Oxford Internet Institute, Research Report No. 1, April 2003

Economics of Trust in the Information Economy: Issues of Identity, Privacy and Security*

Gerardo A. Guerra and Daniel J. Zizzo
Bounded Rationality in Economic Behaviour (BREB) Unit
University of Oxford

William H. Dutton and Malcolm Peltu
Oxford Internet Institute
University of Oxford

* This paper has been jointly prepared for the Organisation for Economic Co-operation and Development (OECD) by the BREB and OII of the University of Oxford. The lead role was taken by Gerardo A. Guerra, who wrote the first draft. The final version was revised and edited by William Dutton and Malcolm Peltu, based on input from Ann Carblanc, Graham Vickery, Francis Aldhouse, Gerardo Guerra and Daniel Zizzo. The authors thank the OECD for their support of this scoping paper.

Contents

1. Introduction

Total worldwide e-commerce revenues have been estimated[1] to have reached about US$2.3 billion in 2002, with a predicted growth rate for 2003 of 69% in the U.S. and higher in developing economies. Internet-generated revenue did not generally slow down with the global economy around the turn of the century. This indicates the increasing importance of electronic marketplaces, where the potential savings and other opportunities have focused attention on the factors that might facilitate or constrain the continued expansion and diffusion of e-commerce.[2]

A number of studies have identified a lack of trust as one of the main possible constraints on e-commerce, particularly in terms of consumer protection and other worries that focus on three main aspects of trust in electronic transactions: identity, privacy and security[3]. The potential for difficulties in establishing the authenticity of the identity of a consumer or online business is one of the characteristics that distinguishes trust issues in electronic environments from most other contexts. For consumers, identity is bound up with concerns about privacy and data protection that have been highlighted ever since computers emerged as an important technology in the 1960s. This has led to the development of guidelines[4] and legislation[5] on privacy and data protection, including security safeguards for information held on information and communication technologies (ICTs).

Although the elements that contribute towards building trust can be identified in broad terms, there are still many uncertainties around the definition of trust in relation to the use of ICTs, such as the Internet, and in developing strategies for enhancing consumer trust in e-commerce. Moreover, there is debate over whether e-commerce might be undermined or enhanced by the adoption of certain strategies designed to enhance trust. The rationale for seeking to develop strategies to enhance trust, including the use of Privacy-Enhancing Technologies (PETs)[6], online Alternative Dispute Resolution (ADR)[7] procedures and other products and services, is sometimes based on the belief that increased trust will reduce overall transaction costs and risk[8]. At the same time, the growth of e-commerce could be inhibited by particular approaches to enhancing trust, for example if strengthening the level of privacy protection or identification procedures is achieved using methods that create

---

[1] Forrester Research estimates.

[2] For example see “Measuring the Information Economy 2002”, OECD, 2002. Chapter 4

[3] For example Ben-Ner and Putterman (2002, p. 24) report survey findings in 2001 that 60% of adults who go online in the U.S. do not do business on the Internet due to privacy and security concerns, and 86% of those who do business have concerns about giving out personal information. See also “IBM-Harris Multi-National Consumer Privacy Survey”, *Privacy & American Business*, January 2000.

[4] For example OECD Privacy Guidelines, see OECD document DSTI/ICCP/REG(2002)3/REV1

[5] For example UK Data Protection Act 1998.

[6] For example DSTI/ICCP/REG(2001)6/FINAL in OECD special Forum Session on PETs.

[7] For example OECD documents: *Resolving E-Commerce disputes Online: Asking the Right Questions about ADR*; *Legal Provisions related to Business-to-Consumer Alternative Dispute Resolution in relation to Privacy and Consumer Protection*; DSTI/ICCP/REG/CP(2001)2 on OECD/Hague Conference on International Law/International Chamber of Commerce conference on ADR.

[8] For example OECD document DSTI/ICCP/IE/REG(2002)2/REV1. See Lorenz (1999) for an alternative discussion of the relationship between trust and traditionally-interpreted transaction costs.

unacceptable increases in costs or operational burdens. Finding an appropriate framework that balances the need to offer consumer protection while maintaining e-commerce growth involves many interrelated uncertainties: economic, psychological, institutional, technical and legal. Unravelling and gaining a better understanding of these issues requires social and economic research that has a broad perception of the co-evolutionary nature of human, organisational and technological systems[9].

This paper discusses some of the major issues surrounding trust in e-commerce, by first defining the concept of trust before identifying and examining some trust-enhancing strategies, products and services and their impacts. The conclusion uses this review to highlight key future research priorities aimed at gaining theoretical and practical insights into how the needs of consumers, citizens, business, government and other stakeholders can be taken into account in a balanced way when developing a strategy for building trust in electronic markets.

2. Trust, Identity, Security and Privacy: Complementarity or Tension?

Trust has been studied at length in many disciplines. Pettit (1995) makes a distinction between the attribute of trust and the behaviour of trust. Misztal (1996) identifies different types of trust according to their role: commercial, problem solving, informational, knowledge and identity. McCullagh (1998) defines three types of trust: behavioural, business and technology, while Kini and Choobineh (1998) make a distinction from three different perspectives on trust: individual, societal and relationship. Baron (1998) identifies trust as a good, a belief and a behaviour. As no consensus has emerged on what trust means, this paper begins by defining (and delimiting) the concept of trust used in this study, before proceeding to examine its role in the information economy.

The Oxford English Dictionary defines trust, in part, as "[…] a firm belief in the reliability or truth or strength etc. of a person or thing. [...] a confident expectation. […] reliance on the truth of a statement etc. without examination." A common factor in this and other definitions of trust is the prevailing degree of confidence, more specifically the degree of uncertainty (e.g. Sobel, 1985; Gambetta, 1990; Kollock, 1994; Sako and Helper, 1998). Without uncertainty, trust is not a significant issue because certainty means the outcome will be the same whether or not a trusting act was involved. Although uncertainty is an important aspect of trust, it is not sufficient to produce trust. For example, a consumer may choose to enter into a transaction to buy a good of unknown high or low quality.[10] By purchasing from the seller, the consumer is not necessarily signalling that she trusts the seller; if the price of the good is lower than the buyer's reservation price for a low quality good, buying it becomes a rational choice, from the perspective of pure self-interest, not a trusting act. Therefore, more than uncertainty is required to define trust and fully characterize a trust situation.

---

[9] For example see Dutton (1999) for a discussion of the multiplicity of interrelated factors affecting how ICTs shape access to people, information, services and technologies.

[10] Akerlof (1970) presents a classical analysis of this case and of how it may lead to market inefficiency and possibly market breakdown.

This study will use the definition of *the act of trust* by Bacharach and Gambetta (2001): "a person *trusts someone to do X* if she acts on the expectation that he will do X when both know that two conditions obtain: if he fails to do X she would have done better to act otherwise, and her acting in the way she does gives him a selfish reason not to do X". The first condition entails *exposure* from the trustor (by allowing the trustee to make her worse off), while the second condition implies *temptation* for the trustee (as he can profit from violating trust). This establishes that trust requires three conditions: uncertainty, exposure and temptation. A typical trust problem is exemplified in Appendix I.

Empirical evidence relating to the precise impact of the Internet and other ICTs on trust is still sparse and sometimes contradictory. Uncertainty in electronic interactions and transactions might be higher than in face-to-face exchanges because the reduced communication channel could make it harder to establish identity by making it more difficult to observe important non-verbal physical cues[11]. This also makes imitation cheaper and easier. However, while acknowledging that less face-to-face interaction, increased impersonality and lack of social context[12] might lead to a reduced ability to establish trust online, Ben-Ner and Putterman (2002, pp. 14-16) argue that this could be offset by the greater availability of high-quality information via the Internet, for example through online product comparisons and specialised expert chat rooms. But this view could be questioned by the large dispersion in prices found in online shops (Morgan, Orzen and Sefton, 2001) and the fact that inter-shop competition appears more in advertising outlays than in prices (Latcovich and Smith, 2001). The 'comparisons' and 'experts' accessed via the Internet can also be deceiving, for instance if they are posted by fraudsters mimicking genuine sources.

These kinds of uncertainties make the establishment of identity very important in e-commerce transactions, in order to determine who you are dealing with, verify his reputation and create accountability. Legal responsibility for payment, promises made and merchandise delivery also requires the establishment of identity for both parties in a transaction, which requires data collection. In this respect, data collection can help trust by creating a legal bond between the parties involved. However, the collection and availability of data can create problems of trust in terms of privacy because individuals may be wary of data surveillance, or of the secondary use of that information. Indeed, privacy is repeatedly identified as a concern that prevents consumers from using the Internet for

[11] For example Wallace (2001, p. 51) notes how "practically all the cues people attempt to use to detect deceit are non-verbal" and the inability to use them makes the Internet a place where "it is so easy to lie and get away with it". Some empirical research reported by Ben-Ner and Putterman (2002, pp. 18-19) supports this conclusion, but other experiments question it, for example the finding of Bochet, Page and Putterman (2002) that the increased trust in face-to-face interactions may be explained by the ability to use language to frame a problem as one capable of cooperative group resolution, which can also be achieved online (e.g. where chat rooms and other forms of social interaction are available). Investigating the relevance to e-commerce of such studies of more general psychological and social dimensions of the Internet is part of the future research agenda recommended later in this paper.

[12] Donald MacKenzie (1999) proposes that uncertainty about a technologically-based artefact is greatest among those most with most 'social distance' from the technology, as well as among the insider's closest to it.

transactions[13]. In this way, there is a "trust tension" between privacy and identity: absence of data impedes trust as accountability is limited, but data gathering creates trust problems regarding the use of the data in question and intrusions on privacy. Given that there is now a recognition of a "universal" right to privacy[14], and that information technology gives people and organizations the power to gather and disclose vast amounts of information, those who collect and disseminate data should be responsible for maintaining privacy. However, protection of the right to privacy has not always been implemented in ICT systems because "privacy is part of ethical codes but not consistently part of computer code" (Camp, 2000, p. 132).

One trust-enhancing product that seeks to ameliorate this tension is the use in e-commerce transactions of various forms of digital "tokens", sometimes called "e-cash" or "digital cash". These are obtained from, and managed by, token suppliers. The electronic tokens are then used instead of credit cards and other "real" money in online transactions. The use of these tokens focuses identity and data collection requirements on the relationship between the consumer and the token supplier, rather than each business-consumer interaction. Other innovative forms of payment are also emerging, such as the "Amazon Honor System". This allows visitors to a web site to make voluntary payments to gain access to various products and services that the site owner feels cannot, or should not, be sold at usual commercial rates. The visitor to a web site using this Honor system can be linked via a paybox to a PayPage on Amazon.com, where Amazon's patented 1-Click technology is activated to make the payment to the owner of the visited web site. Amazon manages consumer privacy and security controls, as well as the accounts of the web site owners (who are charged a small management fee, whereas as the consumer is not currently charged anything). Similar payment systems are being used by "shareware" software developers, who receive voluntary payments for a product that can also be acquired at no cost. Despite the potential economic incentive to 'free-ride' on the information paid for voluntarily by others, this payment method works for some sites by enabling some consumers to fund those product and service providers they use, while leaving the site generally open to all.

Trust can also be enhanced by making effective use of the vast amount of information accessible on the web, in chat rooms and through other Internet-based interactions (e.g. Ben-Ner and Putterman, 2002, pp. 25-26). People who have the appropriate skills to collate and interpret online information can enhance their ability to authenticate the value of products, services and information, thereby enhancing trust. However, others could drown in the flood of information, creating an increased risk of negative outcomes from using the Internet that cause a general loss of trust in the e-economy. This raises concerns about inequalities caused by variations in the skills of different social groups.

---

[13] For example "E-commerce and Development Report", United Nations Conference on Trade and Development, 2002, p. 151; "No Thanks, We Prefer Shopping", The Economist, Jan. 2, 2003; and "Wanted: Reassurance about Online Insurance", BusinessWeek Online, Sep. 2000.

[14] Article 12 of the United Nations Universal Declaration of Human Rights (1995) states, "No one shall be subject to arbitrary interference with his privacy."

3. Economic Aspects of Trust in Electronic Commerce

Kenneth Arrow (1971) points out that even though it should be "rational economic behaviour" to cheat or disregard trust, agents exhibiting trust and confidence are an essential part of a successful economy. Arrow also recognises that, in order to improve efficiency, trust can be enhanced via non-market controls, which can be endogenous (the inherent qualities of individuals) or exogenous (provided by third parties, e.g. through the approaches discussed in section 4 below).

According to Bacharach and Gambetta (2001), there are two types of endogenous trust properties of an individual: *krypta* (unobservable properties) and *manifesta* (observable properties). As already discussed, the reduced channel of communication available in electronic interactions is likely to make it more difficult to detect facial expressions, eye movement, gestures and other non-verbal *manifesta* that are important in establishing trust, which could make online consumers and businesses feel they are more open to "mimics" who pose as something they are not. At the same time, *manifesta* can also be used to deceive. However, when consumers feel that "seeing is believing", establishing trust in an online business can be more difficult, even when access to information and expertise via the Internet can also be used to enhance trust and detect deceit. Given the perception of the reduced possibility to determine individual's qualities in electronic interactions because of the narrower communication channel, the establishment of identity using exogenous third-party controls becomes more important.

Increasing the overall trustworthiness of people may require a long-term cultural change, possibly involving a change in preferences (as suggested by Zizzo, 2003) or through a change in the way that agents perceive the decision problem, for example if they think they are being trusted *and* they are psychologically responsive to the trust placed in them (Bacharach, Guerra and Zizzo 2001; Guerra and Zizzo, 2003). Putting the controls in place to transform unwarranted trust situations into ones of warranted trust may be easier and speedier to do, and may be one of the benefits of introducing controls. However transparency in the establishment of institutions of control is important to allay fears that there is no-one to control the controllers.

The next section discusses examples of possible solutions to the electronic trust problems highlighted above.

4. Enhancing trust in an e-economy

A variety of strategies to enhance trust in e-commerce have been developed. Four of these are particularly suited to meeting the demands of the information economy: identity establishment, third-party certification, loss insurance and legal frameworks.

Establishing identity

Given that imitation in electronic media is inexpensive, consumers and businesses need assurance regarding the identity of the business or person they are interacting with. For instance, in a typical business-to-consumer commerce transaction, it is important to establish both the personal authentication of the consumer by the online supplier and trust in the identity and reputation of the supplier by the consumer. In such an e-commerce transaction, one way to establish the consumer's identity is through the use of a verifier

(e.g. Netscape User Identity) to authenticate the identity of an agent. This kind of product reduces uncertainty, which is one of the main trust factors. The use of authentication impacts privacy, as the verifier has to maintain records of requests for verification, in case a dispute arises. However, this "trail" contains detailed personal information, so consumers are sometimes worried about the effect this has on their privacy. According to a survey[15], 70% of consumers in the US fear that privacy of their personal data is more at risk with the Internet than with the telephone or postal services. Some companies have developed PET-based services to address this fear. Citibank, for example, issues "virtual account numbers" to its clients, which are like virtual credit card numbers specific to individual transactions. This enables the identity of the client to be hidden from the seller, with only Citibank retaining a record of the buyer's identity (as it would in any other financial transaction). This is also an example of the role of third-parties in trust-enhancement processes; the next section identifies other ways in which third parties can influence trust.

Third-party certification

Certification can provide information that goes beyond just the identity of an agent, for instance using products that provide information on aspects such as reputation (e.g. the rating of individual consumers made by Amazon and e-bay) and signals of external approval (for example "quality" seals and trustmarks for web sites, such as the VeriSign secure seal and TRUSTe privacy mark). The main objective of third-party certification is to reveal information about characteristics that cannot be otherwise observed by individuals (see Guerra, 2001 for a detailed discussion on the subject). This kind of certification can reduce both uncertainty and temptation to violate trust (for example when the reputation reported indicates that trust is warranted). Advantages in terms of these two key trust factors makes certification particularly attractive for e-commerce. Such certification can be voluntary, for example with a company deciding whether or not to apply for VeriSign or TRUSTe approval of their web site. In this case, the amount of information disclosed to the third party is clearly specified within defined limits and holders of the certification can control the publication of information, so privacy is not a major concern. When certification is involuntary, however, companies may feel that their feel that the confidentiality of commercially-sensitive information has been compromised, for example when a certifier "tests" qualities on different providers with or without their consent (e.g. using techniques such as the Gomez benchmark and scorecards). Concerns about privacy are likely to be particularly strong when an involuntary sampling process produces unfavourable results.

Loss insurance

Loss insurance limits the potential damage caused to a consumer in e-commerce transactions, thereby reducing the level of exposure, one of the three key trust factors discussed earlier. This reduction of exposure does not increase trust *per se*, but reducing the level of trust required to engage in a transaction has the overall effect of enhancing guaranteed trust transactions. The direct impact of loss insurance on Internet usage is illustrated by the way the U.S. Electronic Funds Transfer Act, which limited consumer

[15] eTrust Internet Privacy Study, BCG. Quoted in 'Implementing the OECD Privacy Guidelines in the electronic environment", OECD, September 1998.

losses in electronic transactions to $50 per credit card, increased electronic purchases and expanded the credit card industry. When it was enacted, however, banking associations generally assumed that such regulation would dampen the credit card market. This illustrates the difficulties of forecasting outcomes from policies relating to trust.

Legal frameworks

Regulation and legislation reduce temptation by making illegal activities expensive, and different regulatory and legal frameworks can address different trust concerns. For example, the OECD Guidelines on Privacy[16] and data protection legislation in many countries, often based on these Guidelines, have been stimulated directly by concerns over consumer protection with computer-based systems. Crimes related to electronic systems (see Appendix II) have also led to computer-related law, such as criminal information legislation, like that enacted in 1978 in the U.S., in 1981 in the U.K. and 1986 in Germany and Sweden. The Electronic Funds Transfer Act of America addresses the exposure aspect of trust (by reducing or limiting it), while laws against computer-related economic crime reduce temptation (by making trust violations expensive, or less attractive). A legal framework can also reduce uncertainty by establishing an effective ADR strategy for resolving online disputes, thereby providing a framework to form expectations in cases of non-compliance.

5. Privacy, Security and Identity Dimensions of Trust-Enhancing Products

Strategies, products and services to enhance trust can be evaluated along five dimensions, each having different implications on trust and privacy: participation, depth, publication, payer and price.

Understanding each is important in developing guidelines and policies for evaluating, monitoring, comparing and developing different approaches and products to deal with specific trust-enhancement goals.

The *participant* denotes *whom* is covered by a particular approach to trust enhancement. For instance, legal frameworks must be universal, while different types of certificates and authentication can be either universal or restricted. While loss insurance should be universal in principle, in practice it is necessary to limit it, in order to allow for adequate reserves to be maintained. When there are several market providers of a trust-enhancing product, such as third-party certification, those being monitored could go “shopping” for the best one they can obtain, thereby diminishing the informative value of that certificate.

[16] The OECD Guidelines specify eight principles: 1) there should be *limits to the collection* of personal data; 2) *data quality* should be accurate, complete and kept up-to-date and relevant to the purposes for which they are to be used; 3) the *purposes for which personal data are collected should be specified*, not later than at the time of data collection; 4) *use of data should be generally limited* to the specified purpose; 5) personal data should be protected by reasonable security safeguards; 6) there should be a general *openness* about related developments, practices and policies; 7) *individuals should have rights to participate* in obtaining and challenging personal data; 8) and *a data controller should be accountable for compliance*.

Cantor and Packer (1995), for example, discuss how bond issuers often seek (and many times gain) an investment-grade rating from another credit-rating agency if one of the two major agencies rates their bonds as non-investment grade. One way to avoid this problem would be to monitor third-party certification agents. However, the implied non-voluntary involvement in this monitoring could result in an infringement of privacy that raises important policy issues

Depth refers to *where* the boundaries are set for a PET or other trust-enhancing mechanism. These boundaries should encompass those characteristics that matter to the user, and provide accurate and useful information. For instance, variations in the scope of a PET are indicated by the amount of information disclosed by each product. Establishing the identity of an agent may be restricted just to whether that person is who he claims to be, or could be extended to include personal demographics (for example age, sex, race) and preferences (e.g. consuming habits, purchase history). The greater the information required by a PET, the higher is the risk of invading the privacy of individuals, although its value in trust enhancement could also be higher. It is important therefore to know the scope of the PET to determine whether it is a trust-enhancing or an information-exploitation instrument. Furthermore, the greater the amount of information required, the higher must be the security controls to avoid breaches of privacy caused by unauthorized access to the information. Depth is well defined for personal authentication, as it generally tries to answer the question “Is this who he says he is?”, which can be answered through the use of a password, personal identification number (PIN), personalised questions and other techniques. Depth is less clear in other areas, such as security and privacy quality seals for web sites, so it is important that the boundaries applied are clearly defined. Trust-enhancing legislation is likely to be most effective when its depth has a well-delineated focus which avoids being so broad that it allows many loopholes, or so narrow that it may be restricted to very particular cases.

Publication addresses *when* aspects covered by a PET, legislation or other trust-enhancing approach need to be made available or released. For instance, information can be made available on demand (e.g. from a third party) or can be shared publicly with all potential participants at the same time. An individual may be willing to share with one online company what she considers to be sensitive personal information, but may be reluctant to make that information available to other online traders. The right to privacy may be violated if the information is made public without the consent of those involved. The significance of the effects of this dimension can be seen when trying to understand the differences in the regulation of privacy in the U.S. and in Europe. The U.S. legal system protects consumer privacy but considers data to be corporate property: once a person voluntarily discloses information, that information is no longer considered private. In the U.S., unauthorised use of information is seen as more of an ethical and public relations problem than a legal one. European regulations, on the other hand, prevent the secondary use of data, which must be collected for a specific purpose and cannot be used for a different one (with the exception of historical, statistical or scientific purposes). European regulation requires that information collected be accurate, that only data necessary for the stated purpose can be collected, anonymous when possible, and the information has to be deleted when no longer useful for the original purpose; there is much current debate in the U.S. on the data-retention issue. Both legislation and loss insurance clearly have to be made public before they can be applied. Authentication and certification, however, can be made public on application or on demand. The benefits and shortcomings of both approaches have to be taken into account to optimise their use.

The *payer* refers to *who* should be charged for the trust-enhancing product or service. When a product is a public good, in that its use by one agent does not prevent other agents from using it, the socially optimal approach may be to have the whole society pay for it. As Beales, Craswell and Salop (1981) point out, information markets present imperfections due to their natural monopoly features (there is a low marginal cost for distributing information once it has been produced) and their potential "free rider" problems (when buyers can resell or give away acquired information to others). Coestier (1998) proposes public financing of certification, given its public-good characteristics, as otherwise there could be too little supply of the certificates that are required.

Price focuses on *how much* is charged to obtain a trust-enhancing product or service, such as certification. This depends on the characteristics of the payee. For instance, if the owner of a web site pays for some form of "quality" mark or other certification, the exposure factor of trust may be increased; this can produce undesirable effects as there is a risk of moral hazard, in which the supplier of the mark who verifies the system might charge a higher price for a better outcome, thereby increasing uncertainty among consumers when they see the mark.

6. Lines for further research

The previous sections provide an overview of the main characteristics of online trust in e-commerce, especially its important identity, privacy and security aspects. This section highlights major areas for further social research, identifying the most important questions to be addressed (Appendix III lists some key researchers in disciplines relating to trust and privacy).

a) Understanding the economic impact of trust

There is wide acceptance that trust is an important factor in nurturing or constraining the growth of e-commerce. But what are the specific economic implications of trust, and how can the economic impacts of different trust-enhancing strategies, such as PETs and ADR frameworks, be evaluated?

- Estimating the economic value of trust: What is the cost-reduction potential of PETs and other trust-enhancement initiatives, in terms of factors such as the decrease of intermediation costs and search costs? What are the empirical and theoretical trade effects of trust-enhancing initiatives, including measures of the economic impact of existing trust-enhancing mechanisms? What are the key externalities affecting trust? For example, to what extent can efforts to create the trust necessary for a consumer to make the first online purchase from a supplier reduce the cost of subsequent transactions? And what are the implications of the "contagion" effect of trust, in which a consumer's level of trust might increase if she perceives that other consumers also trust that online retailer?
- Economics of trust-related products, services and other initiatives: What are the impacts on e-commerce and the broader e-marketplace of the creation of a new industry based on developing, selling and implementing trust-enhancing products and services? What are the implications for start-up and online-only companies of the potential for established 'click and mortar' operations to gain greater trust because of their previous reputation? To what extent is the desire to establish e-commerce trust through alliances with acknowledged blue-chip firms and brand

leaders likely to result in a concentration of e-commerce power among a few large players? Are there steps that should be taken to stimulate a more diverse e-commerce market?

- Online payment systems: How have online payment systems evolved? What new forms of payment are emerging, such as the Amazon Honour and shareware systems? What are the main trust problems that need to be addressed with these new approaches? What criteria should be used to evaluate alternative approaches? What trust-enhancing opportunities are being opened by the new types of payment system, for example in terms of the ability to allocate economic resources directly to producers without intermediation and (potentially) with each consumer contributing an amount equivalent to the economic benefit received?
- Microeconomic analysis: At the micro level, what are the costs and benefits for consumers and online businesses resulting from trust-enhancing policies or products? What are the specific possible costs, and how are these costs, shared among consumers, business and government? What would be the efficient division of these costs and how can possible inefficiencies be addressed?
- Macroeconomic analysis: Internationally, what are the benefits and burdens to nations and regions tied to their decision about the adoption of trust-enhancing policies or products, either in a coordinated or in an uncoordinated way? What are the regional or national variables affecting Internet adoption? How has technology affected different economies? What is the empirical evidence of the effects of the introduction of trust-enhancing initiatives in different countries, for example in terms of comparative tables of adoption rates and economic impact?

b) Reviewing potential trust-enhancing solutions, including the role of the Internet and other ICTs

As indicated in this paper, a proliferating range of trust-enhancing products, services and strategies are emerging for consideration by consumers, businesses and policy-makers. How can these be analysed and evaluated to determine the most appropriate solutions for different e-commerce contexts, and what role do ICTs play in supporting or undermining the establishment of trust?

- Assessing the advantages and disadvantages of trust-enhancing approaches: What are the characteristics of the main approaches to enhancing trust? What factors most influence trust-enhancement outcomes (e.g. why is centralized government information and validation accepted in the U.S. but not in the U.K.)? What impacts have cultural differences had on adoption and usage rates of trust-enhancement products and services already introduced? How do these cultural and social issues affect the acceptance, use and understanding of each approach? To what extent are solutions that work in one country or context applicable to other situations? How can the experience of trust enhancement from different e-commerce contexts contribute to guidelines of real value in a wide range of online environments? What are the likely effects of newly emerging solutions?
- Theoretical and empirical studies on the interrelation among electronic trust-enhancing instruments: What are the complementarities of different approaches in terms of their political implications (e.g. the ability to gain political consent for one PET when the performance of that product depends on the acceptance of other strategies) and economic dimensions (e.g. the degree to which the economic

success of a PET is dependent on the implementation of other trust-enhancing products or strategies)?

- Meta-analysis of different privacy protection strategies and regulation: What main kinds of privacy protection initiatives have been adopted? Which have been most effective and in what contexts? What have their effects been on trust and Internet usage? How well do e-commerce consumers know the privacy policies of their online suppliers? How have the OECD Privacy guidelines been interpreted in different countries, and with what effects? What are the statistics of use of privacy protection products, such as software catering for anonymous surfers (Anonimyzer, Fogbank, Guardster, etc.), privacy filters (Personal Sentinel, Surfer Protection Program, etc.) and cookie busters (Burnt cookies, cookie crusher, Magic Cookie Monster, etc)?
- The effect of ICTs on trust: In what areas can ICTs help or hinder the establishment of trust in electronic markets? What is the empirical evidence of the degree to which people "trust" face-to-face contexts more than other environments (e-commerce, telephone, chat rooms, audio-visual communication, etc.)? How can ICTs be deployed to enhance rather than diminish trust, for instance in providing information to aid evaluations of alternative options?
- The role of the Internet: How do the Internet and related electronic media shape perceptions of trust in e-commerce? What effect has the Internet actually had on trust? Does the use of the Internet generally increase trust, or do trusting people self-select to use the Internet? What evidence is there from general Internet use of how individual and group perceptions and behaviour affect trust issues? How relevant are these findings to e-commerce?

c) Analysing the trust-identity-privacy-security relationship

Analysing the relationship between trust and its three principle aspects highlighted in this paper (identity, privacy and security) is of crucial importance in dealing with trust issues. What are the key parameters in each dimension and what conceptual and experimental frameworks can help to assess how to balance competing and complementary aspects?

- Testing the effects on trust of different trust-enhancing approaches: What are the trade-offs between the dimensions in different contexts and how can they be affected by different trust-enhancing policies and products?
- Understanding the influence of different dimensions of trust: How can the main aspects of trust be affected by different external or internal products and services (e.g. see Bacharach, Guerra and Zizzo, 2001 for the effects of kindness, need and trust-responsiveness)? What are the cross-impacts of different dimension on each other? How can these impacts avoid the dampening effects resulting from interactions between the use of different mechanisms at the same time?
- Analysis of relationships between dimensions: How can the economic need to encourage the growth of free-flowing e-commerce growth be balanced with rights for privacy protection and security of information? What are the complementarities and tensions? Is there a theoretical approach that can assist to determine the equilibrium point in resolving any conflicts?
- Multi-disciplinary analyses of the advantages and disadvantages of a mix of approaches to trust, privacy and other dimensions: What are the relevant issues

that need to be assessed in comparative studies, for example the consequences of, and maintenance required by, each approach and mix?

d) Understanding the social impacts of trust

Social and cultural contexts can play an important role in determining perception of trust in e-commerce. What are the key relevant social issues?

- Influence of culture on trust perceptions: How do different social contexts (for example generational, educational and geographical) affect issues of trust and the design and use of trust-enhancing products, services and frameworks? What policies have attempted to address these? How effective have they been? What lessons are there for policy focusing on trust in e-commerce?
- Social inequalities in the “digital divide”: How do skills in accessing, managing and interpreting information on the web, and engaging in social interactions through the Internet, affect trust outcomes in relation to e-commerce? What is the evidence on the impacts made on this by policy initiatives?

Conclusion

The main objective of this paper was to provide a common ground and a starting point for further research. It has done this by highlighting the complexities of trust as a concept and by outlining the broad scope of trust in the information economy. Potentially effective trust-enhancing strategies, products and service have been explored. Some frameworks for studying trust in e-commerce and other online transactions have also been described, including key priorities for an agenda of multidisciplinary social research to improve understanding of trust in an e-economy.

Appendix I A Basic Trust Game

Figure 1uses purely illustrative magnitudes to present an example of a basic e-commerce trust game based on Bacharach and Gambetta (2001) and Bacharach, Guerra and Zizzo (2001).

Figure 1: An e-commerce trust game

Online Store (Trustee)

		Honour	Violate	
Consumer	Trust	3, 1	-3, z	*Exposure*: y > - 3
(Trustor)	Not	x, 0	y, 0	*Temptation*: z > 1
				Improvement: x < 3

When thinking about making a purchase, e.g. of a product via a web site, the consumer (trustor) in Figure 1 has to decide whether or not to trust the online store (trustee) supplying the product. The numbers on the left in each box display the payoff she would receive, given her and the trustee's actions. Numbers on the right indicate the store's payoffs – what the store would receive given its and the consumer's choices. The payoff to the store if the consumer chooses not to trust is zero. The consumer would *improve* her situation, if the trustee were to honour her trust; however, by trusting the online store she is *exposing* herself to a risk she would otherwise not be subject to, since y > -3 (*exposure* condition): the greater the difference (y – 3), the greater is the exposure for the consumer. The exposure condition implies that it would not be rational for the consumer not to choose "Trust" if she is expecting the store to choose "Violate". The store is *tempted* to choose "Violate", as it can receive more from doing so than from honouring trust (*temptation* condition: z > 1): the greater z is, the greater is the temptation. In general, trust-enhancing measures will succeed insofar as they reduce the temptation for the trustees (the store in our example) and the exposure for the trustors (the consumer in our example).

Appendix II Types of Computer Fraud

Below is a list describing typical forms of computer fraud. It has been compiled from three documents: “FCC 2001 Internet Fraud Report” (FBI 2002), “Network and Information Security: Proposal for a European Policy Approach”, (European Parliament, June 2001), and “COMCRIME Study, Legal Aspects of Computer Related Crime in the Information Society” (European Commission, 1998).

Financial Institution Fraud: Use of deception to perform a fraudulent activity affecting an institution that manages money, credit or capital. Example: Credit Card Fraud.

Identity Theft: Use of other’s personal information to pose as them.

Gaming Fraud: Collecting something of value in exchange for the chance to win a prize, when there is misrepresentation of the odds or events.

Utility Fraud: Misrepresentation by an individual to harm or defraud a government-regulated entity.

Investment Fraud: Deceptive practices involving the use of capital to create more money. Example: market manipulation.

Confidence Fraud: Failure to comply on commonly known expectations resulting in financial loss. Example: Non-delivery of merchandise.

Unauthorized Access: Breach into a computer system without malicious intent, but for the pleasure of overcoming technical security measures.

Network Disruption: Attack on a computer network rendering it inoperative for a period of time. Examples: Server attacks.

Data destruction: Use of malicious software to modify or erase data. Example: virus.

Malicious Misrepresentation: Raiding the identity of a service or system provider to pose as the authorized owner of that identity.

Infringements of Privacy: Use of personal data provided *bona fide* for uses different to those intended when the information was first provided.

Computer Espionage: Unauthorized extraction of confidential or sensitive data from a computer system.

Piracy: Unauthorized copying and use of software.

Illegal and Harmful Contents: Dissemination of child pornography, hate speech and libel.

Appendix III Researchers in trust-privacy related areas

The following is a non-exhaustive list of people conducting research in areas related to this paper.

a) Legal

Jack L. Goldsmith, University of Chicago Law School, jl-goldsmith@uchicago.edu

Lawrence Lessig, Stanford Center for Internet and Society. lessig@pobox.com

Robert E. Litan, Co-director, Brookings Center for Regulatory Studies, Washington, DC. rlitan@brook.edu

Larry E. Ribstein, Corman Professor of Law, University of Illinois. ribstein@law.uiuc.edu

Ulrich Sieber, Head of the Department of Criminal Law, University of Munich (LMU). Sekretariat.Sieber@jura.uni-muenchen.de

b) Trust

Avner Ben-Ner, Professor, Director of Industrial Relations Centre, University of Minnesota. benne001@umn.edu

L. Jean Camp, Professor of Public Policy, John F. Kennedy School of Government, Harvard University. Jean_Camp@harvard.edu

Karen Cook, Professor of Sociology, Stanford University. kcook@leland.stanford.edu

Diego Gambetta, University of Oxford. diego.gambetta@socstud.ox.ac.uk

Gerardo Guerra, BREB Unit, University of Oxford. gerardo.guerra@socstud.ox.ac.uk

Louis Putterman, Economics Department, Brown University. Louis_Putterman@brown.edu

Richard Rose, Senior Research Fellow, Oxford Internet Institute, University of Oxford.

Toshio Yamagishi, Department of Behavioral Science, Graduate School of Letters, Hokkaido University. Toshio@let.hokudai.ac.jp

Daniel Zizzo, BREB Unit, University of Oxford. daniel.zizzo@economics.ox.ac.uk

c) Privacy

Colin Bennett, University of Victoria. cjb@uvic.ca

Christoph Engel, Max-Planck Project Group, Bonn, Germany. engel@mpp-rdg.mpg.de

Karim Jamal, Professor of Accounting, University of Alberta at Edmonton. Karim.Jamal@ualberta.ca

Ben Macklin, Australian National University. bmacklin@emarketer.com

Helen Nissenbaum, Princeton University. helen@princeton.edu

Charles Raab, Department of Politics, Edinburgh University. c.d.raab@ed.ac.uk

Frederick Schauer, Academic Dean, John F. Kennedy School of Government, Harvard University. fred_schauer@ksg.harvard.edu

d) E-commerce

Arthur J. Cockfield, Queen's University -Faculty of Law, Ontario Canada. ac24@qsilver.queensu.ca

Ian MacInnes, School of Information, University of Syracuse. imacinne@syr.edu

Juergen Noll, University of Vienna, Department of Industry, Energy and Environment. juergen.noll@univie.ac.at

Daniel Piazolo, FERI (Financial & Economic Research International), Germany. daniel.piazolo@feri.de

Brian T. Ratchford, Pepsico Chair in Consumer Research, University of Maryland School of Business. bratchfor@rhsmith.umd.edu

Jeanne W. Ross, MIT Sloan Center for Information Systems Research. jross@mit.edu

References

Akerlof, G. A. (1970), "The Market for 'Lemons': Qualitative Uncertainty and the Market Mechanism", *Quarterly Journal of Economics* 84, pp. 488-500

Arrow, K. J. (1971), *Essays in the Theory of Risk Bearing*, North-Holland, Netherlands

Bacharach, M. O. L. and Gambetta, D. (2001), "Trust in Signs", in Cook, K. (ed.), *Trust and Social Structure*, Russell Sage Foundation, NY, pp. 148-184

Bacharach, M. O. L., Guerra, G. A., and Zizzo, D. J. (2001), "Is Trust Self-Fulfilling? An Experimental Study", *University of Oxford, Department of Economics Discussion Paper* 76

Baron, J. (1998), "Trust: Beliefs and Morality", in Ben-Ner, A. and Putterman, L. (eds.), *Economics, Values and Organization*, Cambridge University Press, Cambridge, pp. 408-418

Beales, H., Craswell, R., Salop, S. (1981), "Information Remedies for Consumer Protection", *American Economic Review* 71, pp. 410-413

Ben-Ner, A. and Putterman, L. (2002), "Trust in the New Economy", *HRRI Working Paper 11-02*, University of Minnesota, Industrial Relations Centre

Bochet, O., Page, T. and Putterman, L. (2002), "Cheap Talk and Punishment in Voluntary Contribution Experiments", unpublished paper, Department of Economics, Brown University, Providence, RI

Camp, J. (2000), *Trust and Risk in Internet Commerce*, MIT Press, Cambridge MA

Cantor, R. and Packer, F. (1995), "The Credit Rating Industry", *Journal of Fixed Income* 5, pp. 10-34

Coestier, B. (1998), "Asyméetrie de l'information, Reputation et Certification", *Annales d'économie et de Statistique* 51, pp. 49-78

Dutton, W. H. (1999), *Society on the Line: Information Politics in the Digital Age,* Oxford University Press, Oxford and New York

Gambettta, D. (1990), "Can We Trust Trust?", in *Trust: Making and Breaking Cooperative Relations*, Gambetta, D (ed.). Basil Blackwell, Oxford, pp. 213-237

Guerra, G. A. (2001), "Certification Disclosure and Informational Efficiency: A Case for Ordered Ranking of Levels", *University of Oxford, Department of Economics Discussion Paper* 64

Guerra, G. A. and Zizzo, D. J. (2003), "Trust Responsiveness and Beliefs", *Journal of Economic Behavior & Organization*, forthcoming

Kollock, P. (1994), "The Emergence of Exchange Structures: An Experimental Study of Uncertainty, Commitment and Trust", *American Journal of Sociology* 100, pp. 313-345

Kini, A. and Choobineh, J. (1998), "Trust in Electronic Commerce: Definition and Theoretical Considerations", in Blanning, W. and King, D. (eds.), *Proceedings of the 31 Annual Hawaii Conference on System Sciences*, volume IV, IEEE Computer Society

Latcovich, S. and Smith, H. (2001), "Pricing, Sunk Costs, and Market Structure Online: Evidence from Book Retailing", *Oxford Review of Economic Policy* 17, 217-234

Lorenz, E. (1999), "Trust, Contract and Economic Cooperation", *Cambridge Journal of Economics* 23, 301-315.

McCullagh, A (1998), "E-commerce: A Matter of Trust", in *Proceedings of the 1998 Information Industry Outlook Conference*

MacKenzie, D. (1999), *"The Certainty Trough",* in Dutton, W. H., *Society on the Line: Information Politics in the Digital Age*, Oxford University Press, Oxford and New York, pp. 43-46*.*

Misztal, B. (1996), *Trust in Modern Societies*, Polity Press, Cambridge MA

Morgan, J., Orzen H. and Sefton, M. (2001), "An Experimental Study of Price Dispersion*"*, paper presented at the Oxford Experimental Economics Workshop, November 1

Pettit, P. (1995), "The Cunning of Trust", *Philosophy and Public Affairs* 24, pp. 202-225

Sako, M. and Helper (1998), S., "Determinants of Trust in Supplier Relations: Evidence from the Automotive Industry in Japan and the United States", *Journal of Economic Behavior & Organization*, 34, pp. 387-417

Sobel, J. (1985), "A Theory of Credibility", *Review of Economic Studies*, LII, pp. 557-573

Wallace, P. (2001), *The Psychology of the Internet*, Cambridge University Press, Cambridge

Zizzo, D. J. (2003), "Empirical Evidence on Interdependent Preferences: Nature or Nurture?", *Cambridge Journal of Economics*, forthcoming