segment (figure 6, top-right) the transactions are of high value and high risk for both parties. Representative cases are: online banking transactions, online insurance contracting and tele-medicine. Here, both merchant and the collective market players would expect the application of T&C solutions, although their priorities and requirements differ, and the distribution of responsibilities and costs required for implementing those solutions is not clear cut.

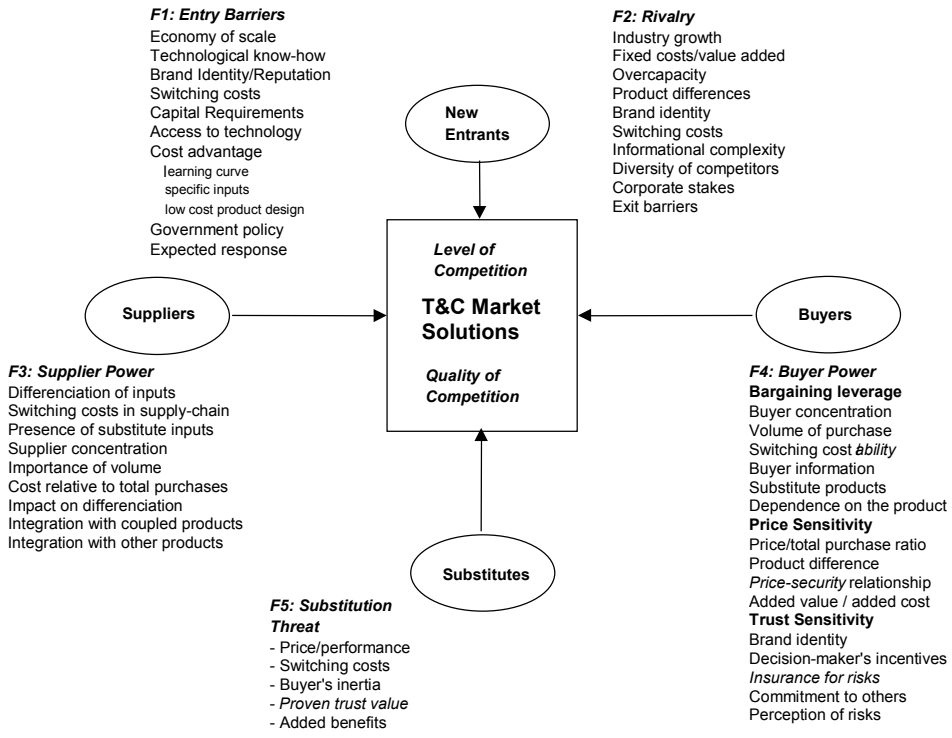
It is in this last segment where e-commerce has yet to be firmly established and primarily where the efficiency of the market forces must be analysed. Would the market by itself be able to develop cost-effective trust and confidence solutions? How would consumers and merchants behave in response of the T&C expenditure to be borne by each? Will there be competition or collaboration in this high-end T&C market? Is there any need for coordination? What is the role of public authorities and policy makers? The next section seeks to respond to some of these questions through analysis of T&C market forces.

## ■ Further Analysis of the T&C Marketplace

In the preceding risk-based analysis of e-markets, based on the supply and demand of T&C, we identified four basic e-market categories. It was revealed that the growth prospects of each category diverge due to the underlying (mis)match between supply and demand. For growth in the high-value, high-risk category, it is clear that further T&C solutions are required in the e-marketplace both at the individual level and the infrastructure level. We shall next turn our attention to the prospective emergence of T&C.

To this end, we employ Porter's five forces model (PORTER, 1980). As shown in figure 7, the object of the analysis is T&C Market Solutions, focusing on the level of competition and the quality of competition. The market is influenced by five forces, viz. entry barriers, rivalry, suppliers' power, the buyers' power and the threat of substitute products.

**Figure 7: Porter's five forces model applied to T&C**



The influence and extent of the five forces are shown in table 2. An analysis based on the key observations in table 2 is presented below.

**F1: Entry barriers**

There are a number of entry barriers to new T&C solutions emergence on the e-market. The greatest obstacle is the complexity of the types and sources of risks and their interaction. This makes it difficult to engineer effective T&C solutions by simply assembling a range of components. The market approach thus far has therefore been to offer stand-alone tools rather than overall comprehensive security solutions.

Since the existing T&C infrastructure for e-commerce is somewhat fragmented, it is relatively easy to introduce a new trust enhancing tool with some specific novel functionality incorporated (e.g. a new virus scanner). It is not however easy to establish the effectiveness of a tool on its own since the security threat arising from other sources can still dominate the T&C landscape, and investment in the new tool would be unjustifiable based on cost/perceived benefit. Moreover, on the Internet, the effectiveness of many security tools decays rapidly as new threats arise for which the old tool was not designed (e.g. new viruses).

The impact of technological complexity is that users needs to be technically capable at an expert's level to be able to assess the threats, select a set of tools by choosing among the available options, deploy them at a given time and upgrade or extend them continually. In the absence of the sophisticated knowledge required, coupled with the absence of an effective distribution mechanism for such tools, users will often take little or no explicit action at all. The effect, then, is a reduction in the apparent demand for such products by virtue of market indifference.

The switching cost and brand reputation are other barriers to entry since consumers tend to rely on a few known brands as the main criterion of trust rather than their own ability to discern the advantages offered by a new product. Again, the existing tools tend to be distributed as pre-installed when consumers purchase their computer and it is difficult for a new product to sufficiently penetrate the market and achieve the economy of scale without targeting major computer distributors. This in turn would require large capital investment not only in developing products but also in marketing them in an entrenched market. In the lack of personal knowledge to judge the product, the benefits of switching to a new product is invisible to the customer.

**Table 2: T&C market analysis based on Porter's five forces model**

| F1: Entry Barriers | F2: Rivalry | F3: Supplier Power | F4: Buyer Power | F5: Substitution Threat |
|---|---|---|---|---|
| Economy of scale | Over-capacity | Importance of volume | Bargaining leverage<br>Volume of purchase | |
| Switching costs | Switching costs | Switching costs in supply-chain | Switching cost / switching ability | Switching costs |
| | Industry growth | Supplier concentration | Buyer concentration<br>Substitute products | |
| Brand Identity/Reputation | Brand identity | Integration with other products (product line) | Dependence on the brandBrand identity | Proven trust value |
| Capital Requirements | Corporate stakes | Differentiation of inputs | Buyer information | Buyer's inertia / willingness to switch |
| Access to technology | Technological know-how<br>Product differences | Technological know-how<br>Presence of substitute inputs | Product difference | |
| Cost advantage | Fixed costs/value added | Cost relative to total purchases in industry | Price Sensitivity<br>Price/total purchase ratio | Added benefits |
| Learning curve | | Ability to innovate | Price-performance goals | Price/performance of substitutes |
| Specific inputs | | Control on inputs | | |
| Low cost product design | Informational complexity | Control on cost differentiation | Added value / added cost | |
| Government policy | Exit barriers | Integration with coupled products | Consumer rights | |
| Expected response | Diversity of competitors | Ability to improve products/cost | Trust Sensitivity<br>Decision-maker's incentives<br>Insurance for risks<br>Commitment to others<br>Perception of risks | |

Moreover, in the face of any enhanced trust value offered by a new product, the expected response from the existing T&C suppliers is predictable: they can easily add a new or superior functionality to their existing products, thus eliminating any justification for consumers switching to a new product.

Governments and regulators have so far shown little compulsion to establish minimum T&C standards for information system suppliers and service providers, or to actively encourage them to include the T&C utilities as an integral part of their products. This strikes a contrast with the approach taken by legislators over the last 30 years on issues of product safety and liability in cases of risks to consumer such as fire hazards, chemical risks and physical injuries to children. Such a lack of initiative could be due to the generally abstract nature of the T&C issues relating to e-markets where, so far, only headline issues such as harmful content for children seem to have received the policy maker's attention, leaving the market to resolve the remaining issues on its own.

**F2: Rivalry**

The rivalry force in the T&C market must be viewed from two perspectives: co-operation and competition. Co-operation needs to occur through use (and definition) of common standards and protocols so that products be interoperable, the development of broader T&C solutions and the incorporation of T&C solutions within IT systems and information infrastructures.

Competition occurs at the level of improved performance, range of functionality, robustness, integration, cost and ease of use. Ease of use is crucial due to users' lack of knowledge of the underlying technology. For this same reason, brand identity remains a strong determining component of rivalry. The companies operating in the sector are at the forefront of innovation and command leading edge technological know-how. Co-branding with other related products and alliances with large IT players provide further consolidation of this force.

Exit barriers in the software industry are low, and the competitive landscape can shift rapidly due to bankruptcies, acquisitions and mergers. Another key element of competition is agility and speed in offering enhanced functionality, although lack of consumer ability to discriminate acts as a deterrent to proactive pursuance this objective. Due to the specialised nature of T&C products, apart from certain virus scanning applications, the market for consumer T&C products remains undeveloped whereas that for corporate T&C products continues to develop parallel to the underlying technology. The diversity of competitors therefore varies. It has been

primarily for B2C applications such as secure payment systems that the corporate sector has invested in developing and deploying T&C tools.

Given that the T&C market is still immature, there is no question of over-capacity on the supply side. Due to the potential growth of the T&C market in a variety of common applications, rivalry among the competitors is expected to grow, offering high-value, high cost solutions such as digital signatures, digital passports and smart cards with bio-identification, with potential large-scale application in the financial and healthcare sectors. Since T&C depends partially on familiarity, the cost of switching to a competitor's products is more psychological rather than real.

**F3: Supplier power**

T&C providers exist at various levels on the e-market: network infrastructure, network services, ISPs, computing platform (hardware and operating system), browsers and other end-user applications. In addition to this, interacting parties such as e-merchants are expected to adopt a variety of T&C enhancing tools that rely on protocols used to boost confidence in e-commerce.

Within such a broad spectrum of trust applications, the market of demonstrable benefits, rather than the implicit benefits, drives suppliers. Along with this is the fact that certain, more complex risks are easier to demonstrate and explain to customers than others. Thus it is relatively more attractive for the supplier to offer a virus scanner, for instance, than a port scan blocker: a tool used to detect a problem rather than one to prevent one. For new security technologies, the importance of volume of the mass market has a lower priority than the high value-added business market. It is expected that, if left to the market forces alone, the T&C market will go the way of technology distribution in many other technological sectors where solutions are first offered to the business sector, and only later find their way into the consumer sector.

In any case, technological know-how is the key input for T&C solutions, and some countries are known to have better a record for developing T&C technologies (including the underlying mathematical models) than others. Looking at recent examples of solutions, however, (e.g. anti-piracy software in the music industry) it seems that there is no geographical concentration of T&C solutions' input skills nor of end solution providers. In other words, there

exist varied sources of technological know-how and substitute inputs for T&C solutions.

Although there seem to be no formal studies available on the nature of the T&C supply chain, the chain clearly exists and involves several players. Although it is logistically easy for a computer manufacturer to switch from one T&C utility to another, the final choice is governed by a combination of business and performance factors: independent press reviews, volume and cost of licenses and prior relationships between the parties.

In the consumer IT sector, there is no hard or direct evidence of the relative importance of the basic performance attributes of the product/service versus the specific T&C attributes. However, considering that marketing efforts in the IT sector focus primarily on the basic functional attributes such as CPU speed (MHz/GHz), memory, bus access speed etc, rather than on robustness, reliability and security, it appears that there is little motivation for suppliers to enhance the T&C attributes of their products/services. As we mentioned earlier, it is the integration of basic IT products with other T&C products that is currently lacking.

Relative cost for T&C products in the industry is not a specific source of supplier power since the input skills are generally widely available, and experts can easily move from one competitor to another. Hence the ability to innovate lies in building a stable team of experts and turning their knowledge into marketable products. Integration of T&C tools with a wide range of coupled products is, however, key to supplier power. an encryption utility, for example, can be deployed in a range of applications involving secure storage or voice, data or text transmission.

**F4: Buyer power**

Buyer power is normally associated with two aspects of consumer behaviour: bargaining leverage and price sensitivity (GUPTA, STAHL & WHINSTON, 1999). We believe that in a commercial transaction, particularly online, bargaining ability and price sensitivity alone do not influence buyer behaviour, and this because trust is a prime component of the nature and extent of consumer involvement in e-commerce. We therefore include an additional element: trust sensitivity.

Buyers' trust sensitivity has a number of attributes. First it depends on their perception of risks. Buyers can be justifiably sceptical, unduly afraid

(even paranoid) or glibly confident about carrying out a transaction. Thus their ability to rationally determine the risks (or at least understand them) is a key, regardless of their ability to bargain or their preference for a lower price. The risks can include personal losses or derive from obligations or commitments to others. In some situations, if buyers are able to contain probable losses, e.g. by obtaining insurance against certain types of risks, they will be less sensitive to a risky transaction. As a T&C building strategy, creating a chain of mutual obligations or commitments to others has worked as a successful mechanism in the insurance industry, and this could well constitute a model to adopt for e-commerce as well.

Buyers' price sensitivity in the online market is somewhat exaggerated. For T&C products, it is hard to determine consumers' price sensitivity since they cannot generally evaluate the T&C attributes being offered by competing products. It appears that consumer T&C products tend to have a price range that comparable to pricing trends in the consumer software industry.

Similarly, there is no evidence of price bargaining being used directly between a merchant and consumer for T&C products – such as virus scanners and firewalls – unlike classic consumers products that are offered through consolidators (e.g. letsbuyit.com). Since T&C products can be bought by consumers on a one-off basis, volume purchase discount is not an option for consumers, as it is for businesses. This type of product has now begun to be bundled by system integrators (e.g. for home PCs), however, and does therefore not provide consumers with any real commercial choice.

The availability of substitute products can be a key factor of consumer power, again based on the evidence from software industry. For technical products, many consumers tend however to rely on independent advice such as technical reviews or sales staff. They tend generally to switch from one product to another comparable one only when they have had a bad experience. (Some may even stop e-shopping in the case of a severe loss of trust and confidence). First time consumers tend, however, to choose the products based on either brand reputation or personal recommendation, or on their confidence in the regulation (e.g. safety regulations of the airline industry).

This last criterion is a significant indicator of how regulation can support T&C in a fledgling market, e.g. online banking, even if it cannot sustain T&C on its own. Similarly, brand identity alone is not enough to inspire T&C. It is

common knowledge that after an online banking security breach, the confidence in online banking transactions suffers a shock. A spate of bad publicity can damage the general reputation of an entire sector, confirming the importance of the general confidence that the customer has in a sector as a whole, even if there has been no personal loss of trust in a particular operator.

One of the online market's greatest contributions to buyer empowerment is information. It is believed that an average online buyer tends to be more informed about the product s/he buys compared to an average offline buyer.

Although we have theoretically analysed the trade-off between risk and benefit for online shopping, empirical studies need to be carried out to determine the precise nature of the relationship between buyers' trust sensitivity and price sensitivity.

**F5: Substitution threat**

Lastly, we turn our attention to the threat of substitution in the T&C market. Existing T&C products depend on the underlying e-commerce and information infrastructure. Many products will not be needed if there is a change in the environment's architecture. Secure payment systems, for instance, could be altered as a result of changes in the form of e-money and its management.

Other threats of substitution such as switching cost to another product, buyers' inertia or willingness to switch, and price/performance benefits have already been referred to above. One crucial substitution threat still remains for all e-merchants (more than in the offline world): the proven trust value of a product. Any substitute product will need to prove its enhanced trust value to replace a weaker-trust product. Due to the abstract nature of this attribute, it remains the greatest challenge to be able to define metrics for proven trust value.

## ■ Towards a T&C Strategy for E-Commerce

The analysis above has underlined the following points:

- There is an unavoidable mismatch between the supply and demand of T&C solutions in certain situations, due to divergent perspectives on the risks that consumers and merchants might encounter in the B2C transactions.
- There is a mismatch between consumers' and suppliers' capacity to influence the emergence of T&C solutions.
- The market is affected by third parties (such as government policy, consumer rights groups, co-branded products, proven trust value and added benefits of substitute products) that might interfere with the market forces.

### T&C architecture

A suitable approach to the deployment of adequate T&C solutions has to consider the various concerns and viewpoints of the different B2C players. For these reasons, T&C need to be developed systematically through a concerted approach if rapid growth of e-commerce is to be achieved. As argued earlier, T&C will not occur by chance and will need to be nurtured in e-marketplaces. T&C solutions should be the object of a deliberate process of building, enhancing and maintaining. A solution that might be adequate today, might be unable to support users' T&C requirements tomorrow.

A typical process for this sort of T&C solutions development should integrate the following phases:

**1.** Establishing T&C protocols: At the technical level, e-commerce involves data processing and communication. This data will include users' information assets, leading to their T&C requirements and the way in which they are satisfied by the other parties. T&C protocols would be languages used for defining the rules and behaviour for governing information asset management. Protocols could have different levels of semantics and should be understandable by all the nodes involved in an e-commerce infrastructure. T&C protocols will therefore be an agreed-upon means for communicating between two e-commerce agents, allowing them to guarantee a transaction's required T&C attributes.

**2.** Developing reliable T&C mechanisms: The protocols should be designed through a structured series of technical and organisational initiatives. T&C solutions will consist not only of standalone applications or devices but also of structured, interoperating systems based on the above protocols. T&C solutions are created by combining social and business processes with technical elements.

**3.** Implementing assured T&C by technological means: At some point, best practices and dependable technologies will no doubt be deployed for implementing the T&C mechanisms. Implementations could therefore vary and change depending on technological developments.

## Current T&C tools

We will next use the previous scheme for analysing the typical T&C tools that are currently offered on the marketplace. The range of T&C tools can be classified in several functional groups: user authentication, workstation protection, security analysis, privacy enhancing technologies (PETs), cryptography, network security protection and redress mechanisms (KHARE & RIFKIN, 1998).

- Typical "User Authentication" tools are password/PIN management, hardware tokens for identification, one-time password, biometrics. They vary in terms of sophistication and level of security protection. Most of these tools are technologically simple and application specific, or are only valid in a particular environment (e.g. relationship of customer with a bank). They require little technical capability on the part of the user, and can be easily adopted and understood. Nevertheless, more sophisticated tools, such as biometrics, due to their cost and complexity, will tend to be used in more social situations and in several e-commerce situations. Here there is a need for some agreement at the protocol level. There is currently a lack of broadly accepted solutions, and we can predict that biometrics will not gain market acceptance if they are not supported by a basic agreement at the protocol level.

- Typical "Workstation Protection" tools are explicit access control/privileges, authorised logging, anti-virus (including worms, trojan horses), monitors (resource use, network traffic and connections, file access), integrity verification, intrusion detection systems. Most of these solutions are implemented as commercial tools that require a certain level of technical proficiency on the part of the user. Their weakest point is the lack

of compatibility among them, added to which when users cannot access the benchmark standards for such tools, they have difficulty in judging the quality of each product. Markets are therefore limited and can only progress when the users are technically capable, and prepared to install each particular solution.

- Typical "Security Analysis" tools are vulnerability identification and scanning, probe and mapping tools, intrusion analysis, traffic analysis tools (protocol violations, packet traffic). These tools require a highly competent user and it cannot be expected that lay consumers will adopt (or even understand the need for) them. These tools would have to be integrated into other more composite solutions. There is some remote possibility that major commercial stakeholders could offer such a solution, integrated with their own commercial tools (e.g. browser, operating system). In that case, a lack of general definition of standards will undoubtedly diminish the competition for innovative solutions and the customer may be forced to accept a poor quality solution.

- Typical PETs are cookie managers, advertisement blockers, anonymizer, PET tools, privacy networks (pseudonym, multiple identities), identity guards, avatar and persona management. Some of these tools are simple to install and use though not well understood by lay users. Most of them (mainly those that rely on networks) are dependent on agreed protocols for inter-operable solutions. There is an ongoing discussion in W3C on the principles that all privacy-related tools should respect. The various utility producers could then translate these principles to technical solutions for online privacy to be used by web portals or individual e-commerce sites. Here again, the problem is inter-operability. The more complex solutions can only be achieved if based on a shared definition of common protocols and mechanisms.

- Typical "Cryptography" tools are checksums, message digests, encryption, PGP/RSA, Digital signatures, PKI, certificates. All of them are highly mysterious and difficult to comprehend for the lay consumer. E-commerce cannot expect their wide adoption if not integrated into other desktop tools. Moreover, some solutions (such as PKI) can only happen if supported by a social infrastructure. This is a characteristic area where the lack of collective action prevents the activation of the extensive application of feasible technological responses to concrete problems. In this context, it is worth noting that the Dutch government has launched an initiative to issue digital passports and digital signatures to all its citizens by 2005.

- Typical "Network security protection" tools are Proxies, firewalls, IP admin, content filters. Although some of these solutions are beginning to be

integrated into common desktop environments, most of them are still beyond the comprehension of the consumer. From a practical standpoint, if consumers are expected to implement some network security on their PCs, this can only be ensured through bundled solutions. Even for advanced users, there is a problem of identifying effective products on the market. This can only be supported by common technical quality standards.

- Typical "Redress Mechanisms" are codes of conduct, self-regulation, co-regulation, alternative dispute resolution (OECD, 2001b), cross-border e-commerce law. These are the emblematic social solutions, and still in their development phase. Although they are not technically complex for the consumer, the details for accessing these mechanisms are complex, expensive and time consuming. Again, the end result is their inaccessibility for the common consumer. For cross-border e-commerce, it is evident that they will require a concerted and complex collective action to develop and support them.

**Figure 8: A map of T&C tools in personal-collective action**

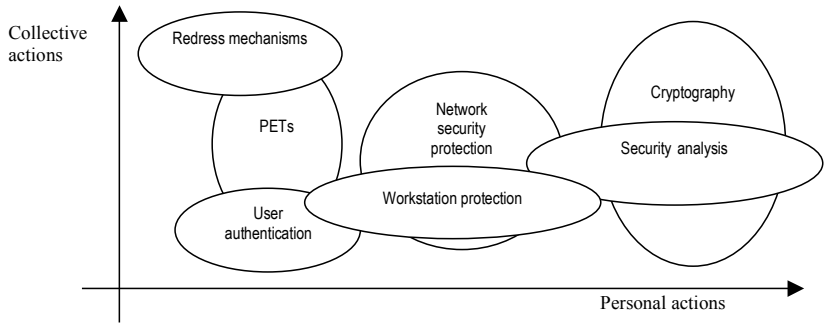



Figure 8 illustrates the different T&C tools distributed in an area defined by personal and collective actions. Personal actions refer to the amount of skills, knowledge and effort required from the individual user to enable him use these tools. Collective actions refer to the extent of societal actions (e.g. agreement among the different suppliers in an industry, or among the players of a value chain) needed for the implementation and deployment of the tools at the infrastructure level.

**A trust and confidence strategy for B2C**

Based on the previous statements, it becomes clear that an adequate supply of T&C solutions matching the demands of all B2C parties is key to developing e-confidence. Development and deployment of these solutions requires: 1) personal actions on the part of the consumer and the trader, and 2) collective actions on the part of the industry and the e-governance players.

- *Personal actions*

For T&C solutions to be adopted widely by consumers, they should be easy to install and use, and consumers should be able to appreciate the tangible benefits from their use in terms of the protection of personal information assets and capabilities.

- *Collective actions*

On the supplier and regulatory end there is a need to outline a concerted T&C strategy in a public-private partnership to promote the growth of B2C e-commerce.

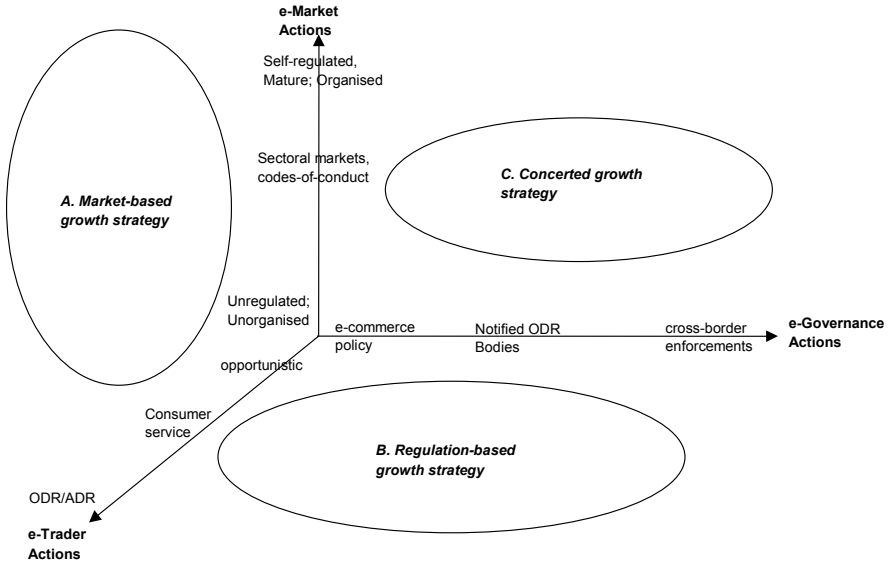
Figure 9 shows three options for T&C strategy for the information society in general, and e-commerce in particular.

It shows that the market-based growth strategy (A) only relies on the actions by the e-trader and the e-market. In this case, the growth rate cannot be predicted, even though the solutions can be highly innovative, provided genuine competition exists. Unfortunately, this is not the case with the IT sector where the PC market has a powerful monopoly, and the network equipment market an oligopoly. If left to self-governance, the adoption of satisfactory built-in T&C solutions for consumers could take an indefinite amount of time, at best. Worse still is the scenario where, in the absence of choice, the pre-packaged solution could lead consumers into a false sense of security.

The regulation-based growth strategy (B) relies on extensive regulation and on e-traders' compliance. This strategy is fundamentally unworkable in a sustainable manner since regulation tends to lag considerably behind technological developments. Moreover, regulation encourages market players to comply with a minimum-possible level of quality standards, without promoting innovation leading to highest achievable standards and thus impeding dynamism and competitive growth.

A concerted growth strategy (C) based on joint action by the regulators and the market is expected to counterbalance the ill-effects of the previous two strategies, while delivering the benefits of both: guaranteed T&C standards, inter-operable solutions, cross-border e-commerce, private-public partnerships and, ultimately, efficient technical solutions for T&C within a predictable time frame.

**Figure 9: Options for a T&C strategy in B2C e-commerce**




## ■ Conclusions

The need to establish consumers' trust and confidence is essential for the growth of B2C e-commerce. This paper has addressed the nature of trust and confidence (T&C) in e-commerce, focusing on business-to-consumer (B2C) transactions. The concept of information assets and e-capabilities was introduced. The issue of trust was analysed in terms of the value attached and the risk posed to citizens' information assets and e-capabilities. Trust and confidence were treated respectively as individual and collective initiatives aimed at developing and sustaining a B2C relationship.

We have analysed the influence of the market type on the consumers' attitude, as well as merchants' attitudes towards risks and their willingness to

engage in a transaction. The discrepancy between the supply and demand of risk was revealed to be an impediment to e-confidence, and the area where infrastructure-level action was required to build confidence.

A segmentation of e-markets based on T&C relationships was presented. It was shown that for low-risk, low-value transactions such as e-mail and infotainment, the market action alone was adequate to sustain growth. On the other hand, for high-risk, high-value transactions such as online banking or health services, the consumer must simultaneously have high trust and high confidence in the marketplace, and that the growth of this sector cannot be achieved without collective action at the infrastructure level.

A further analysis of the T&C marketplace was presented based on Porter's Five Forces model. Consumers' and suppliers' ability to influence the growth of T&C solutions were found to be imbalanced, thereby underlying the significance of the influence of third parties such as governments and coupled IT products.

An analysis was carried out on an inventory of currently available T&C tools and mechanisms. They were mapped in the personal-collective action area, in order to highlight the level of effort required on the personal level and the collective social level to deploy these tools. We observed that a majority of T&C tools were still incomprehensible for the common user, thus preventing personal action on their part. Many tools require concerted social actions in terms of common standards and interoperability.

These conclusions led us to propose a three-tier T&C architecture for e-commerce: establishing protocols, developing reliable mechanisms and implementing them through secure technological means. We showed that different types of markets require different strategies for building trust and confidence in e-commerce. These strategies involve three dimensions: 1) e-market actions, 2) e-trader actions, and 3) e-governance actions. It was suggested that a concerted growth strategy involving all three players was required to promote innovation, interoperability and timely delivery of T&C solutions to consumers.

**References**

CommerceNet (2000): *"Barriers to Electronic Commerce",* CommerceNet.

CVETKOVICH G. & LÖFSTEDT R. (Eds): (1999): *Social trust and the management of risk*, London: Earthscan.

FREWER L.J., HOWARD C. & SHEPHERD R. (1998): "Understanding public attitudes to technology", *Journal of Risk Research*, vol. 1, pp. 221-235.

GBDe (2000): "Statement of the United States and the European Union on Building Consumer Confidence in e-Commerce and the Role of Alternative Dispute Resolution", http://consumerconfidence.gbde.org/us_eu_statement.html, December 18.

GUPTA A., STAHL D. O. & WHINSTON A. B. (1999): "The economics of network management", *Communications of the ACM*, Vol. 42, No. 9, September.

JONES S., WILIKENS M., MORRIS P. & MASERA M. (2000): "Trust requirements in e-Business", *Communications of the ACM*, vol. 43, no. 12, pp. 81-87, December.

KHARE R. & RIFKIN A. (1998): "Trust Management on the World Wide Web", *First Monday,* http://www.firstmonday.dk/issues/issue3_6/khare.

LYNCH J. (2000): *Action-based model of organisational evolution in the e-commerce environment,* MBA Thesis, University College Dublin, August.

OECD:
- 1997: "Business-to-Consumer Electronic Commerce, Survey of Status and Issues", OCDE/GD(97)219.
- 2000: "Building Trust in the Online Environment: Business to Consumer Dispute Resolution", DSTI/ICCP/REG/CP(2001)2, OECD Conference, The Hague, The Netherlands, 8-9 December.
- 2001: "Consumers in the online market place, OECD Workshop on the guidelines - One year later", DSTI/CP(2001)5, Berlin, Germany, 13-14 March.

PORTER M. (1980): *Competitive strategy: Techniques for analyzing industries and competitors*, New York: Free Press.

SCRIBBINS K. (2001): "Should I Buy? Shopping online 2001: An international comparative study of electronic commerce", *Consumers International*, http://www.consumersinternational.org/CI_Should_I_buy.pdf , ISBN 1902391365.

SIEGRIST M. & CVETKOVICH G. (2000): "Perception of hazards: The role of social trust and knowledge", *Risk Analysis*, vol. 20, pp. 713-719.

TEMMERMAN D. (1999): "Security and trust in electronic communication", Conference on Modern Government – *Working across Boundaries*, http://www.hos.horizon.ie/presentations/mg030699/temmerman/sld005.html, Dublin, June.