OECD PROCEEDINGS

GATEWAYS
TO THE GLOBAL MARKET
Consumers
and Electronic Commerce

PUBLISHER’S NOTE
The following texts are published in their original form to permit faster distribution at a lower cost.
The views expressed are those of the authors, and do not necessarily reflect those of the Organisation or of its Member countries.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996) and the Republic of Korea (12th December 1996). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).
FOREWORD

Despite the rapid evolution of information technologies and widespread access to the electronic network that is the Internet, its use in commercial transactions is still in the early stages of development. The emerging electronic marketplace now comprises only a small portion of the world economy but analysts predict its potential for growth is exponential over the next few years. Businesses and governments alike are taking notice of this potential with an eye to expanding international markets and facilitating global trade.

Low barriers to entry and the potential to reach a vast international market make the Internet an attractive tool for reputable businesses and service providers. However, these same attributes are also enticing to perpetrators of fraud and abuse. Pyramid scams and “get-rich-quick” schemes that are spread by word of mouth or mass-mailings can reach hundreds or perhaps thousands of people in the terrestrial world. On the Internet, these same scams have the potential to reach millions worldwide with the simple click of a mouse.

Consumer questions and concerns in the electronic marketplace are not limited to issues of fraud and illegal conduct. Existing consumer protection mechanisms must be assessed and perhaps revised to address traditional marketplace issues that also arise in cyberspace. Questions regarding privacy, contract enforcement, product liability, consumer redress, and refund and chargeback issues must be taken under serious consideration in this new global marketplace. Some of these issues might best be resolved through industry-self regulation, competition, technological solutions, and consumer education as businesses work to provide a safe, secure and attractive environment for potential customers. Others may require a coordinated international government response.

The borderless nature of the electronic marketplace and its potential for anonymous interactions can compound enforcement problems on the Internet. Laws and regulations that protect consumers in their home countries
may not be applicable in other nations and other jurisdictional issues may also arise. It may be necessary to develop novel, international approaches to consumer redress and dispute resolution. Consumers must be confident that this electronic environment will afford them the same protections against fraud, injury and loss that they benefit from in their other daily interactions. To earn this consumer confidence, the electronic marketplace must include a global framework of clear, reliable, and harmonised courses of consumer protection and redress.

Participants were asked to consider the following issues in preparation for the Forum:

- Electronic Commerce Benefits and Prospects for Consumers
- Consumer Confidence in the Borderless Global Market
- Establishing Identity
- Preserving Privacy
- Avoiding Fraud and Misrepresentation
- Finding and Examining Goods and Services for Suitability and Quality
- Creating Binding Agreements to Purchase
- Making Payment
- Recovering Damages Caused by Failure to Perform and Defective Products

These proceedings are published on the responsibility of the Secretary-General of the OECD.
# TABLE OF CONTENTS

**Executive Summary** ........................................................................................................... 7

**Opening Session**

Jytte Olegaard, Chairperson, OECD Committee on Consumer Policy .............. 11

**Opening Remarks**

Donald Johnston, Secretary-General, OECD ................................................................. 13

**Keynote Addresses**

John Bridgeman .............................................................................................................. 17
Jay M. Tannenbaum ........................................................................................................... 20
The Honorable Robyn McDonald .................................................................................. 24

**Background Note**, Professor Carey E. Heckman .......................................................... 27

**Panel Summaries** .................................................................................................................. 65

---

**Session I. Consumer Options in the Global Marketplace** .............................................. 67

*Panel 1* - The Internet Operating Environment ............................................................. 68
*Panel 2* - Virtual Money: Consumer Payment Options .............................................. 75

**Session II. Consumer Privacy and Data Protection** ....................................................... 83

*Panel 1* - Cryptography .................................................................................................... 85
*Panel 2* - Protecting Transactional Data .......................................................................... 90

**Session III. Jurisdiction in Cyberspace: Who Protects Consumers?** ..................... 99

*Panel 1* - The Role of Business and Government in International Consumer Protection ................................................................. 102
*Panel 2* - Protecting Consumers From Cross-Border Fraud and Misleading Conduct .............................................................................................................................................. 114
*Panel 3* - Unsafe Or Defective Merchandise: Product Liability Protection in The Global Marketplace ........................................................................................................... 122

**Session IV. Summation**

Christine A. Varney, Reporter ............................................................................................. 131
EXECUTIVE SUMMARY

The evolution of the Internet from its roots in academia to its current immersion into the commercial marketplace has been swift. There is great potential for this new commercial tool to change the economic landscape, allowing goods and services to be delivered to a market that largely ignores political and geographic barriers -- improving productivity and communication and providing global market access to businesses and consumers worldwide. Low barriers to entry and the potential to serve an expansive global market base could offer business and industry unparalleled opportunities.

However, along with the promise of this new technology and its potential benefits and opportunities come uncertainties and risks. This new medium presents consumers with new questions regarding individual privacy, information security, contract enforcement, product liability, and redress in cases of fraud and misconduct. In turn, governments are faced with the question of how best to protect their citizens without inhibiting the growth of this evolving electronic marketplace. They must determine whether current rules and practices are sufficient and applicable on the Internet and, if not, how to best proceed in developing and implementing an effective and practicable market framework.

Addressing the challenges of the global electronic marketplace requires an understanding of the advantages and limitations of the technology and determining the appropriate balance between government intervention and industry self-regulation in achieving market goals. In March 1997, the OECD Committee on Consumer Policy held a conference entitled Gateways to the Global Market: Consumers and Electronic Commerce, which explored the issues and concerns of consumers’ online. At this two-day conference, a diverse international group representing government, consumer agencies, industry, the financial services industry, academia, direct marketers, and advertisers gathered to discuss the enormous potential of the Internet and electronic commerce. Recognising their shared interests in the security and the
integrity of the global electronic marketplace, this international coalition worked together to explore ways to promote the evolution of electronic commerce with consumers' interests in mind. Forums such as these will lay the groundwork for developing a harmonised and predictable legal and commercial framework for the online environment.

The conference opened with remarks by the OECD Secretary-General, Donald Johnson. The Secretary-General noted that as an international and multi-disciplinary organisation, the OECD is well suited to examine a wide variety of issues related to the global electronic marketplace. He stated that the OECD’s goal is to work to dismantle the barriers to global electronic commerce in an effort to aid the expansion of world trade. The Secretary-General also noted the OECD’s commitment to establish mechanisms to ensure consumer protection on the Internet and promote consumer confidence in the online environment. Protections that foster consumer confidence in the safety of electronic commerce are essential for growth and prosperity in the electronic marketplace. Finally, Mr. Johnston mapped out the OECD’s continuing agenda for electronic commerce issues including the November 1997 Forum in Turku, Finland entitled “Dismantling the Barriers to Global Electronic Commerce,” and culminating with a conference planned for October 1998 in Ottawa, Canada entitled “A Borderless World.”

Participants were then given an overview of the electronic marketplace as it exists today. Companies currently doing business online expressed their overwhelming support for the global marketplace and stressed their belief in its potential for exponential growth. They also stressed that as responsible companies doing business on the Internet, they too were interested in providing their customers with a convenient and secure environment. They urged government policymakers not to move too swiftly to regulate at this early stage.

There was then extensive discussion of consumer payment options and the security of payment information and transactional data. This included an introduction to several competing technologies including the Secure Electronic Transactions (“SET”) software solution, traditional credit cards, and the value loaded electronic purse. Each of these competing technologies hinge upon the same consumer issues: convenience, interoperability and most importantly security. The ensuing discussion of transactional security stressed the need for verification and authentication and the various means for achieving it including the use of passwords, third party verifications, and digital signatures. Since no specific payment option has been accepted as the standard
for electronic commerce, all of the presenters agreed that any regulation in this rapidly evolving, technologically driven field would be premature. However, encryption technology was noted to be key to transactional security and safety in electronic commerce. The international challenge is to find the necessary balance between the need to provide secure data protection and individual government concerns regarding national security and law enforcement.

The issue of consumer privacy and the collection and use of personally identifiable information was also of great concern. Questions were raised about the security of personally identifiable information and transactional data on the Internet: what and how much information is being collected, who has access to that information, and what control does the consumer have over its collection and use? Much of the discussion focused on technological solutions -- secure payment systems, privacy software solutions, encryption, trust marks, and digital signatures. Consumer advocates were concerned about the limitations of such technology and the level of individual privacy that should be guaranteed in the electronic environment. Again, there was a divergence of opinion between those who advocate strict, government-enforced privacy laws and those who favour industry self-regulation. Special attention was paid to the privacy rights of children and other “vulnerable populations.” It was suggested that unified international government intervention regarding data collection from children was a more likely possibility than the implementation of strict and general privacy regulations.

Throughout the conference, speakers that noted the growing concerns about consumer fraud and deception online could dampen enthusiasm for the Internet as a commercial medium. The question of how to best protect consumers as they interact online was met with a varied response. Concerns were also expressed regarding the enforceability of electronic contracts and avenues of consumer redress in cases of fraud or in the event that goods did not meet the consumer’s expectation. Some speakers called for immediate and comprehensive government regulation. Others argued that additional government regulation in this early stage of development could be counter productive and that the rapid pace of technological advancements could make such rules immediately ineffective or obsolete. These participants argued that market-based solutions and industry self-regulation would better serve solve the contractual problems in the evolving marketplace.

There were several areas of consensus over the course of the conference. First, that the global dialogue between governments, industry, academia and consumer groups is a positive and imperative step. Speakers also
noted the importance of the creation of a global legal regulatory plan -- a simple and predictable set of legal tools and goals that can work with the rapid evolution of technology on the Internet. Finally, everyone agreed that consumer education is a critical element in any marketplace, and that the Internet itself may provide the most effective distribution tool available.

Overall, the conference was an informative and provocative international forum. It examined both government and private sector options and efforts to protect and empower consumers to enable them to make informed and secure choices that provide them with the benefits of interaction in the global marketplace.
OPENING SESSION

Jytte Olegaard
Chairperson, OECD Committee on Consumer Policy

On behalf of the Committee on Consumer Policy, I welcome you to this important conference Gateways to the Global Market: Consumers and Electronic Commerce.

The OECD Committee on Consumer Policy has organised this conference with the help of another committee within the OECD, the Committee for Information, Computers and Communication Policy. I wish to thank this committee and their secretariat for their invaluable assistance. The Consumer Policy Committee is composed of the senior consumer policy and law enforcement officials of OECD member countries. The Committee has been interested in the idea of a global marketplace for consumers for a number of years. In the early '90s we envisioned that catalogue shopping and other forms of direct marketing might become international in scope, benefiting consumers greatly. It was clear then that many consumers already had internationally accepted payment cards, that a number of firms already provided international parcel delivery services and that international telephone charges should drop substantially in coming years. Thus, we envisioned a time when consumers sitting in the comfort of their homes would use the telephone to shop the world over for goods and services. Following the first conference we held in 1994, we began studying several issues of great practical importance to the development of this global marketplace. The possibility that payment card intermediaries could provide a form of redress in international transactions, the possibility that direct marketers could establish meaningful codes of conduct to govern their behaviour and the possibilities for bringing down the high cost of international parcel delivery. Now, just a few years later here in 1997, we have the Internet and the possibilities for a global marketplace have expanded exponentially. At the same time, issues of concern to the Committee on Consumer Policy have expanded as well.
What will we and the Committee on Consumer Policy do following from this conference? That will depend on whether we identify issues to which we can contribute and which fall within our law enforcement or our consumer advocacy functions. In some areas, such as enforcement of consumer protection laws, the members of our committee have direct responsibilities in their governments. Thus, ideas for improved cooperation and the control of misleading, false or fraudulent marketing practices fall directly within our competence. In other areas we can serve as advocates for change within the OECD and within our respective governments. For example, in our work on the high cost of international parcel delivery, we are trying to put the issue of streamlined custom clearance procedures on national and international agendas. In still other areas, we can serve as advocates for change before the private sector. Thus, in our work on redress through payment card intermediaries, we are trying to stimulate the private sector to take up voluntarily responsibilities which will increase consumer confidence in international transactions and help that marketplace to grow.

Our deliberations over these two days will increase our knowledge of and our understanding about the world of electronic commerce and will focus our future work. Thus it is vital that we learn from this gathering ways in which the committee can contribute in both the advocacy and law enforcement domains. Equally important will be to learn which issues are well covered in other fora in order to avoid duplication of effort.
OPENING REMARKS

Donald Johnston
Secretary-General, OECD

Electronic commerce already plays an important role in our everyday personal lives, from the use of an automatic teller machine to conduct banking transactions to the use of the Minitel to order theatre tickets. When first developed, these tools were considered “revolutionary.” However, these tools -- and many others developed using information and communications technologies -- have enabled businesses and consumers to conduct countless electronic commercial transactions.

Today we are experiencing a new revolution -- that of Internet-based electronic commercial transactions. This latest revolution is gaining momentum at a rate which is at once thrilling and alarming.

The Internet, which began in 1969, was developed as a system of open networks in which universities and government agencies could exchange information almost instantaneously. In 1990, the World Wide Web introduced another mechanism for parties to exchange information beyond just text. With the Web, video images, graphics, and sound could be blended in with the text. Today, these tools are playing an increasingly important role in everyday life, changing the way people communicate and do business and they are bound to have a widespread impact on society and economies.

This explosive growth of information and communications networks and technologies has created a borderless digital world where goods and services can be exchanged world-wide almost instantaneously. Using the Web as an advertising tool, businesses can market products and services to consumers worldwide. In 1990, only a few academics knew of the Web; today it is estimated that over 50 million people “surf” the Web. All of them have a plethora of physical goods and services -- from financial and educational services to entertainment -- available to them instantly -- literally at their finger
tips. The number of Web sites is estimated at over 400,000 today and the number of Internet hosts at over 16,000,000.

Electronic commerce is still in its infancy and estimates of current sales over the Internet and future prospects vary widely. For example, estimates of consumer transactions in 1995 vary from several hundred million US Dollars to several billion dollars. Projections for coming years span a similarly wide range, from several billion dollars by the turn of the century to hundreds of billions of dollars in a further five to ten years.

For each of us as consumers, electronic commerce provides an unprecedented opportunity for global exchange. From practically anywhere in the world, we are now able to shop from the many thousands of sites on the World Wide Web. As consumers the world over gain access to the Internet, there is thereby real potential to increase world trade.

The OECD, because it exists to advance the well-being of its citizens, is vitally interested in removing the barriers to such transactions. Expanding world trade through innumerable individual transactions will increase consumer welfare as surely as trade expansion through traditional commercial channels.

The OECD is well suited to help in the expansion of electronic commerce. Because we are an organisation of governments, we can help reduce governmentally-created barriers to trade. For example, we are examining the costly red tape of customs procedures applied to cross-border consumer purchases. Because we are multi-disciplinary, we can attack a problem from many angles simultaneously. Thus we can cover issues as diverse as cryptography, privacy and consumer fraud, as government officials responsible for each of these areas participate in OECD deliberations.

The OECD also exists to improve the functioning of governments. Thus, we look at electronic commerce from other perspectives as well. Our financial markets and tax experts for example, must assure that efficient electronic payment mechanisms being developed do not become tools for money laundering or tax evasion.

Most importantly, the OECD exists to envision and then to help realise a better future for us all. Thus, the OECD’s Committee on Consumer Policy, which has organised this conference, has long imagined a time when consumers would be able to shop the world over for goods and services. In 1994, they held their first conference on A Global Marketplace for
Consumers which anticipated many of the issues which concern us now; their vision is fast becoming reality.

Today’s conference is just one in a series of OECD forums and discussions of the benefits and barriers we face in the electronic marketplace. The OECD the will also sponsor a conference in Turku (Finland) in November 1997 entitled Dismantling the Barriers to Global Electronic Commerce, which will again draw together policy makers in government, private sector leaders and other key international organisations active in electronic commerce. The conference in Finland will set the stage for a major symposium on electronic commerce scheduled for October 1998 in Ottawa, Canada where we hope to achieve consensus on general principles for the operation and use of global information networks. Our goal with all of this work is to dismantle the barriers to global electronic commerce.

Consumer confidence is fundamental if the global marketplace is to prosper and develop to its fullest potential. But the world of the Internet is a fertile environment for fraud and misconduct. The world of cyberspace is potentially “lawless” because sellers can be based beyond the reach of national courts, increasing consumers’ exposure to unfair marketing practices, unsafe products, insecure payment methods, and loss of personal privacy. Should consumers fear that an order placed through the Internet will never arrive? Should they fear that their credit card will be misused once its number gets into cyberspace? Should they fear that the product will prove unsafe in their home, endangering themselves or their children? In order for electronic commerce to achieve its fullest potential, there is a need to establish mechanisms to ensure consumer protection within the world of cyberspace, for fear too can be a powerful barrier.

So it is our responsibility to ensure the creation of an environment which avoids making consumers victims. Thus, you will be tackling over these two days a variety of consumer protection issues ranging from the safeguarding of financial and transactional data to protection from misleading, false or even fraudulent marketing practices. The Consumer Policy Committee is already working to improve cooperation among national consumer law enforcement officials, to establish rights of redress through payment cards and to establish high standards for direct marketers. The Committee is working in other ways as well to help realise the potential of the Internet, for example by trying to bring down the high cost of international parcel delivery. Likewise, the Committee for Information, Computer and Communications Policy, which
has also supported this conference, is expected soon to release the OECD Guidelines on Cryptography Policy.

The borderless nature of the virtual world requires that these concerns be dealt with at the international level. As an international, inter-disciplinary and inter-governmental organisation, the OECD is the ideal forum to address these consumer issues effectively.

I welcome all of you, governmental officials, consumer representatives and members of the private sector to what is just the very beginning of this unified effort. It is imperative that we seize the moment and take advantage of the new and innovative ways in which the world community can participate in shaping this borderless cyber marketplace. The goal for the conference should be to establish principles and parameters for consumer protection in the world of cyberspace.
KEYNOTE ADDRESSES

John Bridgeman
Office of Fair Trading, United Kingdom

Secretary General, Chairman, ladies and gentlemen, it gives me great pleasure to deliver one of the keynote addresses to this conference. I have been asked to set out the areas of policy which governments, international organisations, business and consumer bodies will need to address in the area of electronic commerce. I shall also be saying a few words about how those problems may be approached.

As we approach the third millennium, we are witnessing developments in electronic commerce that will revolutionise the conduct of domestic business and international trade. Their first impact is already being felt in transactions between businesses, not least because businesses will have faster access to the new technology that is needed, but they will increasingly spread to consumers. These changes will offer new opportunities for consumers to choose, and even to seek out, the most competitive products in a global market.

At present, we are seeing just the beginning, with the development of key technologies in communications and information technology. Satellite and telecommunications developments have allowed low cost, high bandwidth communications across large parts of the world. Meanwhile, advances in computer hardware and software make it normal for ordinary citizens of the more developed countries to have in their homes computing power that 25 years ago the biggest businesses would have envied. The linkage between telecommunications and computing has made possible the explosive growth of the Internet, and we are now beginning to see the development of specific technologies, most notably in secure payment systems, that will transform it into an everyday tool for business. One of the most important characteristics of that tool is, of course, its global reach, with information flowing around the world as easily and quickly as across a single city. Indeed, many Internet users
often lose track of the countries from which they are accessing information, and generally have no idea at all of the route by which they get there.

Clearly, business and consumers will benefit immensely as these technological developments open the way for new competition amongst firms to provide goods and services for the consumer. When they are coupled to new developments in payment systems, about which we shall be hearing in this conference, they make possible radical changes in wholesale and retail marketing as we know it today.

In saying this, I do not necessarily embrace all the wildest visions that have been offered for the future. History shows clearly that technical possibility and commercial viability are not the same thing. I have only to mention quadraphonic sound or the personal hover car to make my point. We cannot assume that all consumers will want to forego the social contact of shopping, or the pleasures of handling the goods they are about to buy. Nor can we assume that delivery costs will ever fall to the point where it would be sensible for me to buy my groceries from New York. It is also easy to overestimate the pace of change. In particular, I suspect that much home shopping will only be attractive when high speed graphics are available to the consumer. This in turn will depend on high capacity links into the home. These points are worth making, because they mean that, for consumer transactions at least, we do not need to rush into legislation. We have some time to get it right. The present volume of consumer transactions over the Internet remains tiny as a proportion of the total and, incidentally, they will generally be conducted by the consumers most able to look after themselves. Nevertheless, I do expect that there will be radical changes, and though some of those currently predicted will never happen, others will take us almost entirely by surprise.

The sophistication of electronic commerce using these new technologies requires us to consider the respective responsibilities of government, international organisations, business and consumer organisations in meeting the challenge offered by these new developments. One of the key policy issues is whether electronic commerce should be purely market based, regulated, or a mixture of both. The social and economic theorists of the eighteenth and nineteenth centuries, especially Adam Smith, advocated a laissez faire approach to the free market. In the twentieth century, however, under the influence of theorists such as Keynes, Schumpeter and, of course, Karl Marx, much of liberal capitalism was replaced by managed economies. As the failures of this approach became clear, not only in the economies of
Eastern Europe but also in my own country and many others, we have turned to deregulation, regulatory reform and privatisation. Even in areas which depend on a fixed infrastructure, like telecommunications, competition is rightly seen as the best way of driving innovation and efficiency, for the benefit of users. Regulation is a poor substitute, to be used only when competition fails.

Yet while regulatory reform and competition dominate at the macro-economic level, every developed economy recognises a need for regulatory systems, whether statutory or voluntary, to underpin individual transactions. We all have systems of contract law, banking supervision, laws against fraud, and arrangements to protect consumers in what are inevitably unequal transactions with business. Translating these into the new electronic environment will not necessarily be an easy process. For example, when a consumer buys insurance, he expects to have a written contract and the law implicitly or explicitly expects that too. If there is a problem later, there will at very minimum be an agreed text about whose meaning people can argue. If the contract is concluded electronically then, unless special precautions are taken, it may be possible for one party to manipulate the text and argue that the contract was different from what it actually was. This is simply one example, not of a problem that is beyond solution, but of one that requires some thought for the new environment.

We also have to address such issues as security and privacy, advertising and information, liability and redress. If electronic shopping becomes commonplace, tracking an individual's purchases will provide a great deal of information about them, just as a credit card record may do now. Who has the right to collect and use that information, and for what purposes? Again, standards of taste and decency in advertising currently depend on where the advertisement is placed. Stricter standards are imposed on advertisements on poster sites than in adult magazines. Should a web site be treated like a poster, or like a magazine which people deliberately choose to look at?

Above all, we must address these issues in a trading environment which crosses the boundaries both of nation states and of trading blocs. If I visit a web site on a computer in Canada, and as a result buy something from a business located physically in the USA, whose law applies? Whose courts have jurisdiction? There are of course answers to such questions in the text books of international law, but the issue is whether those answers will produce effective systems for both enforcement and redress in the new environment. A consumer needs a case to be heard in a court to which he can get access, under law he understands and, if he wins, he needs to be able to receive his money.
The last of these is often the most difficult. Similarly, there is no point in an enforcement authority having power to act unless it can catch up with the offending business and, after whatever legal processes are necessary, apply some sanction if the business does not conform. Being able to catch up with the business is critical and may, in the new environment, dictate who should regulate. We may be forced to accept a system of home country regulation. This will be uncomfortable enough among the developed countries in this room. We all know that what is acceptable in Britain may not be acceptable in Sweden, or vice versa in terms of TV advertising to children. But how shall we cope with businesses that choose to site themselves in countries with very weak systems of consumer protection, especially when their true location may be hidden from the ordinary consumer?

In speaking of regulation, I do not necessarily assume that this will be done by governments. Other models are possible, involving more or less self-regulation. Indeed, I should be astonished if some elements of self regulation were not part of the way forward. One of the things I hope we shall explore in this conference is the roles and responsibilities of government, international organisations, consumer organisations and, perhaps above all, the various kinds of businesses who will trade in the new environment. We must find a way to allow competitive markets to flourish and consumers to trade with as much confidence across national borders as they currently can do at home.

Jay M. Tannenbaum  
Founder and Chairman, Commercenet, United States

I would like to talk about the two issues that, to my mind, have the highest potential for nipping the Internet commerce revolution in the bud. First are the growing concerns about issues like security, privacy, liability and other perceived risks of doing business on the Net that, if not addressed adequately and soon, will make consumers go elsewhere to do their shopping. Second is perhaps the even greater risk of governments, with the best of intentions, attempting to insulate consumers from those risks by over regulating and thereby nipping the technology and the evolution of innovative business practices in the bud.
Last year was a real watershed year, milestone for the Internet. For the first time, more than half of the people who were using the Internet actually bought something on the Internet, 54 per cent up from about 37 per cent the year before. This represented, by my estimates, about $500 million, and the estimates are expected to grow to around $1 billion this year and as much as $100 billion next year. I believe that these numbers are underestimates simply because they count only transactions that are consummated on the Internet. One of the most interesting numbers is that some much larger percentage than 54 per cent actually consulted the Internet in making a major buying decision, even if the final purchase was actually consummated by going down say to an automobile dealership and writing the check.

Now for a dose of reality. This 54 per cent of Net users is only about 5 per cent of the consumer population in the United States, and I venture to say this number would be 1 per cent or less of the general population in most of the rest of the world. So we do have some work to do to be able to move Internet commerce across what Geoffrey Moore calls the "chasm" to get to the mass market. Consumers and merchants alike must feel comfortable about doing business on the Internet.

I've long thought that Internet commerce has a lot in common with international trade because in both cases you don't know who you are dealing with. In international trade, basically two things emerged in order to provide some assurance; one is a legal and regulatory framework that people can understand and that set the ground rules, and the second is a set of commercial trust services to manage the risk which is inherent in doing business. That risk is not going to be eliminated. The law simply sets the framework and the trust services are what provide the guarantees and recourse by and large. The very same things apply in Internet commerce.

A second issue that was already alluded to by John Bridgeman is the fact that the Net is really global from the beginning. When a transaction can take place involving players on multiple continents, there are serious issues about whose laws apply, what a contract means and how you get recourse when something doesn't work. I think there is no alternative but to have the global Internet equivalent of a Uniform Commercial Code.

There are a whole range of services that have grown up in international trade to manage risk, things like letters of credit and escrow services and credit rating services and so forth -- those are the same types of services that in fact map over fairly well to the Internet. In the recently
proposed U.S. Global Electronic Commerce Framework which Ira Magaziner put together for President Clinton, it really does emphasise the two major principles that I think are important to see this Internet commerce move forward aggressively, while protecting the legitimate concerns of consumers. First we must realise that this is and has to be a global environment and that everyone has to get together. Our members are afraid of the possibility that countries will preemptively pass legislation that will make taxes and tariffs and the meanings of digital signatures vary from one country to another. The second is that in order to be able to protect consumers we need to have trust services that grow up within the context of this legal framework, but that are largely shaped by market forces.

So now let me talk about what some of those trust services might be, beginning with one that certainly all of you are familiar with, namely the very important services that are provided by card associations like VISA and MasterCard.

When a consumer makes a purchase, the merchant can take a card and swipe it through the little box and it goes back through VISANet to the consumer’s bank to determine that the account is good. VISA plays a very important role by setting policy, issuing credentials, providing governance, and, ultimately, underwriting the whole system by providing recourse mechanisms if necessary. There are many other trust services that organisations like VISA can provide and they still need to provide in terms of policy, governance and recourse. The first, of which we will hear a lot about during the next two days, is the digital signature. Verisign is one of many companies trying to establish themselves as certificate authorities for validating digital signatures. This system is very similar to the VISA model where banks themselves are the most obvious organisations to serve as certificate authorities and to have the ability to validate and guarantee digital signatures.

The kind of real time trust services that organisations like Visa provide today in verifying credit cards can also be applied on the Internet to a number of other trust services. Companies like Dunn and Bradstreet could vouch for an organisation’s credit rating while others, like Verisign, certify their very identity. Risk is an inherent factor in many business transactions. However, ameliorating these types of market risks can best be thought of as an opportunity and an area for businesses to take action rather than as something that requires government intervention. Indeed, since a global legal or enforcement system does not exist, commercial organisations such as Visa can
be far more affective in getting merchants to conform to set policies than can
governments.

There is great interest in trying to make the entire system convenient
and familiar because consumers are not going to want to know about the
esoteric mechanics of either digital payments or digital security, that all has to
be transparent. I believe it is inevitable that this will merge with the payment
and security infrastructure in the physical world. People will have one "smart
card" which will allow them to identify themselves and to shop in the physical
world or on the Net and I think we are going to see it coming very, very soon.

One thing I haven't talked about which is probably highest on the
agenda is the issue of privacy. I would like to argue that privacy is very much
subject to market forces and fits very nicely within this model as well.
Certainly, if there are two businesses, one of which says I will be completely
indiscriminate in giving the information that I gather about you to whomever I
like, and another business says I will rigorously protect your information, it is
quite clear which business the consumer is likely to chose to do business with.
The only problem is that the consumer needs to understand what the policies of
a given business are and have some assurance that the business is going to be
following these policies.

This assurance is what another trust service can provide. One such
service is called TRUSTe, which is a non-profit organisation started by
CommerceNet and the Electronic Frontier Foundation (a consumer privacy
advocacy group -- so we have both the commerce side and the consumer side
covered) designed to provide just those kinds of assurances about trust.
TRUSTe is an authenticated or branded logo, much like the Better Business
Bureau, except what the TRUSTe logo means is that this business discloses
what its privacy polices are and assures consumers that it will adhere to those
policies. This is not about right or wrong, what privacy policy should or should
not be, but rather only that a business will say what it is going to do and then do
what says it is going to do based on the principle of informed consent. You
want to be able to say that some information should never be revealed to
anyone and other information should be revealed under certain circumstance.
For instance I am interested in receiving information about cameras because I
am in the market for a camera, so anyone who wants that information can have
it. Perhaps the consumer will even be willing to reveal certain personal
information in exchange for financial compensation.
I would like to close by simply saying that I have three recommendations for what our members would expect from government in order to propel this move forward. Number one is that we do need the global legal regulatory framework that I mentioned. Second is to support the kind of market driven trust services that TRUSTe and many others represent. Finally, I hope the governments will get involved in their traditional role as first movers to promote the active use of the Internet in interactions between government and their citizens. One of the first of which is to recognise the legality of digital signatures as it relates to various kinds of electronic filings, tax returns, and the like.

I’d like to put forward a broader call for action. We have a unique opportunity in Internet commerce to get global commerce right. At the moment, much of trade is governed by a hodgepodge of bilateral trading agreements or regional trading agreements. The Internet is a green field, let's really take the opportunity to put together some landmark agreements that will set the stage for a global market place and perhaps that in turn will come back and teach the physical market place how to get things like a united Europe right.

The Honorable Robyn McDonald
Minister of Consumer Affairs, New Zealand

As we move towards the twenty-first century, using technology is now a way of life for people worldwide. I believe the twentieth century will be remembered as the age of technology. We have been fortunate enough to live in an era where advances in this area have been so rapid as to be breathtaking at times.

In turn though, these technological advances create many issues, whether they be ethical or particularised in the way that they are used. In this technological environment, consumers of goods and services can frequently feel like David facing Goliath, even more so now with the increasingly global market. There is huge potential in this new global market -- huge potential for benefits for consumers and huge potential for rip-offs.

New Zealand is seen as pioneering in its open approach to the marketplace. We have regular visits from intrigued officials and politicians
from all over the world -- places as disparate as Japan, Mongolia, and Tonga -- who come to talk to politicians and officials about the process and the practice of deregulation.

Deregulation and the changes to our public sector over the past decade have fundamentally changed the way New Zealand's economy operates. What hasn't changed is the enthusiastic way in which New Zealanders embrace new technology. It seems to be part of our culture. We are geographically isolated, but also travellers. Remember, our families travelled far to settle New Zealand, it is in our blood. For decades New Zealanders have decided that if the world can't make it to New Zealand, New Zealand will go to the world. Now with the Internet, the world is coming to New Zealand.

Our local research shows that seventeen percent of New Zealanders over the age of ten have access to the Internet with six percent having used it at least in the last month. Four percent of New Zealanders have shopped by the Internet, behind seven percent of Australians. I suspect that situation will not exist for long -- New Zealanders challenge Australians in most arenas. So we are no longer isolated but able to participate on a daily basis in the global market.

The potential advantages of an electronically accessible global market allows greater choice and potentially lower costs on a range of goods and services for consumers and similarly allows New Zealand companies to access huge new markets. But there are dangers too, the proliferation of pyramid style schemes offered on the Internet is an example of the perils consumers face if they don't have the right information. Equally important is the uncertainty of the support of their rights through legislation and methods of redress.

New Zealand is a world leader in consumer protection legislation. Our deregulated economy is based on the power of the consumer to make choices about the goods and services they wish to purchase. In such an economy, information and legislative back-up is essential. We have a framework of legislation including a Fair Trading Act, the Consumer Guarantees Act, and a Weights and Measures Act that provide both a protection and a mechanism for redress for contracts or purchases within New Zealand.

Both the global market and shopping by Internet present new challenges. These include cross-border fraud, obtaining redress across-borders when transactions go wrong, security of payment systems, privacy of information, and international approaches to product safety and liability. Yet it
is vital that governments do not lag behind technology in out-analysing and addressing the potential problems as well as embracing the benefits of the global market.

The issues I have just raised are obviously not going to be solved overnight, but international forums such as this are a positive step towards addressing them. In New Zealand we are attempting to understand the business opportunities and issues impacting the electronic consumer. We are aiming to encourage consumer and community groups and the business sector to think about and discuss the implications of electronic technology for New Zealand.

Determining the role of government and business in responding to the opportunities and issues which the Internet and the global market provide is a matter for each country to decide. Over all, the New Zealand government favours market based solutions to any problems that arise; responding to the gaps in the market in a way just illustrated by offering a new service to consumers.

Self-regulation within a sector or industry is another way of providing protection for both consumers and businesses which showed clearly that they are aware of the importance of responding to consumers promptly in maintaining credibility in the marketplace. This does not mean that the New Zealand government would hesitate to introduce legislation or regulation where it was demonstrably needed. However, a global market can make legislation aimed at protecting consumers within New Zealand impotent outside of it.

As Minister of Consumer Affairs, I support the introduction of an international code of practice for companies selling goods and services electronically. If companies selling on the Internet agree to abide by the code, and were recognised as having agreed to do so, consumers would have protection across borders that covered all these issues and mechanisms for redress. I am aware that legislation which sought to reach cross borders on the other hand would be difficult to write, unwieldy to administer and near to impossible to police.

Governments, consumer and community groups and business people worldwide need to move on this issue. An agreed code of practice will take time to hammer out and in the meantime consumers are a little like David facing Goliath without a slingshot. We have an opportunity at this international forum to work on ways which will empower consumers to make choices that provide them with the benefits of the global market and allow them to avoid the pitfalls.
Electronic commerce currently offers consumers significant advantages and significant risks. Securing widespread consumer benefits from electronic commerce requires reducing the actual and perceived risks without destroying the advantages. Electronic commerce technology appears poised for tremendous growth and broad adoption. What remains to be seen is whether appropriate regulatory policies can be devised, implemented, and kept current with the technology so that consumers can enjoy the significant advantages with sufficient safety.

1. Electronic commerce: Benefits and prospects for consumers

Consumers and suppliers alike can enjoy benefits from electronic commerce not possible from other means of selling goods and services. The number of consumers buying through electronic commerce is already increasing rapidly. These benefits coupled with the rapidly growing consumer use of personal computers and data communications services lead many experts to project dramatic growth in the quantity and breadth of the electronic commerce consumer marketplace.

1.1 Consumer benefits

A wonderful world of buying power and convenience is getting closer to consumer keyboards. Electronic access to a global marketplace can bring more powerful and efficient purchasing, greater choice, lower prices, more personalised service, and new kinds of products and services together with new ways to purchase.
More Powerful and Efficient Purchasing. The consumer in the electronic marketplace can escape many limitations found in the non-electronic realm.

Global data communications networks, especially the Internet and the World Wide Web, deliver greater and more flexible access to information. A consumer can learn about a supplier on the other side of the world as easily as about one around the corner. Because suppliers are freed from the much greater cost of physical publication, more detailed information is likely to be available. A supplier can afford to include ideas on how to use a product rather than state only terse technical specifications. Information is also likely to be more current because of the lower cost of changing electronic information.

A wider variety of information can be delivered electronically than in print or over television or radio. In addition to reading text, a consumer can hear audio and view a still two- or three-dimensional picture or a video. Some observers predict that future personal computers will allow the consumer to experience the scent and texture of the products being displayed.

Interaction with audio-visual material is also possible. For example, by moving the mouse, a consumer can cause the picture of a pair of slacks to rotate so that the back can be seen or the selection of a different colour. The consumer can change a picture’s magnification or stop a video at a single frame. The consumer can see how the slacks will look with various styles of shirts, shoes, and other apparel. The more sophisticated installations bring new meaning to self-service. A consumer can get answers to questions and complete complex orders without talking to a salesperson.

Electronic information is available whenever the computer containing the information is operating and connected to the network. The infirm consumer can access electronic commerce without physical travel. Racial, ethnic, gender preference, and religious minority consumers are more likely to receive non-discriminatory treatment because vendors have no physical contact. World Wide Web information is typically accessible twenty-four hours a day, seven days a week. Today, a consumer can order flowers, buy a book, book airline tickets and rental cars, secure tickets to a concert, authorise the purchase or sale of securities, transfer funds between bank accounts, and acquire computer software at any time of day or night, anywhere in the world where a connection to the Internet is possible.

Too much information could be worse than not enough, delivering more than the consumer has time or patience to read, hear, or watch. But
electronic information can be organised so that the consumer selects what to receive. General information can be skimmed. Additional details are available with a click of a mouse. This puts the consumer in control of how much information is read and the sequence in which it is read. Search software automates identification of relevant data. This allows the consumer to define what is desired, such as information about “pillows” and “down” and made in Italy, and dated within the past six months. The search software applies the criteria and reports the qualifying locations.

The World Wide Web and the Internet also permit linking information between suppliers. A screen of product descriptions can include references to products and services offered by others. This lets a consumer shop for related products from different suppliers. For example, a consumer could select a set of golf clubs from one manufacturer, then with a click of the mouse bring up another manufacturer to select a golf bag, and then complete the transaction with another click of the mouse to move to a package delivery service so that shipment can be arranged. The result is a “one-stop” shopping experience without being confined to any single vertically-integrated supplier.

Purchasing productivity could increase still further with wider use of “software agents.” A software agent is a computer program that performs tasks without human involvement based on instructions initially given by the agent’s owner. A consumer could direct one of its software agents to search on the World Wide Web for the lowest-priced business class ticket from Tokyo to Paris and purchase the ticket if the price did not exceed some value. While the consumer took care of other business or slept, the software agent would execute its search, make the purchase on the consumer’s behalf if low enough pricing was found, and report the results back to the consumer.

New Kinds of Products and Product Information. Improved consumer interaction with suppliers creates the possibility of new kinds of products and product information. Instead of selling the same novel to everyone, a publisher can offer story modules with the consumer selecting from alternative plot and character choices to assemble a custom version. A manufacturer could evolve the features and varieties of products based on customer interaction. “Customers may increasingly enter into symbiotic relationships with producers, becoming quasi-collaborators in product development and improvement,” writes David Bollier in the Aspen Institute report The Future of Electronic Commerce.
A similar process is possible for product information. A supplier could make it possible for consumers to post information about the supplier’s product or service, such as a movie or book review, or the compilation of consumer responses to an electronic survey. Consumers could therefore have the benefit of other consumers’ experiences.

More Vendor Competition. Eliminating constraints of distance and time zones, electronic commerce places a global marketplace at the consumer’s command. The lower cost for communicating information electronically and for processing transactions allows this marketplace to include smaller as well as more geographically dispersed vendors. Both the total number and the diversity of vendors should increase dramatically.

Lower Prices. Giving consumers access to suppliers around the world creates global price competition. Lower transaction costs can also contribute to lower consumer prices. Bollier reports that the Internet Shopping Network can handle a software order at 4-10 per cent of the cost of a telephone order and 2-3 per cent of the same transaction in a retail store. With physical distribution accounting for as much as 80 per cent of the total cost for some consumer products, significantly lower prices are possible for products and services that can be delivered as well as purchased electronically. Providing music, books, videos, software, and the like electronically reduces delivery cost to nearly zero.

1.2 Supplier benefits

Those who create, distribute, and sell goods and services to consumers also have reason to look forward to this new mechanism. All enterprises, including the small and medium-sized, can reach customers throughout the world instantly and comparatively inexpensively. Many vendors can sell globally without the costly infrastructure of world-wide retail stores, sales offices, distributors, or warehouses. Greater sales and inventory efficiency may be possible through the increased interaction with prospective customers that electronic commerce can afford. One-to-one marketing becomes possible on a massive and global scale.

Alert suppliers will also benefit from the new structure of product and service distribution likely to result from electronic commerce. With conventional distribution, a manufacturer must rely on wholesalers and retailers to serve customers in large volumes. Electronic commerce’s automated customer self-service capabilities can eliminate the need for these
intermediaries. The manufacturer no longer has to share profits with others. In addition, the manufacturer gains direct contact with consumers that can facilitate future sales.

Nevertheless, as the role of conventional intermediaries — such as retail store clerks, travel agents, bank tellers, and wholesale sales representatives — may diminish or end, new intermediaries have started to appear.

Conventional distribution focuses on getting the physical product and information about the product within convenient reach of the consumer so that a sale can and will occur. Thus conventional distribution is conceived in geographical territory terms. The complexity of responding to large numbers of consumers with different tastes, interests, degrees of sophistication, and so on, together with the efficiency of shipping products in bulk for as much of the distance to the consumer as possible, compels the manufacturer to form partnerships. Retailers service types of consumers within their physical area. Wholesalers service types of retailers within their physical area. Information and products flow physically from the manufacturer to the consumer through this hierarchical structure much as military commands flow through the ranks from generals to privates.

Electronic commerce connects manufacturers directly to consumers. The consumer gets product information directly from the ultimate source. The manufacturer can get customer preferences and needs directly from the ultimate source. Each consumer’s physical location no longer determines who the consumer contacts to purchase a product. With the purchase of intangibles that can be delivered electronically, physical location becomes irrelevant to product delivery as well. The Internet makes the connection between a French consumer and an Egyptian supplier virtually indistinguishable from the connection between a Parisian consumer and a Parisian manufacture.

Indeed, the physical location of a manufacturer or consumer cannot be known with certainty using today’s Internet technology. A manufacturer may be able to learn that the consumer’s computer has an address assigned to the Netherlands. However, the consumer may have in fact been in Belgium, and was dialling into the Dutch computer.

But if making the sale no longer requires conventional intermediaries, new types may arise in their place. Consumers will connect to brokers, aggregators, negotiators, matchmakers, directories, and the like for help navigating through the dense jungle of global marketplace suppliers. New
intermediaries will also be engaged to consummate a sale. Consumers will not tolerate having to learn a different payment procedure for each supplier. Many suppliers will not want to conduct their own investigations of consumer creditworthiness or pursue customers who do not pay as required. A payment intermediary could give consumers a consistent payment procedure (and a single bill to pay each month) while conducting a single credit investigation would relieve the need for separate inquiries by each manufacturer.

In addition, the one-to-one sales and marketing of electronic commerce requires the ability to deliver efficiently individual product quantities to numerous individual locations. Manufacturers will want to delegate this logistical complexity to a delivery company that has the necessary transportation and information management resources in place so that it can comparatively cheaply and reasonably quickly get nearly anything to nearly anywhere.

1.3 Prospects for electronic commerce

Significant electronic commerce takes place today. More than 20 per cent of the 10.3 million households in the United States using the Internet in 1995 bought something while on-line, according to one report. The three most common purchases were computer software, airline tickets, and clothing. Consumers spent an estimated US$2.2 billion buying products on the Internet.

Consumer electronic commerce has not yet come of age, but many intriguing examples have emerged:

- **Internet Liquidators** (www.internetliquidators.com): Online shoppers bid against each other for products. The products are offered during a limited time period, with prices dropping as the period elapses.

- **Internet Book Shop** (www.bookshop.co.uk): Claiming to be the largest online bookstore in the world, this British site allows users to choose books from a catalogue of more than 915,000 titles. The site also provides book reviews and news about forthcoming titles.

- **CDUniverse** (www.cduniverse.com): Discount-priced music in compact disc and tape cassette form can be selected by song title, artist, album title, or type of music. The user can hear a sample of the music or subscribe to an electronic mail newsletter
personalised to the user’s interests. Listings of selections include ratings and links to similar or influential artists.

- Virtual Vineyards (www.virtualvin.com): Established in 1995, this site has shipped tens of thousands of bottles of wine to online purchasers globally.

- Weekend a Firenze (www.nettuno.it/mall/): This site offers products from Florence, Italy, with 48-hour delivery promised throughout the world. Winner of numerous awards, the site also provides a virtual tour of Florence and weekly specials.

Several factors suggest consumer electronic commerce may grow rapidly. The equipment for electronic commerce is becoming commonplace. Analysts project 1996 world-wide personal computer sales as having exceeded 71 million units. Approximately 35 per cent of the 102 million households in the United States already own at least one computer, about the same number as owned television sets in the mid-1950s. World-wide personal computer sales are expected to grow 16.6 per cent a year, reaching over 130 million units in the year 2000.

Internet use is also increasing quickly. Today, over 35 million people are using the World Wide Web. Some 23.4 million households in the world have at least one member who is online. By the year 2000, that is expected to nearly triple to 66 million households. The number of World Wide Web sites is also growing rapidly, doubling every two to three months.

Greater proportions of Web users say they plan to buy a product or service over the Internet in the future. Although estimates vary widely, within the next five to ten years as much as US$600 billion of purchases will be made annually using the Internet. This represents 7.5 per cent of total forecast buying.

2. Consumer confidence in the borderless global market

Despite the great potential of electronic commerce for consumers, serious obstacles threaten achievement of this wonderful electronic commerce world. The very benefits that distinguish electronic commerce positively also create the risks that undermine consumer confidence in this marketplace.

Consumer safety risks must be eliminated or at least minimised. Only if appropriate practices, procedures, and protections make electronic commerce
practical and pleasurable for consumer use will the forecast droves of consumers materialise. Although consumers are already experimenting with electronic commerce in growing numbers, regular use by mainstream consumers will not occur until they perceive it to be a productive and safe way to do business.

2.1 Gaining and controlling access

A consumer cannot take advantage of electronic commerce without first being able to access it. This presently requires use of a computer connected to an online service or the Internet.

Although, as noted above, the consumer population with this capability is expanding rapidly, it remains a minority of all consumers. A critical mass of consumers using electronic commerce must exist before this marketplace will truly come into its own. Obtaining the full measure of that growth to critical mass requires making the electronic commerce consumer population more geographically and socially representative. The expense and knowledge needed to use electronic commerce impairs participation by those with less wealth or education. Many parts of the world lack adequate telecommunications facilities.

Technology may help. Computing and communications are likely to continue growing more powerful, flexible, and accessible. Using electronic commerce is becoming easier, demanding less training or prior experience. Terminals connected to the Internet have already started appearing in some airports, and may become as common as pay telephones. It remains unknown, however, whether access will become adequately universal and soon enough.

On the other hand, a jurisdiction may lack enthusiasm with all that electronic commerce has to offer. The borderless, global characteristics of electronic commerce conflict with policies aimed at protecting local manufacturing, distribution, and sales enterprises or regulating consumer purchases of any products or services that can be delivered electronically. Uncontrolled access to electronic commerce will also hinder if not eliminate a jurisdiction’s ability to keep a period of time free from commercial activity, such as during an official religious holiday. Then again, access controls could operate as a new form of trade barrier.

An individual consumer also may want to limit his or her access to electronic commerce. In some communities, consumers know that certain kinds
of businesses have been restricted to a specific geographical area. A consumer who does not want to encounter the restricted businesses can do so by avoiding the areas where they are located. Mainstream consumers may not use electronic commerce until a notice or other mechanism allows the consumer to avoid contact with similar kinds of businesses.

However, an enforceable electronic commerce “red light district” is nearly impossible to create.

Participants were asked to consider the following questions:

− Should governments adopt policies to promote greater universal consumer access to electronic commerce?
− If governments should adopt universal access-promoting policies, what policies would be likely to be the most productive?
− Should consumers have a right to avoid contact with types of businesses, and if so, what needs to be done to ensure that right?

2.2 Establishing identity

Lacking the means consumers use in conventional commerce to authenticate suppliers and suppliers use to authenticate consumers, electronic commerce has to adopt technological substitutes. Nonetheless, every transaction may not require the same degree of certainty about the consumer’s identity. Greater certainty of identification reduces anonymity and privacy. Too much certainty of identification therefore could be as harmful as too little.

In conventional commerce, physical contact simplifies supplier and consumer identification of each other. A walk-in consumer can know he or she is dealing with the desired supplier and not an impostor by examining the sign in front of the store, the signs and labels inside the store, and government permits to do business. An impostor store would be unlikely to survive long. Physical contact aids consumer identification. The supplier’s sales representative can see and speak with the consumer, and if particularly cautious, can ask to see a driver’s license or other government-issued identity card.
Although less identity information is available in mail order and telephone order transactions, it is typically sufficient for the supplier. The consumer’s payment by check or money order also reveals identity data. The shipment destination may also help. Finally, the supplier has the reassurance of talking to the telephone customer and seeing the postmark on the envelope and perhaps the consumer’s handwriting on the order form.

The mail or telephone order consumer may be at risk, however. One form of consumer fraud is for the impostor to call a consumer claiming to be a reputable company seeking to resolve a billing problem. The trusting consumer reveals information, such as a credit card number and expiration date, that will let the impostor make fraudulent charges.

Internet and the World Wide Web technology impairs each party’s ability to identify the other with certainty. Information packets are relayed from Internet sender to receiver without reliable identification data. True, electronic mail and World Wide Web communications include at least the name of the computer host originating the communications. But this host name may be unrelated to the sender’s location or identity. For example, a consumer in Toronto may dial into a computer host in Boston with the consumer’s own computer operating only as a remote terminal. The Boston computer host would be the originator of any electronic mail or World Wide Web communications. It would appear to the receiving supplier exactly as if the consumer were located in Boston. Furthermore, anonymous remailers and proxy World Wide Web servers exist that intentionally relay communications to isolate the sender’s identity from the recipient.

Finally, a communications sender with limited skill can replace the correct host name with something else, and thus mislead the recipient. This “spoofing” would allow a consumer to assume a fraudulent identity or geographical location. Spoofing is also used by fraudulent suppliers. World Wide Web sites have recently emerged that deliberately pose as authentic sites. By capitalising on an authentic site’s inadequate security, the impostor modifies the authentic site’s pages to reference consumers to the impostor site. This tricks the consumer into sending credit card or other payment information to the impostor.

It remains unclear how much the lack of dependable authentication will deter consumers from electronic commerce purchasing. A recent survey of United States consumers reveals that although 59 per cent worry about giving out their credit card information over the telephone, 71 per cent shopped by
telephone in 1996 and 57 per cent say they will make more purchases by telephone this year. Nothing has surfaced to indicate that merchants are suffering from more fraudulent transactions from electronic commerce than other means.

Even so, marketing and technological countermeasures have already appeared. In December 1996, VeriSign announced its Authentic Site Program. A participating supplier gives VeriSign information proving its identity. If VeriSign confirms this identity, VeriSign authorises the supplier to include the VeriSign Digital ID in the supplier’s electronic commerce World Wide Web pages. A consumer may then click on the Digital ID logo to gain confirmation that the page is truly that supplier’s and not a counterfeit.

Thus World Wide Web technologies can help solve problems World Wide Web technologies help create. But the VeriSign Digital ID Program, and others like it, in effect only re-target consumer trust from each supplier to the certifying intermediary. The intermediary must take measures to earn and retain that trust.

Passwords, passwords with third-party or smart-card verification, and digital signatures all exist today. Biometric verification may be common in the future. Each of these technology systems seeks to achieve two objectives: a means of creating an identification sufficiently difficult to forge, and a means of connecting the identification to the actual person with a sufficiently high degree of confidence. A mechanism will allow authentication without fear of a later repudiation on the grounds that the identification was forged.

**Password Authentication.** Computers have used password authentication for decades. Some systems require that a password meet certain criteria, such as a minimum and maximum length and the inclusion of at least one non-alphabetic character. Some systems also exclude passwords from a list of words most obvious to a potential intruder, such as the names of professional sports teams, and profanity.

Password authentication offers easy implementation but delivers limited security for electronic commerce purposes. It is only as good as the care exercised to keep the password confidential. If a consumer writes the password on a piece of scrap paper taped to his or her computer at work (an altogether too common occurrence), the password has limited value. If the password is transmitted from the consumer to the computer system in plain text over unsecured communications, the password has limited value. If the computer system requesting the password has little or no security for the file of
passwords in its data storage, the password has limited value. Some protection against fraudulent password use is possible by asking the user to provide identifying information in addition to the password, such as mother’s maiden name or government identification number. But the additional information is nothing more than an additional password capable of being compromised to the same extent as any other. Simple password authentication is also inadequate for electronic commerce because a consumer will either have the inconvenience of establishing and using a different password with each supplier or the insecurity of having one password stored with multiple suppliers so that a security breach at any one allows fraud on all.

Third-Party Verified Password Authentication. Improved password authentication is possible when combined with verification by a third party or the intervention of a smart card, or both.

With third party verification, the consumer sends the password (or other identification information) to a third-party authentication server together with the identity of the supplier with which the consumer wishes to transact business. The authentication server checks the consumer’s information. If it approves, it sends the consumer’s computer a “ticket” with encrypted information identifying the consumer to the supplier and valid for only a limited time period. The consumer’s computer software sends this ticket to the supplier.

Third-party verified passwords allow centralising the password verifying function. Even though the consumer is using a single password to access many different suppliers, each ticket is for a specific supplier for a specific time period. If it falls into criminal hands, the encryption prevents the ticket from revealing the consumer’s identity and the time limitation prevents the ticket from being used again. The third-party authentication server assumes responsibility for linking the password to the identity of the consumer. When the supplier accepts the ticket, it is trusting the third-party authentication server to have reliably confirmed that the person identified in the ticket is the person who transmitted the password.

But if an intruder compromises the authentication server’s security, or if the third-party’s authentication software or procedures are faulty, every consumer using that authentication server would be at risk. Both suppliers and consumers will depend on third-party verification from third-parties with a trustworthy reputation and sufficient wealth to reimburse losses, subject to legal action, should a security breach occur. Public or private insurance
coverage would spread the risk of loss among insured while introducing a party with the economic interest and leverage for imposing risk reduction practices. A government guarantee would also increase confidence in third-party verifying enterprises, although it is unknown whether taxpayers would be willing to underwrite this risk.

One way of limiting the financial exposure, and thus the cost, would be a legal limit to liability. Treaties, conventions, and statutes of this kind already exist in international practice, such as the limit on recoverable air travel baggage losses. Consumers can be encouraged to do their part to keep identification security intact by requiring the consumer to pay some portion of suffered losses. United States law currently compels consumers to pay the first US$50 of fraudulent credit card charges to give consumers incentive to protect their credit card from unauthorised use.

**Smart Card Verified Password Authentication.** Smart card verification can enhance security over the simple memorised or third-party verified password approach. The authentication process starts with the consumer sending a password to either the supplier’s or a third-party’s computer system. The computer system generates a random password and sends this back to the consumer. The consumer enters the random password into his or her smart card. Using the random password and some previously entered information about the consumer, such as a birthdate, the smart card calculates another password which the consumer sends to the computer system. The computing system knows the consumer identifying information, the random password, and the formula used by this consumer’s smart card, and therefore can run the same calculation to establish that the password is authentic.

Use of a smart card prevents access by someone who does not have the correct smart card in his or her possession at the time access is requested. Smart cards usually require entry of a memorised password (a personal identification number, or PIN) to restrict unauthorised smart card operation. Because a new password is calculated by the smart card and computing system with each consumer use, an intruder who intercepts a password gains nothing.

**Digital Signature.** The digital signature combines the advantages of third-party verification with asymmetric passwords, eliminating the need to entrust secret passwords to a common repository.

The heart of a digital signature resembles operation of safety deposit boxes at many banks. Each safety deposit box owner receives his or her own
box key. That key is required but not alone sufficient to open the box. Also required is the key kept by the bank. Only by using the two keys together, the box owner’s and the bank’s, will the box be opened.

Although the public and private keys result from a mathematical formula, the formula is sufficiently complex that someone who knows an owner’s public key cannot calculate the private key. The owner keeps the private key secret. The public key can be shared widely.

Each public key corresponds to one and only one private key. Consequently, only a password owner’s public key will match up with encoding by that owner’s private key. Anyone can possess the public key. What matters, as in the example of the bank safety deposit box, is the combination of the two public and private keys. No longer must a password owner share a secret password with others, fearful that breach of another’s security will put the password owner at risk. No longer will an entity tempt theft by keeping a database of secret passwords belonging to others.

Establishing that an owner’s public key corresponds to the encoding by the private key is only the first step towards authentication. Individuals and corporations can adopt public/private key combinations arbitrarily. Nothing about a public/private key combination in and of itself identifies any specific individual or corporation.

Authentication requires a second step, linking the private key to its owner’s identity. One answer would be to leave this to case-by-case solution. A consumer doing business with a merchant for the first time could demand information necessary to corroborate the merchant’s ownership of its public/private key combination. However, it is hard to imagine what information a consumer in Australia could ask a Danish merchant that would prove the merchant’s key ownership if the Australian consumer knew nothing about the merchant or Denmark. It might not eliminate the possibility of a knowledgeable impostor. In any event, requiring this exercise would make it nearly impossible for the Australian consumer to do business with numerous distant merchants, let alone take advantage of software agents to transact business automatically.

A more practical answer would be for a trustworthy person or organisation to establish the connection between public/private key pair and identity and then make that information available on request. Digital signature terminology calls the identity-corroborating information a “certificate,” and the trusted third party providing the information a “certification authority.” A
comparable mechanism operates today in connection with passports, national identification cards, and driver’s licenses. Issuance of the documentation by a responsible government agency known to use appropriate measures to prevent counterfeiting creates confidence that the documentation accurately identifies the person presenting the documentation.

The certification authority’s trustworthiness remains essential to digital signature authentication. A digital signature certificate faces if an impostor can issue fraudulent certificates by pretending to be the certification authority.

A chain of certification could be used to certify the certification authority. Each certificate from the authority could include the authority’s own digital signature verifiable through some “higher” authority. Thus a highly trustworthy agency, such as a government department, could investigate and license a limited number of certification authorities. A licensed authority could in turn investigate and sanction certification authorities. No one would have to process each and every certificate request. The organisations below the initial (“root”) level would compete with each other on the basis of dependability, responsiveness, and cost. On the other hand, complete authentication would require the effort of working up the chain of certification to the root level. Furthermore, massive commercial disruption would result if, for example, the root level certificate authority revokes or suspends its certificate for the next level because that would trigger revocation or suspension of all certificates issued by that level and so on down the chain.

An alternative to a chain of certification would be for a certification authority to sign its own certificate, relying on its own reputation to back the certificates it issues. That reputation could be based on each authority’s size, insurance coverage, and experience in connection with other activities, together with actual experience over time with the value of its certificates.

Insurance and auditing mechanisms would bolster confidence in authentication from either the chain-of-certification or self-certification models. Certificate authority insurance would guarantee a source of funds for recovery of damages caused by bad authentication. It would also lead to insurance companies compelling certificate authorities to meet and continue meeting standards as a condition of getting insurance and remaining insured. As with financial information, auditing would introduce a disinterested professional who would evaluate compliance of the certification authority’s procedures with established standards. A clean audit report is likely to be one
of the prerequisites to insurance. A higher level authority in the chain-of-certification model is also likely to insist on a clean audit report for subordinate authorities.

Yet another alternative is known as the “web-of-rust” model. Instead of certificate authorities and subscribers, each user participates in the web-of-trust by publishing a database of electronic mail addresses and public keys the user has reason to trust as being dependably linked to each other. A user seeking to authenticate a public key can either consult a database belonging to someone he or she already knows or can check several databases, on the theory that the more nodes in the web validating the link, the greater confidence the link is authentic.

Regardless of the authentication model, network technologies simplify requesting and supplying certificates. A certificate request can be sent over the Internet to the certification authority. The certification authority can automatically check its database and dispatch the certificate over the Internet. Nothing limits the certification authority to existing physically in any particular province, nation, or continent provided the certification authority has Internet access. If the certification authority discovers that it is misidentifying a public/private key owner (perhaps because the original investigation was based on misinformation or because the owner failed to preserve the secrecy of the owner’s private key), the certification authority can stop issuing certificates.

Biometric Identification. Instead of a password or private key that can be entered by anyone who comes to know it, biometric identification depends on a physical characteristic unique to each individual human. This may be a finger print, retinal scan, voiceprint, DNA analysis, or some other accessible characteristic shown to be unique. Identification of this kind would eliminate the need to memorise a password and would prevent unauthorised use (short of coercion or other violent act).

Biometric identification is already in use today. A credit union in Indiana uses a finger imaging scanner to read a finger print and convert it into an algorithm for subsequent comparison. Finger-image identification achieved an 83 per cent approval in a study conducted by Alan F. Westin, professor of public law and government at Columbia University. Some biometric identification scanners check for warmth and blood circulation. Nonetheless, widespread use of biometric identification is estimated to be four or five years away. Biometric identification systems are still bulky and costly. The effectiveness and safety of these methods also lacks general experience.
Smaller and cheaper biometric systems are almost certain to be developed, and greater use is likely to result that will provide a better basis for assessing dependability and safety.

**Participants were asked to consider the following questions:**

- Should government:
  - limit third-party verification liability for losses?
  - create public insurance or guarantees for third-party verifying entities?
  - require third-party verification entities disclosure of assets and liability terms?
  - sanction an industry self-regulation body to certify, audit, and police third-party verification entities?
  - license third-party verification entities?
  - leave third-party verification entirely unregulated?

- Are uniform laws necessary to avoid states competing to attract third-party verification entities by protecting consumers least, or will market forces discourage inadequate protection?

### 2.3 Preserving Privacy

Electronic commerce also raises privacy concerns for consumers and suppliers. Authentication and accountability thwart anonymity. Long-distance transactions increase the difficulty of determining the trustworthiness of the other party. Low security networks leave unprotected electronic transactions vulnerable to interception. Databases of electronic transactions are easily accumulated, easily analysed for patterns, and easily transferred to others for unanticipated combinations with other information. Little wonder privacy protection ranks as among the greatest barriers to consumer use of electronic commerce.

Consumers today often participate in in-person, mail order, and telephone order transactions based on assumptions about the risk of others gaining access to sensitive information or the likelihood that information about the transactions will be given to others or used for other purposes. Part of these assumption come from direct knowledge of the supplier. Well-known,
reputable merchants and service providers, especially those in particularly sensitive markets such as financial services and health care, are commonly believed to have adequate measures in place to protect consumer privacy. Part of these assumptions come from past experience and education. Many consumers are complacent about their privacy protection with traditional transactions. Many consumers are unaware of the new technologies, changing practices, and other privacy risks even these transactions involve.

Some of these assumptions stem from the logistics of the transaction. Purchasing laundry detergent at the grocery store can be limited to direct, physical exchange of anonymous cash for detergent. The store captures no information about the consumer. The cash contains no information useful to a third party for tapping the consumer’s other financial resources or compiling the consumer’s buying habits. The consumer makes no contact with any grocery store systems that might turn over any of the store’s sensitive information. Even mail and telephone order transactions involve a communication medium consumers believe to be secure.

The characteristics and novelty of electronic commerce interfere with these assumptions. Electronic commerce permits customers and suppliers to do business over large distances. The consumer will often transact business directly with the manufacturer rather than through a distribution intermediary. Electronic consumers and suppliers are likely to use an authentication mechanism, eliminating the anonymous transaction possible in the grocery store. Electronic commerce forces creation of machine-readable data records capable of far easier, cheaper, and more powerful retention, analysis, combination with other information, and exchange than paper transactions. The patchwork communications quilt of the Internet includes numerous security weak links at least theoretically susceptible to unauthorised access. Mass media news stories, films, and television programs have increased consumer awareness, and fear, of how risky it may be to conduct business electronically.

Privacy Protection Policymaking. Electronic privacy concerns surfaced globally during the 1960s and 1970s in response to the consequences of the growing computerisation of records, public and private. Numerous stories appeared in all media showing impersonal and allegedly infallible mainframe computers causing individual suffering because of erroneous information or information improperly disclosed to others, or information produced by drawing false conclusions from database combinations. The regulatory responses in Europe and the United States differed dramatically, however.
Strong feelings about personal information privacy as a human right led to adoption of significant legal regimes governing both public and private data collection. The European Union recently completed a data protection directive that will mandate data protection laws throughout Union membership. These laws create a central privacy authority, require database registration, and regulate information transfer.

Privacy protection in the United States introduced far less regulation of private data practices. Federal and state legislation was enacted for public recordkeeping. New federal laws also governed specific industries, such as credit information, and electronic communications. Proposals for more pervasive privacy regulation or creation of a central privacy commission have gathered little significant political support to date. U.S. Federal Trade Commissioner Christine Varney has suggested characterising privacy protection as a business practice to bring it within the FTC’s regulatory jurisdiction. It remains unclear whether this view will gain acceptance.

The 1970s debate continues over the possible dangers and proper regulation of central databases. Additional debate is inevitable over the additional privacy threats from personal computers, distributed databases, data communications networks, satellite and other wireless data communications, and other post-1970s technologies. Regardless of the technology involved, questions have to be answered concerning who has how much control over information access, who can inspect and correct information and prevent others from modifying information, and who must take what measures to ensure information accuracy on an ongoing basis.

Notice and consent are the essential precepts for modern privacy protection, according to a 1995 report of the Privacy Working Group of the United States government’s Information Infrastructure Working Group. Customers have a right to know what information is being collected and how it will be used. Many consumers have little awareness of current information practices, such the use of frequent customer programs to compile a detailed transaction history for each participant. The Privacy Working Group report also concluded that consumers should be able to limit the use and re-use of personal information.

Technology can facilitate solutions as well as create problems. One example is the CommerceNet-coordinated TRUSTe initiative. Built on the assumption businesses will want to include an TRUSTe certification logo on their World Wide Web pages to ease consumer fears, the TRUSTe initiative
conditions the right to display the TRUSTe logo on compliance with TRUSTe guidelines. Basic guidelines oblige the business to disclose its information practices, to notify consumers about information collection and subsequent use before collecting the information, to allow consumers to delete or correct collected information, and not to transfer or display information identifiable to a particular consumer unless already public. A business assumes additional obligations depending on whether it wishes to display trustee's “No Exchange (Anonymous)” mark, “1 to 1 Exchange” mark, or “Third Party Exchange” mark.

Central to the TRUSTe initiative’s likelihood of success is the ease and speed with which the Internet can deliver consumer awareness of the TRUSTe certification mark and its significance. Each TRUSTe mark is a link that explains its meaning to the consumer, something not possible with a print certification program. World Wide Web technology also makes it practical to require a business to delete a certification immediately after it is determined to be out of compliance.

The sharp international differences in privacy protection approaches themselves impede electronic commerce. Suppliers have no dependable way of knowing where a consumer is located. They therefore have no dependable way of knowing what legal compliance may be necessary. Communications on the Internet often different routes, even within a single message transmission. Information for an electronic commerce transaction may travel through another nation without the knowledge or control of either party to the transaction.

**Encryption Policymaking.** Data encryption offers consumers and suppliers a technological means of preventing unauthorised interception of transaction information or access to stored information. Encryption codes a message based on complex algorithms and a user-selected key. The longer the key is in length, the more possibilities an intruder may have to try before stumbling into the correct key by brute force. But faster and more powerful computers decrease the effort required. A computer science student recently linked 250 computer workstations together and in less than three and a half hours decoded a message encoded with a 40-bit key.

More powerful encryption may introduce dangers as well as advantages. Modern law enforcement plays a communications cat-and-mouse game with international terror, organised crime, global espionage, and other criminal elements. More powerful encryption could keep law enforcement from intercepting criminal communications. Analogous to hand guns and other
modern personal weapons, the same encryption that can be used for consumer
defence can also be used for criminal perpetration and information warfare.

The United States government has struggled to limit availability of
powerful encryption primarily through the use of export controls. No law
restricts development or use of encryption within the United States. However,
U.S. software publishers have in general avoided incorporating powerful
encryption into their products. Few want to tackle managing separate U.S. and
non-U.S. product lines. Fewer want to risk the severe penalties United States
export control laws authorise against negligent as well as intentional export
control violators. Uncertainty over interpretation of export control regulations
combined with government confusion over what is and is not “encryption” has
also hindered implementation of non-encryption technologies such as digital
signatures.

For several years the Clinton Administration has been advocating
loosening export controls on more powerful encryption provided the encryption
technique lets law enforcement gain access to a key. The most recent policy
will grant a company licenses to export of 56-bit encryption software if the
company agrees to submit a plan for implementing a “key recovery” scheme.
Several companies recently received export licenses under this policy.
Nevertheless, software publishers and privacy advocates have continued to
express strong opposition to the policy.

In 1996, the National Research Council’s Committee to Study
National Cryptography Policy issued its report in response to the study
requirement contained in the 1994 defence authorisation statute. The committee
recommended, among other things, easy export of encryption using the Data
Encryption Standard and 56-bit keys. The committee also recommended
allowing export of more powerful encryption if the product developer agreed to
help law enforcement have a method of decrypting messages.

France and the United Kingdom have each been developing
encryption policies involving trusted third parties to hold keys under sufficient
security and to provide the keys to law enforcement under appropriate
circumstances. Other countries are considering policies based on trusted third
parties. The European Commission has proposed creating a European network
of trusted third parties.

The OECD has organised an international forum to facilitate
international co-ordination of encryption policy. This effort has included
participation from trade associations from across the OECD’s membership.
Participants were asked to consider the following questions:

- If privacy needs vary from consumer to consumer and transaction type to transaction type, how can public policy best support this degree of flexibility without leaving consumers completely unprotected?
- How can consumer requirements for access to encryption protection best be reconciled with reasonable law enforcement concerns?
- What steps should be taken to better educate consumers as to their electronic commerce privacy threats, rights, and responsibilities?
- How can privacy and encryption policies function in the borderless, global electronic marketplace and yet accommodate national differences?

2.4 Avoiding fraud and misrepresentation

Electronic commerce confronts consumers with few new fraud or misrepresentation problems. Similar schemes exist regardless of the technology. The global, borderless electronic marketplace complicates compliance with consumer protection regulations on the one hand and enforcement of consumer protection regulations on the other, although the Internet and World Wide Web also make it easier for consumers to learn about fraud and misrepresentation risks.

Fraud and misrepresentation online differ little from fraud and misrepresentation anywhere else. According to the Internet Fraud Watch of the National [U.S.] Consumer League’s National Fraud Information Center (http://www.fraud.org), the top five Internet scams are:

- **Pyramid schemes**: Multi-tier marketing arrangements with profits based on fees for recruiting new sales agents, rather than selling products.
- **Service scams**: Gaining advance payment for services ultimately never performed.
- **Sales scams**: Gaining advance payment for goods never delivered.
− **Business opportunities:** Securing large fees for the purchase of business opportunities based on unrealistic earnings projections and promises of support that are never delivered.

− **Work-at-home scams:** Sale of business opportunities, or business tools, supplies, or information, or both, for a work-at-home business far less than the promised income opportunity.

These same schemes also appear the most using mail order, telephone, and other fraud mechanisms.

A rare instance of World Wide Web-specific fraud was recently halted by a United States court at the request of the U.S. Federal Trade Commission. According to the FTC press release, a firm posted advertisements on several World Wide Web sites offering free “adult entertainment.” To access the information, however, the consumer had to first download a special “viewer” software program. Without notice to the consumer, running the viewer program turned off the speaker in the consumer’s modem and then dialled a telephone number in Moldavia. The consumer would stay connected at charges of more than US$2 a minute until the computer was turned off.

Regardless of whether the fraud or misrepresentation is novel or time-tested, it too can harness the power of the World Wide Web. Using the World Wide Web, the fraudulent supplier can cheat orders of magnitude more consumers at a fraction of the time and expense. For example, in its mere seven week lifespan the Moldavia modem fraud is estimated to have grossed US$1 million or more. Moreover, the fraudulent supplier can base its information anywhere in the world, snare numerous consumers before the true nature of its operation becomes known, within a few seconds move to a server located anywhere else on the globe, and begin again with a new identity. No boiler rooms to construct or attract attention. No staff members who may become police informants. No temptation to be based physically in a jurisdiction with more stringent rules or law enforcement.

Even if law enforcement can identify and locate a fraudulent supplier, successful apprehension and prosecution will often depend on co-operation from multiple jurisdictions. Regulations created for older technologies may leave it unclear whether a violation occurred at the physical location of the supplier, the physical location of the World Wide Web server delivering the information, the physical location of the consumer receiving the information, or some or all of these locations. Equally unclear in many jurisdictions is the compliance responsibility (if any) of third parties, such as the concern
providing the fraudulent supplier with its connection to the World Wide Web. With fraudulent suppliers so difficult to pursue, providers of World Wide Web telecommunications, financial, delivery, and other services make much easier targets. Some argue that service providers are best positioned to police its customers on law enforcement’s behalf. They have financial assets, physical locations, technical expertise, means of sharing enforcement costs across many customers, and significant stakes in preserving reputation and remaining in operation. Others respond that service providers cannot reasonably monitor how their services are used any more than telephone companies can prevent use of their services for telemarketing fraud. Instead, legitimate consumers and suppliers will be hurt as service providers withdraw rather than assume a legal responsibility they cannot fulfil.

The characteristics of the World Wide Web also increase the likelihood of more innocent violations of consumer protection regulation. Easy and inexpensive access to the World Wide Web brings to the global electronic marketplace suppliers without the expertise or resources to comply throughout the world. Even large, experienced suppliers are confounded by the compliance problems caused by the instantly global nature of this electronic commerce marketplace. The supplier neither knows nor can control the location of his customers. The supplier has no practical mechanism for avoiding violation of the inconsistent, sometimes contradictory, consumer protection rules throughout the world.

On the other hand, the World Wide Web also facilitates distributing information that can increase consumer self-protection and supplier compliance with law. Inexpensive access to frequently updated information can alert consumers to scams. The Internet Fraud Watch is one example. Another is BBBOnLine, sponsored by the Council of Better Business Bureaux in the United States. BBBOnLine monitors advertising claims and provides online reliability reports. A participating company or organisation can include a BBBOnLine symbol on their World Wide Web pages that will link consumers to that participant’s reliability report. Consumer protection agencies can use the World Wide Web to inform suppliers about regulations.

Participants were asked to consider the following questions:

− How can jurisdictions better harmonise consumer protection laws to simplify compliance?
To what extent, if any, should service providers, financial institutions, physical delivery services, or other third parties be held responsible for policing against fraudulent suppliers?

What mechanisms are needed to foster greater cooperation among consumer protection law enforcement agencies in pursuing trans-jurisdictional violations?

How can development of World Wide Web fraud information sites and other non-enforcement anti-fraud measures be encouraged?

2.5 Finding and examining goods and services for suitability and quality

A consumer will often find that the electronic marketplace provides greater product and service information coupled with immediate delivery of text, audio, graphic, video, computer software, or other intangible products. Then again, as with mail order, telephone, and other remote transaction mechanisms, an electronic marketplace consumer may find that the product or service they receive fails to satisfy expectations. Characteristics of the electronic marketplace may make it more difficult for a consumer to avoid product suitability and quality problems.

As noted above, the electronic marketplace can offer a consumer far richer information about products and services the consumer may want to buy than in-person or remote transaction mechanisms. Few retail stores offer seven day a week, twenty four hours a day access to detailed product specifications, application ideas, and experiences of other consumers. Catalogues cannot deliver audio and video in addition to graphics and text. Technology available today allows consumers to manipulate information from the supplier, rotating a picture or seeing how the product will work with other products.

But the electronic marketplace also offers new sources for misunderstanding. The lack of colour accuracy standards for monitors and printers interferes with consumers seeing what they will receive. Future enhancements to electronic marketplace technologies, such as full-motion video, tactile sensation, aroma, or interactive immersion may increase the perceived realism of the depiction beyond what the product’s or service’s reality, much as toys in television commercials can fail to come to life in the actual toy. The instantly global World Wide Web audience challenges suppliers
to select and describe what they sell in universally appropriate terms, accommodating global differences in language, culture, and taste.

As with intentional fraud and deception, the World Wide Web’s powerful information providing abilities may equip consumers to make wise decisions about products and suppliers without requiring new laws. And also as with intentional fraud and deception, the characteristics of the World Wide Web make it far harder for law-abiding suppliers to comply with consumer protection laws that vary significantly from jurisdiction to jurisdiction.

Participants were asked to consider how advertising and disclosure regulations should be adjusted to take into account the new capabilities of the global electronic marketplace.

2.6 Creating binding agreements to purchase

Consumers and suppliers in the global electronic marketplace must be able to enter into enforceable agreements. But conventional paper contracts with hand-written signatures are impractical for the global electronic marketplace. If consumers are to enjoy the benefits of electronic commerce, agreements in electronic form and signed digitally must receive the same legal recognition as those on paper with hand-written signatures.

Dependable agreements have long been necessary for commerce. A supplier will not provide goods or services without assurance of being paid. A consumer will not pay for goods or services without assurance of recourse if the supplier fails to perform as promised. An enforceable agreement gives each party greater confidence the other will fulfil its part of the bargain.

Early contract law detailed rituals required to form an enforceable agreement. Modern practice minimises the significance of formalities. But enforcing a lawful agreement still includes proving the agreement’s terms and the actual consent of each party to those terms. A written agreement, complete with each party’s signature, provides the needed evidence should any doubt later arise as to what the agreement said or whether each party in fact agreed. It must be made possible to prove conclusively the agreed-to terms for an agreement in electronic form together with the assent of each party to the agreement. Even if each party has established reliable authentication of the other, the act of approval must be connected tightly to the terms approved. No change in the agreement terms should without each party’s consent.
Increasing that risk for electronic agreements is the manner in which they can be formed in the first place. Captured as machine-readable data, electronic agreements can be constructed by machines. A supplier’s software agent program can communicate the terms under which the supplier is willing to do business. A consumer’s software agent program can receive this communication, and based on criteria programmed by the consumer, respond with the terms the consumer will accept and the revisions the consumer desires. If the supplier and consumer have programmed their respective software agent with ranges of acceptable terms, the two programs may be able to identify a mutually acceptable agreement. This could occur in a matter of seconds and without the direct, contemporaneous human intervention normally associated with legally enforceable agreements. Furthermore, because the electronic agreement is only represented in electrical signals, it may be more readily modified without leaving a trace.

Some jurisdictions have statutes denying judicial enforcement of agreements for certain transactions unless the agreement is captured in a signed writing. Fortunately, many have updated their laws to accept electronic agreements as a writing. Article 11 of the UNCITRAL Model Law on Electronic Commerce authorises an agreement offer and acceptance by data messaging. But the existence of jurisdictions that still require a written, paper agreement, combined with the inability of consumers and suppliers to determine with certainty the geographical location of the other, creates a risk that an electronic agreement will not be enforceable.

If electronic agreements are recognised, the digital signature technology used for authentication can furnish a means of proving the agreement terms and their approval by the parties. Instead of transmitting only a digital signature, as in the case of authentication, the signing party associates the signature with the agreement text. A mathematical algorithm called a “hash function” converts the text into a shortened but unique version. This is encrypted using the signing party’s private key and sent to the other party along with the agreement text.

The receiving party verifies that the agreement text is exactly what the signing party signed by apply the same hashing function to the text. Using the signing party’s public key, the receiving party can confirm creation of the digital signature by the signing party’s private key and that the hash results are identical. Any discrepancy in the hash results indicates that the text as received is not identical to what the signing party signed, whether because of a transmission error or intentional tampering.
Jurisdictions are beginning to enact statutes legitimating digital signatures. The state of Utah’s act follows the U.S. American Bar Association guidelines by accepting digital signatures based on public key technology. The state of California’s act limits authorisation of digital signatures to transactions with the state, but adopts a technology-neutral approach. It legitimates any digital signature that is unique to the sender, is under the sender’s sole control, can be verified by the receiving party, and by its own content will reveal whether any change has been made to the associated text. Article 7 of the UNCITRAL Model Law on Electronic Commerce uses even broader technology-neutral terms, legitimating a digital signature if it identifies the sender, indicates the sender’s approval of the associated text, and uses an appropriately reliable methodology.

Participants were asked to consider the following questions:

− Should consumers get special protection from the speed of electronic contracting, for example by providing a “cooling off” period during which a consumer may repudiate an electronic agreement, or from automatic formation of electronic agreements by software agents?

− If consumers get special protection, how will suppliers know that it is dealing with a consumer entitled to protection?

− Are consumer interests better served by technology specific or technology neutral digital signature legislation?

2.7 Making payment

Effective methods for tendering payment are as critical to electronic commerce transactions as in any other setting. Financial services industry consultant Cynthia Glassman identifies seven fundamental requirements for a payment system:

− **Reliability:** Payments received in the specified form at the expected time, every time.

− **Accuracy:** Payments are for the correct amount to the correct party at the correct time.

− **Privacy/Security:** The system is safe from fraud, security breaches, and privacy breaches.
− **Safety**: The system can withstand shocks (for example, capacity transaction volumes or the loss of a communications line).

− **Accessibility**: All users can access the system.

− **Liquidity**: The system provides funds when needed.

− **Recourse and Finality**: The consumer retains a limited ability to reverse erroneous payments, but at some predetermined time the payment become irreversible.

Suppliers want to be certain they are paid. As in in-person, telephone, and mail order transactions, consumers want an easy to use payment system with coverage as universal as possible. “The question is, can people trust that their electronic money will be accepted now and in the future?,” writes David Bollier in the Aspen Institute report *The Future of Electronic Commerce*.

Credit card, virtual credit card, and stored value/virtual cash systems currently vie to become electronic commerce standards and the consumer payment mechanism of choice. Each system type and variety has its advantages and drawbacks. New, small companies are competing against established, multinational financial services enterprises. Meanwhile, governments have started contemplating how these payment systems may affect monetary policymaking.

**Credit Cards** Credit cards enjoy far wider acceptance today than all other electronic commerce payment systems combined. One market research firm predicts that up to 15 million World Wide Web sites will accept credit card payment by 1998. Many (but not all) consumers already purchase using credit cards. The mechanisms for settlement of credit card charges are well established and involve financial institutions with extensive assets, global operations, and considerable experience. Credit card transactions leave a clear audit trail, a benefit for those wishing to document their expenses and a detriment for those concerned about protecting their privacy.

The greatest consumer concern about using credit cards for electronic commerce payments is the fear credit card information will fall into criminal hands, leaving the consumer to pay fraudulent charges and recover their credit rating. Suppliers try to reassure consumers by noting that credit card information is more likely to be intercepted at a restaurant or a store than online. United States law limits credit cardholder liability for unauthorised use to US$50, and other jurisdictions have similar statutes. But consumers
victimised by unauthorised use or theft of identity also suffer tremendous disruption, inconvenience, and embarrassment.

In early 1996, Visa International, MasterCard International, IBM, and other associations created SET (Secure Electronic Transactions) to bring safe credit card payment to consumer electronic commerce. The first secure end-to-end transaction using SET took place on 6 January 1997, when IBM’s Nordic Director purchased a copy of Stephen King’s novel “Rose Madder” from Landemanns Forlag with a Eurocard/MasterCard and an attached certificate authenticating the purchaser’s identity.

A SET transaction begins with encryption of the purchase order as one document and of the purchaser’s credit card number as another. Accompanying the credit card number is a digital signature that authenticates the cardholder and the cardholder’s desire to purchase from the supplier. The encrypted information is then scrambled according to a SET algorithm and encrypted again before being sent to the supplier.

The supplier uses SET-compliant software to decrypt and unscramble the information package. Using the cardholder’s public key and the hashing algorithm, the supplier can confirm the purchaser’s identity and the integrity of the purchase order. The supplier has no reason to decrypt the purchaser’s credit card information. It can forward that information to its bank in encrypted form for settlement. Consequently, the supplier has no responsibility for keeping secure a database of unencrypted customer credit card numbers.

*Virtual Credit Card.* An alternative to encryption for permitting a consumer to pay by credit card while keeping credit card information from the network can be based on adding a trusted fourth party to the existing consumer, supplier, and credit card company. This contributes the additional benefit of facilitating participation by suppliers too small to qualify for credit card merchant status, such as many of those newly serving the global marketplace by exploiting electronic commerce’s low entry and transaction costs.

First Virtual Holdings has built a virtual credit card payment system of this kind. As of the end of 1996, nearly 2 000 suppliers and 150 000 consumers were using the First Virtual Holdings System.

To become eligible to purchase through the system, a consumer first calls First Virtual Holdings on a telephone and supplies a credit card number. First Virtual Holdings will issue the consumer a personal information number.
The consumer purchases goods and services by sending its order and the First Virtual Holdings personal information number to the supplier. The supplier responds with an electronic mail confirmation. Then the supplier transmits the purchase amount and personal information number to First Virtual Holdings. First Virtual Holdings charges the consumer’s credit card account and deposits funds in the supplier’s account.

An impostor might learn a consumer’s personal information number and make fraudulent purchases, just as a credit card thief would purchase using stolen credit card information. First Virtual Holdings could be expected to watch for unusual activity. A consumer’s First Virtual Holdings account could have an intentionally low daily and total transactional limit, independent of the consumer’s limit on the credit card, to minimise the damage from an impostor.

Stored Value/Virtual Cash. Credit cards offer convenience, but at a price. In 1996, First Virtual Holdings’ charged suppliers US$29 for each transaction plus 2 per cent of the transaction amount. This would be prohibitive for a supplier of online information that frequently needs to collect amounts of less than a dollar for downloaded data. Credit card systems are not sufficiently efficient for micropayments at this level. Moreover, not all consumers want or can qualify for credit cards. Neither the credit card nor virtual credit card payment system is accessible to these consumers.

Payments through the CyberCash system of as little as US$25 become possible once the consumer has deposited funds by check or credit card into a special bank account. The consumer can then purchase by sending an encrypted order and payment information to the supplier. The supplier sends the encrypted consumers information and the supplier’s identification to CyberCash. CyberCash decrypts the information and transmits it to the bank over a private network to authorise payment.

DigiCash’s stored value payment system, first implemented by Mark Twain Bank, adds consumer anonymity as if the consumer paid the supplier directly in cash. As of the end of 1996, Mark Twain Bank was serving 100 suppliers and 1 000 consumers with its system.

The Mark Twain/DigiCash system is built around a digital bank connected to the Internet. A consumer who wishes to make a purchase first contacts the digital bank to request the number and denomination of digital tokens or “coins” the consumer requires. Each coin is an information packet containing the denomination amount and the serial number. The software running on the consumer’s computer generates a random serial number for each
coin and then encrypts the serial number using an algorithm DigiCash calls the blinding factor. If the consumer’s account at the digital banks does not contain enough funds, the consumer must order a “real” money transfer in an amount at least equal to what will pay for the desired coins.

The digital bank takes the blinded serial numbers received from the consumer and encrypts them again using the bank’s digital signature private key. This authenticates the coins. After deducting the total value of the generated coins from the consumer’s digital bank account, the digital bank transmits the coins to the consumer where they are kept recorded on the consumer’s storage device until used for a payment. These coins are said to be in the consumer’s “virtual wallet.”

The consumer pays a supplier by instructing the DigiCash software on the consumer’s computer to transmit sufficient digital coins to total the payment amount. The supplier has no need to authenticate the consumer’s identity. Instead, it authenticates the validity of the coins by sending them to the digital bank. The digital bank confirms that the coins have a properly encoded serial number and have not been spent previously. Then the bank credits the supplier’s account and the serial numbers of the spent coins are retired permanently.

Electronic currency has been called “the biggest revolution in currency since gold replaced cowrie shells.” Each payment system stretches existing practices and creates potential dangers for consumers. Mitigating these dangers compels re-examination of first principles concerning monetary systems and policy. Stored value payment systems return private companies to the business of issuing private note currency, raising similar issues of acceptance, conversion, redemption, valuation, money supply management, counterfeiting, currency laundering, payment speed and accuracy standards, reserve and insurance obligations, liability responsibility and limits, financial disclosure and auditing, consequences of electronic payment enterprise bankruptcy, obligation to honour stop payments, consumer privacy protection, and more. Uncoordinated policies could further confuse consumers and payment system enterprises alike.
Participants were asked to consider the following questions:

- What blend of regulation of electronic payment enterprises and marketplace competition will best protect consumers with respect to:
  - payment speed and accuracy standards?
  - financial disclosure and auditing?
  - liability responsibility and limits?
  - reserve and insurance obligations?
  - obligation to honour stop payments?
  - consumer privacy protection?
- Should consumers have a right to execute anonymous payments?

2.8 Recovering damages caused by failure to perform and defective products

Once the thrill of global shopping subsides, electronic commerce consumers will have to face the reality of suppliers who fail to perform as promised and products that arrive broken or otherwise defective. Consumers have these problems today with telephone and mail order buying. Except few consumers use telephone or mail order to purchase from suppliers on other continents speaking in languages, operating in cultures, and regulated under legal regimes all quite possibly very different from the consumer’s own.

Purchases of intangibles delivered electronically may pose additional problems. Line noise or a local communications interruption could keep a consumer from receiving intact the software, graphic, text, or other machine-readable intangible. But the supplier may have no way of verifying the consumer’s claim. Alternatively, the supplier can blame many other parties and problems beyond its control along the route up to and including the consumer.

Incompetent suppliers and poor quality products may not endanger consumers all that much. Information can travel quickly and inexpensively in the World Wide Web environment. New intermediaries are already focusing on helping consumers discern suppliers and products deserving patronage. Although the present blur between information and advertisement can tax the consumer’s critical judgement skills, reputations for expert, objective assessments may well emerge to show consumers the way.
Intermediaries may also emerge as the answer for enabling consumers to recover damages. Credit card companies already intervene on behalf of consumers to convince suppliers to solve legitimate problems. In many instances the supplier responds to the threat of losing future purchases through that credit card. Consolidation of electronic payment systems could give electronic payment intermediaries similar clout. In some instances the credit card company absorbs the loss to retain its relationship with the consumer. Credit card companies now purchase insurance policies to gain competitive advantage concerning the protection afforded consumers using that card while at the same time reducing the situations in which the credit card company is caught in the middle of conflict between its consumer customer and its supplier customer.

Arguably too much consumer protection may threaten the growth of electronic commerce more than too little. If a jurisdiction with a significant population of electronic commerce consumers has laws that unduly punish suppliers and shield consumers, many suppliers may decide that the risks outweighs the benefits. As observed above, at present a supplier in the borderless, global marketplace cannot select the jurisdictions where the supplier will not do business. The supplier must in effect decide to do business everywhere or nowhere.

The rapid and inexpensive flow of information may also generate an environment too hostile for many suppliers. False rumours about a company or its products can spread rapidly, gaining perceived veracity from repetition alone. Provocative information, whether true or false, tends to persist for years or decades. A number of myths have gained what seems to be a permanent place in people’s memories. No quantity of correction seems sufficient to erase the error. The borderless, global marketplace needs reliable, professional information sources to inform not inflame consumers.

**Participants were asked to consider the following questions:**

- In what respects, if any, do product liability issues in the electronic commerce marketplace differ from product liability issues in other commercial environments?

- How should electronic payment intermediaries be encouraged to buffer consumers from the risks of the borderless, global electronic marketplace?
2.9 Knowing what laws and regulations govern

A recurring problem undermining appropriate consumer protection in the borderless, global marketplace is the conflict and uncertainty over what jurisdiction’s regulations will govern. The borderless, global marketplace in its present form has little correlation to geographical divisions of sovereignty. Regulatory differences can disrupt operation of the electronic marketplace throughout the world. On the other hand, both creation of a world government or an agreement to leave the borderless, global marketplace to self-regulation appear unlikely to occur.

From liability for incorrect authentication to product liability regulation, uncertainty over what regulations will apply is the overriding impediment to rapid and broad-based development of global electronic commerce. Businesses are unsure how they can comply with varying and sometimes conflicting regulations. Consumers are unsure what protections will be available. These uncertainties prevent electronic commerce from fulfilling the visions of a more competitive, efficient, and productive global marketplace.

Local Governance Model. The most commonly applied model to date has been to assume that the borderless, global marketplace has physical boundaries and can tolerate inconsistent regulation analogous to the physical in-person marketplace. The local governance model denies that the electronic marketplace differs in any significant respect from conventional marketplaces.

Thinking of this kind allows the Assistant Attorney General of Minnesota to declare “if you are on the Internet, you are coming into this state, so there is jurisdiction here.” It allows the government of Hong Kong to file a US$13 million lawsuit against a U.S. citizen for violating Hong Kong copyright law by making available pictures from Action Asia magazine through an Internet server in the United States. It allows a British court to permit an English physicist to sue a Swiss researcher under British libel and slander law for comments posted to the Internet. It allows a federal court in New York to issue an injunction under United States trademark law for unauthorised use of the trademark on a World Wide Web site located in Italy.

The local governance model has superficial attraction. It requires no understanding of how the Internet or the World Wide Web function. No change in thinking is necessary. Instead, the court applies local law to protect the rights of local citizens.
But use of the local governance model also produces harmful consequences. Although it may protect local citizens pursuant to laws enacted to protect them, it creates a compliance nightmare for anyone publishing information or selling products in the borderless, global electronic marketplace. The sole strategy available to a reasonably risk adverse business is to comply with the regulations of the most restrictive jurisdiction, regardless of that jurisdiction’s size or location. It brings Leonard Wibberley’s satire *The Mouse That Roared* to life, allowing a small duchy to determine the world’s regulatory policy. It also promotes international forum shopping. The willingness of British courts to apply Britain’s strict liability libel standard to statements published over the Internet from anywhere in the world invites a flood of libel action filings in Britain.

**World Government Model.** If local governance causes inconsistency, disruption, and forum shopping, the logical alternative would be to negotiate an international treaty that organises a global electronic commerce governing body. The borderless, global electronic marketplace would have a single governing authority. One set of rules would apply. One tribunal would resolve disputes and make interpretations. The global governing body could also develop the technical expertise to write intelligent regulations.

Nevertheless, no global treaty or global governance appears likely. Many of the issues touch deeply rooted differences. Some countries believe in strong central government protection of privacy while others believe in minimising intervention in the private sector. Some countries have a tradition of strong individual rights to free speech. Others accept the state as a protector of social morality. No consensus is likely to support creation of a global governing body, either.

**Brave New World Model.** Several legal scholars have suggested that the borderless, global marketplace represents an entirely new domain, a New World that should evolve its regulations independent of the physical world’s institutions and precedents. David Johnson and David Post of the Georgetown Law Center, the chief proponents of this model, support their view by observing that physical location has no relevance to the global marketplace environment. Information and transactions in this realm transcend physical boundaries. Rather than struggle to impose a physical model on the intangible, the global marketplace should be recognised as something separate.

Johnson and Post cite as an analogy the evolution of the *Lex Mercartoria* or Law Merchant to govern international trade during the Middle
Ages in the absence of co-operation among European kingdoms and empires. Official government lacked the authority and expertise to establish pragmatic commercial law. Those who understood the environment best, the merchants themselves, were best able to devise the most appropriate rules of conduct and resolution of disputes. Similarly, Johnson and Post contend, official governments today lack the authority and expertise to regulate the World Wide Web. The better answer is to let World Wide Web users evolve the rules best suited to the World Wide Web.

A variation on the Brave New World model proposes use of technology to channel behaviour instead of rules and institutionalised dispute resolution. At the extreme, fraud would not occur in the global electronic marketplace because software would be programmed to filter World Wide Web sites declared to be fraudulent. More down to earth, instead of a government agency prosecuting an electronic commerce scam, information about the scam would be exposed in detail. Individuals and companies could then guide their own behaviour without paternalistic government intervention.

The Brave New World model offers advantages. First, Internet and World Wide Web users have engaged in self-regulation for many years. Many conventions, technical and behavioural, have evolved successfully through process. Establishing the global marketplace as an enclave protected from national and local governments would allow this tradition to continue. Second, self-regulation requires little or no institutional infrastructure. Leaving this emerging community to define its own rules would relieve governments from the expense of writing and enforcing regulations. Third, sub-communities would be left free to develop their own codes of conduct. Those who wish to trade in full-motion video clips could establish the rules best suited to that purposes while those who wish to trade in jazz records could establish the rules best suited to that. This capitalises better on the global electronic marketplace’s distributed network architecture than conventional “one size fits all” regulation. Fourth, the Brave New World model preserves the utopian aspirations for the global electronic marketplace. Some see the Internet and World Wide Web as a fresh start, a community where structures fostering true liberty and justice can develop without the baggage of prior attempts to create free and just societies.

Despite the utopian optimism of the Brave New World, it too seems unlikely to prevail. Self-regulation can work when the participants share values and have approximately equal resources and political power. A mainstream global electronic marketplace would hardly fit this description. Participants from throughout the globe would represent a wide diversity of values. Self-
regulation is unlikely to protect the poor, ethnic and other minorities, and those with more limited education or technical understanding. Allowing a law of the commercial jungle to govern would not create the promised liberty or justice, but would reinforce the power of those already in control.

Moreover, the Brave New World model is constructed on a false premise. The global electronic marketplace may not respect traditional borders. It may represent a new technology that allows world-wide relationships at high speeds and low costs. But it cannot claim an existence wholly divorced from the rest of human affairs. Humans are the marketplace’s participants. How the global electronic marketplace functions affects humans, even those who never directly participate. Existing government institutions will not stand idle and allow behaviour on the global electronic marketplace to inflict harm on their constituents.

Participants were asked to consider the following questions:

- What criteria should be used in determining the most appropriate source of principles for regulating the borderless, global electronic marketplace: consistency with established practice? ease of implementation? local control? promotion of commerce? protection of consumers? administrative efficiency? fairness?

- Can the technology and regulation of the borderless, global electronic commerce marketplace be designed to operate effectively without accommodating more local interests and concerns?
PANEL SUMMARIES - Day One

Session I. CONSUMER OPTIONS IN THE GLOBAL MARKETPLACE

Chairman
Mr. Roscoe Starek (Federal Trade Commission, United States)

Panel 1 - The Internet Operating Environment
Mr. Yves Leroux (Digital Equipment, France)
Ms. Sally Green (The Internet Bookshop, United Kingdom)
Mr. Alex Dalgliesh (American Express Interactive International, United Kingdom)

Panel 2 - Virtual Money: Consumer Payment Options
Mr. Per Ladegaard (PBS A/S, Denmark)
Mr. Andrew Konstantaras (VISA International, United States)
Mr. Robert Caplehorn (Mondex International Ltd., United Kingdom)

Session II. CONSUMER PRIVACY AND DATA PROTECTION

Chairman
Mr. William P. Fagan (Office of Consumer Affairs, Ireland)

Panel 1- Cryptography
Dr. Mads Bryde Andersen (University of Copenhagen, Denmark)
Mr. Amisha Marty (Service Central de la Sécurité des Systèmes d’Information, France)

Panel 2 - Protecting Transactional Data
Mr. Simon Davies (Privacy International, United Kingdom)
Mr. H. Robert Wientzen (Direct Marketing Association, Inc., United States)
Mr. Jacques Ribs (Commission Nationale de l’Informatique et des Libertés, France)
PANEL SUMMARIES - Day Two

Session III. JURISDICTION IN CYBERSPACE:
WHO PROTECTS CONSUMERS?

Chairman
Mr. Pierre Gabrié (Directorate General for Competition, Consumer Affairs and Fraud Repression, France)

Panel 1 - The Role of Business and Government in International Consumer Protection
Ms. Christine Varney (Federal Trade Commission, United States)
Mr. Dan L. Burk (Seton Hall University, United States)
Ms. Glee Harrah Cady (NetCom, United States)
Mr. Jim Murray (European Consumers’ Organisation, Brussels)
Mr. Atsushi Niimura (JCB, Japan)

Panel 2 - Protecting Consumers from Cross-Border Fraud and Misleading Conduct
Mr. François Benveniste (Calvacom, France)
Mr. John Rothchild (Federal Trade Commission, United States)
Mr. Christian Huard (Association de l’Education et d’Information du Consommateur de la Fédération de l’Education Nationale, France)
Mr. Tadahiko Fukuhara (Chuo University, Japan)

Panel 3 - Unsafe or Defective Merchandise: Product Liability Protection in the Global Marketplace
Mr. Edward A. Cavazos (General Counsel, Interliant, Inc., United States)
Mr. Jeffrey B. Ritter (ECLIPS, Ohio Supercomputer Center, United States)

Session IV. SUMMATION
Reporter
Ms. Christine A. Varney (Federal Trade Commission, United States)
Session I

CONSUMER OPTIONS IN THE GLOBAL MARKETPLACE

Summary of Remarks

Chairman

Mr. Roscoe Starek
Commissioner, Federal Trade Commission, United States

Panel 1 - The Internet Operating Environment

Speakers

Mr. Yves Leroux, Corporate Security Program, Digital Equipment, France
Ms. Sally Green, Senior Marketing Manager, The Internet Bookshop, United Kingdom
Mr. Alex Dalgliesh, Director of Interactive Travel, American Express Interactive International, United Kingdom

Summary of Questions and Answers

Panel 2 - Virtual Money: Consumer Payment Options

Speakers

Mr. Per Ladegaard, Managing Director, PBS A/S, Denmark
Mr. Andrew Konstantaras, Vice President, VISA International, United States
Mr. Robert Caplehorn, Company Secretary and General Counsel, Mondex International, Ltd., United Kingdom

Summary of Questions and Answers
Session I

CONSUMER OPTIONS IN THE GLOBAL MARKETPLACE

Roscoe Starek
Commissioner, Federal Trade Commission, United States

I have the distinct honour of being chosen by my colleagues of the Consumer Policy Committee here at the OECD to be the chairman of the working party on consumer markets. In that working party over the last few years we have been following up on some of the issues raised in our 1994 conference on the global marketplace. One of the projects we undertook at that time examined the various forms of payment cards, how do they work, and how consumers obtain the rights to redress if, for example, the transaction that they engaged in cross-border was fraudulent, or the goods were damaged, or lost. Here in 1997 we are looking at how commerce is conducted on the Internet. What are the forms of payment, how do we do business on the Internet, how do we get goods and services, and are those transactions that we may or may not want to engage in going to be secure? Then, what forms of payment we do have available to us, what forms will be available in the future, and what are the rights of consumers for redress if while conducting business on the Net?

Panel 1 - THE INTERNET OPERATING ENVIRONMENT

Summary of Remarks

Yves Leroux
Corporate Security Program, Digital Equipment, France

Surveys have shown that the majority of Internet users today are men (66 percent) with relatively good levels of education and income although more recent data shows a marked increase in the number of women online. These Internet users spend an average of 5 1/2 hours per week online primarily
searching for information and using Electronic Mail. I would like to give you an overview of what electronic commerce represents to Internet users today by introducing you to some of its most innovative and useful features.

Electronic commerce is generally divided into two parts, 'business to business' transactions and 'business to consumer' transactions. We are primarily interested in transactions between businesses and consumers.

The first example I would like to show you is a music shop found at 'www.cdnow.com,' which sells compact discs for both music and films. The difference in this online shop is that, just as in a real record shop, it is possible to listen to a musical clip. You click on the piece of music you want to hear, and you will listen to it using a device called 'Real Audio.' Real Audio allows for the immediate (real time) playback of an audio clip but it sends no data to your computer which means that it cannot be replayed. In some areas, this real time playback sufficiently addresses the problem of copyright protection. However, in certain countries, Authors and Composers Societies consider this real time playback to be the same as broadcasting music, and that each time someone logs into the server, a payment should be made for each piece of music that is heard.

My next example comes from Canada, where there is a system which allows people searching for a house to see the offer on the Net. With the click of a mouse, you can go into an increasing degree of detail to find exactly what and where you want to rent or buy. This system also contains a 'tunnel' that enables real estate agents to be connected directly to the server using specially coded and authenticated access. The special access afforded only to real estate agents allows them to load new offers on the server or to withdraw properties which have already sold. Thus, the file is kept up to date in 'real time' and can be accessed 24 hours a day by people both in Canada and around the world.

Another interesting use of the Net stems from the launching of 'Windows 95' by Microsoft. The company needed an efficient way to respond to questions from potential clients and to register incoming orders. During the launch of its preceding program, Microsoft had used a toll-free telephone system for this consumer interaction. However, even with 2 500 operators responding to calls, people were forced to wait in a 40 minute queue to get a response. The quality of the replies was also far from optimal for most people, as it was geared to an audience of computer specialists already familiar with the software. Microsoft decided to create a web site to respond to consumers during the subsequent launch of Windows 95 -- consumers logged in and were
provided all the information they could reasonably want to know about the program. This site -- which used five computers -- ultimately received 1,800,000 calls and resulted in 200,000 sales of the software package.

The Internet is also being used successfully to improve the image and services of an institution. The Massachusetts Motor Vehicle Registrar set up a server that allows citizens to pay traffic fines using a credit card. The transactional part of this operation is secure and coded; you send in your name, address and payment specifications and the information is encrypted in the system. The server also allows you to renew your car registration. (The initial registration must still be done in person at the registration office because you cannot prove via the system that you are the owner of the car.) Access to the service has reduced the time and frustration for a great many people who have taken advantage of it and has generally raised the image of the Motor Vehicle office.

In the area of banking we have Wells Fargo Bank, which has made its entire customer service operation available on the Net. Customers can open an account, ask questions and obtain a variety of information, and even use online demonstrations to test specific services. Consumer credit could equally be simplified. People would be able to make their request for credit by filling in a form which sets out all of the necessary parameters. If they see that one parameter has been omitted, they add it and relaunch the process. This too could be conducted in an environment providing coding, authentication, and the transactional security that is one of the primary preconditions of electronic commerce.

These are just a few examples of the innovative uses being made of the Internet, and if the expansion of the medium continues, they are only shades of what we have ahead.

Sally Green
Senior Marketing Manager, The Internet Bookshop, United Kingdom

The Internet Book Shop is one of the largest electronic book shops in the world at the moment. Our store is open 24 hours a day and features integrated online ordering. We have more than a million book titles available -- which means we have 12 miles of virtual bookshelves for you to browse and advanced search criteria so you can get exactly the book you want. The site
contains descriptions, contents, reviews, jacket covers, and sample chapters in order to make it as much like going into a book shop as if you are touching and feeling the books. We have a shopping basket so our customers can put their purchases into a shopping basket and run it around the shop to their hearts content until they are ready to check out.

When we opened the Book Shop in June 1994, we had printed order forms and no sales at all. We now have online credit card entry, we accept all types of credit cards and we process nearly 7 000 orders per month. Since November of 1996, we have seen a 25 per cent growth in orders month-from-month. We have 50 000 regular users and because we can track people, we know when they have come back, who they are, and what they bought before.

I think probably the best way for me to describe how we respond and behave with our customers is to give you a whistle stop tour around the shop. I'll concentrate on the ordering process because that is the area where our customers are most concerned about security and payments. You can either search for a book that you want or you can take our recommendation. We offer a whole range of featured titles including our "top one hundred" so which allows you to see what other people have bought and buy it too. You'll get information about the authors with links to other pages to give you very comprehensive information. We also have a very complex search engine where you look for a book by title, choose an author, an ISBN (the number on the back of the book if you happen to know it) or by publisher.

Once a customer has selected a book, he has the option to either place it in his shopping basket and continue shopping or order it immediately. When a customer is ready to check out, he is also presented with an option for payment. He can either check out securely, where everything is encrypted and goes into our secure server, or he can check out nonsecurely and fax or telephone us with their credit card details. At the end of the process, the customer gets a receipt with a reference number that gives him something tangible to print out if he wish to follow up.

We give you as much information as we possibly can about what we know about you and your order online. You can also access and maintain your own account which allows you to change your credit card details, your name, and your address and you can do it all online. More sophisticated technology is now becoming available that allows us to do some very complex and personalised marketing to our customers. But we do give all of our customers a
choice, and we only use the information that each individual allows us to use and only for the purpose for which it is intended.

Alex Dalgliesh
Director of Interactive Travel, American Express Interactive International, United Kingdom

I work for the interactive travel group at American Express. What we do is sort, develop, and implement a range of automated solutions that meet the need and expectations of our leisure and corporate travel customers.

Why is travel suited ideally to the Internet? For travel suppliers, like airlines, reportedly their cost of distribution are approximately 20 per cent of their total costs, and there is considerable pressure on the industry to reduce these costs. The industry is already online. Airlines, for example, have had computer reservation systems automating their reservation process for over 20 years. The current range of airline sponsored global distribution systems (GDS) host not only all major airlines, but most major hotel groups, nearly all major car rental companies, and an increasing number of tour operators, cruise companies, and related travel suppliers. In addition, every day airlines input more than 200,000 fare changes into their systems in an attempt to fill those last seats on their aircraft. Real time access is critical, and we believe the Internet is well suited to that task.

In the U.S., spending on travel over the Internet reached $126 million in 1996, and a they’re predicting a ten-fold increase to $1.5 billion in the year 2000. In global terms, we believe the potential is quite enormous. There are something between seven and ten million travellers using the Internet right now, and that represents a spending power of more than $10 billion.

We’ve had our own commercial website in the U.S. since April 96 and we have a website for student card members that began some years before that. The growth of this website has been beyond our expectations. Although we offer a number of American Express services in the travel field, we’re actually targeting leisure air, small business air, and large corporate air travel. We are currently getting over 4,000 visits to this site each day. In addition to travel, we have an area for card information, including online applications for new card members. We provide a shopping feature allowing our card members to shop over the World Wide Web providing some price guarantees and
purchase protection if they use our card products. We also provide a range of advice to small businesses in our business services area and a financial services area which includes online investment opportunities and access to market funds.

The AMEX website is a secure site. What this means is that users with browsers that support our security protocols will get an on screen message advising them that they are accessing a secure site, and conversely warning them when the site is not secure. We are also using the latest secure socket layer encryption technology which effectively scrambles data which is transmitted from computer-to-computer and we believe this gives our customers a reasonable level of security today. But we are moving however towards the SET (Secure Electronic Transactions) protocol, which we believe will provide the highest level of security available in the industry. As a further safeguard for us as much as for the consumer, we are currently restricting commercial transactions on our U.S. websites to consumers with a U.S. billing address or U.S. issued credit cards. Because of local pricing issues and airline fare regulations requiring local ticketing in each country, it would be quite difficult for a start-up company to provide a truly global website, so there are barriers to trade in my business.

I believe that if we as an industry get payment security right, then the consumer should feel even more secure when booking over the Internet then some of the more traditional methods of booking, like the telephone. The consumer should also benefit from lower prices. After all, they are now doing the work and they should share in the agency supplier distribution cost reductions I referred to earlier. The travel service provider that can provide all of the benefits you see there, these are the people that are going to win in the global market place of the future.
Panel 1 - THE INTERNET OPERATING ENVIRONMENT

Summary of Questions and Answers

The discussion following the panellists presentations began with a question about the cost-savings involved in doing business on the Internet and whether or not the savings realised through a reduction in administrative and other transactional costs are being passed on to consumers. The panellists indicated that where margins are sufficient and they had the ability to offer discounted merchandise, services or shipping, they do intend to pass the savings on to online consumers.

There was also some discussion of the use and potential benefits of alternative distribution channels -- either developing relationships with wholesalers and distributors based in another country or major market or distributing goods electronically directly online. All options were being considered.

This led to a discussion of potential problems with copyright infringement and royalty payments to authors, artists and others with intellectual property concerns. It was noted that this problem is compounded by the differing regulations and tariffs imposed by countries around the world.

Finally, a question was posed regarding privacy and the fair treatment of transactional data. Panellists noted that responsible companies take consumers’ privacy and security concerns seriously and make their specific privacy policies known. However, even where a company’s privacy policies are made readily available online, their experience has shown that consumers do not generally access the information on the site. It was also noted that security and the protection of information on the Internet is imperative and that companies interested in promoting Internet commerce must take online data security seriously.
Panel 2 - VIRTUAL MONEY: CONSUMER PAYMENT OPTIONS

Summary of Remarks

Per Ladegaard
Managing Director, PBS A/S, Denmark

When we look at the future we expect that chip cards, home banking, and the Internet will be the three major elements that will influence the future infrastructure for payment systems and banking. We expect the three will be integrated in the near future. The Internet is really taking off now as it becomes part of the global infrastructure for information and payment transactions. What is interesting with an infrastructure solution is that upon that you can build applications and business solutions. Without doubt, the chip card will be the future bank card not only due to the potential for fraud but because it affords us the opportunity to combine different functionalities into one chip. We also expect that the bank card will be quite embroaded as it will always be in the pocket of the customer.

The SET solution combined with the chip card environment might be one of the driving forces toward the development of the chip card infrastructure. The number or the points of interactions will continue to increase. We started with the ATM, added PC shopping, and in the coming years we may see TV and telephone equipment with payment options as well. We don't think this will happen unless the parties involved realise that security is the key to customer acceptance and confidence in the Internet and the electronic future.

Security is a question of combining a variety of elements. We believe that the security for vital data must be based on public key encryption, certificates and digital signatures. Operating on the Internet without a digital signature will be just as insecure as using an ATM system without personal identification number codes. Everyone has the potential to benefit from a global industry standard like SET, both from the easy access and standard equipment worldwide and from the transactional security measures it provides.
Consumers are interested in online shopping primarily due to convenience; 24-hour accessibility, less travel and time savings. Merchants can get immediate and secure payment with authentic cards, access to a worldwide customer base, and a shop that is open 24 hours a day.

The SET solution involves installing a secure software solution on the cardholder’s computer which can generate certificates and digital signatures. The same software is installed on the merchant’s side. PBS issues digital certificates and provides a payment gateway to the existing card payment systems which are connected internationally.

We are already considering converting home and office banking solutions to the Internet. We will provide our banks with software solutions that will enable them to convert existing home and office banking systems directly to the Internet using the same security philosophy we have in SET. These new solutions have the ability to do more encryption than what is currently used in SET including offering the ability to encrypt entire documents. In the medium to long-term, we see the chip card integration with the Internet making it even more convenient for customers to use electronic commerce -- a chip card that can be used from any PC and not be bound to a single PC with SET software installed.

Security is the key to success, and many security elements which will be used on the electronic commerce solution have, to some extent, already been used in the banking environment in the past. I think many industries here can learn from the experience in the banking environment.

Andrew Konstantaras
Vice President, VISA International, United States

I think that today for the consumer portion of payment the appropriate theme is trust. When we look at how trust is developed, I think we will learn so many things about how we ought to proceed. My basic premise is trust is not something you can legislate. Trust is not something you can purchase. Trust is something that is earned through experience, and I think if we remember that in the context of Internet commerce it will give us some very clear direction as to the path we should take.
In the industrial age and the post-industrial age, banks were the entities people trusted with their tools of commerce. We believe that in the information age, banks once again will have that role because they have already earned the trust of consumers. I think it is important for us to remember that trust crosses all jurisdictional boundaries and that banks are the primary financial bodies for managing consumers' money.

I think it is important to compare the difference between traditional commerce and electronic commerce. In traditional commerce, there is a whole range of goods that you can purchase and the environment is a face-to-face. You can pay with cash, you can pay with check, or you can pay with a payment card.

Payment cards have been seed to be one of the saving graces of the old system because they may allow you to conduct commerce on the Internet. However, there is a security problem in current Internet structure. People can listen in on your communications and take your card information, and it is possible for them to commit fraud with that information.

At VISA, we explored how to promote Internet commerce so that our banks can offer a secure service for their customers -- both the card holders and the merchants.

It first came down to defining security. We believe that security has three components. There must be privacy of the card holder information relating to the card account, the expiration date, etc. There must also be data integrity, so that the information is not changed and, very importantly for us, there must be authentication of the parties - knowing who you are dealing with.

VISA worked together with MasterCard, IBM, Microsoft and several other technology companies to put together the SET protocol, which stands for Secure Electronic Transactions. SET was designed to be a global solution that would provide a method for full security for payment information. Our goal was to focus on the payment component.

We came up with what is called a protocol. Which is a series of messages that go back and forth between various parties. We are not promoting any actual code, we are promoting a method for communicating between various parties. The important thing is that each company that comes up with a SET application must conform to the message description in the SET protocol. In this way, we will have interoperability between all the applications, and we will be able to shop with a Microsoft browser on a
Netscape server with a PBS back-end. As long as they are complying with the SET protocol, we will have a solution that is international and interoperable.

VISA is very conservative with respect to security. The Internet provides a very different environment with respect to the safety of electronic commerce. Simply because there is not a tremendous amount of fraud today, does not mean that it is not a very real possibility. The approach chosen by VISA and MasterCard in SET to protect against fraud and loss is known in cryptography circles, as message level encryption. What this does is take single message, a payment instruction, and secure it.

In contrast, there is also something called channel level encryption where you create a pipe between two parties and you send lots of things down that pipe, so no one else can break into it. That approach does not provide the necessary authentication. You may be sure that no one is interrupting your conversation through the pipe, but you do not know who is on the other end. Another important aspect of SET is providing that authentication component.

My recommendation is to remember that trust cannot be legislated, and trust cannot be bought. It needs to be earned through time. VISA and other payment entities have developed that trust, and it is important to continue to use and build on that trust as we move into the information age. Too much legislation too soon can do far more damage to the consumer than good, and it is important to keep that in mind.

Robert Caplehorn
Company Secretary and General Counsel, Mondex International, Ltd.,
United Kingdom

We all need to keep an open mind and appreciate that principles that have worked well in relation to physical commerce and existing payment systems, may not be appropriate for the new paradigm that is emerging. With this in mind, a fundamental point to realise from the outset is that the electronic cash embodied in a smart card, although it bares a superficial similarity to other forms of plastic payment card, is a very different concept from those types of cards which up till now have been carried around in our wallets. Credit cards, debit cards and cash machine cards all have one thing in common: they represent means by which a consumer can affect a transaction by instructing the financial institution that holds his or her account to effect a payment, either
to a third party merchant (in the case of credit and debit cards) and to the consumer himself (in the case of cash machine cards.) Regulatory regimes to cover these types of cards are well established, and the consumer can draw considerable comfort from the knowledge that the institutions which offer these products are appropriately controlled and regulated.

Electronic cash systems all represent novel methods of payment. The important thing to note is that they are not all the same. Many make use of a smart card based platform, while still others exist in a software form solely to effect payments across the Internet via personal computers. Mondex works the same way in the physical world as it does in the virtual world. Card based initiatives work by the consumer loading electronic value units, usually from a bank account denominated in the currency of the country. The value is then used just like physical money to make purchases at merchant outlets. Not only does the technical platform on which these cash products are based differ, they also differ in terms of the contractual and operational framework within which they operate. Some operate on the basis of full transaction clearing, in the same way as traditional banking systems. This means that when the electronic cash is loaded onto the consumer’s card and then spent at merchant outlets, each transaction is separately identifiable and is routed back to the financial institution to which payment should be directed. This means that there must be a full scale clearing system standing behind the network in order to affect settlement, and this naturally costs money. Many of these systems operate on some degree of truncation, in order to reduce the volume of transactional data that needs to be settled. Other systems, notably Mondex, focus on reducing the amount of data that is collected, and have developed contractual and operational structures designed to facilitate simplified settlement systems and to generate the economic benefits of low transaction costs.

Electronic cash systems are primarily aimed at providing a payment mechanism for low value transactions in the areas of the marketplace where traditional payment cards have failed to penetrate. This is usually because the commission the merchant pays to the bank is disproportionate to the value of the transaction involved. This cost arises largely from the need to set up clearing and settlement systems covering each transaction made by a consumer. There are, of course, many merchants that are unlikely ever to be able to accept payment cards that involve this cost. Examples are tobacconists, green grocers and bakers, as well as certain mass transit systems and car parks. If these merchants are going to accept any form of payment card, a way must be found for them to do so economically. This can only be achieved by reducing the amount of data that is captured by the system.
Electronic cash cards differ from traditional payment cards fundamentally in that the card itself, once loaded with electronic cash, has intrinsic value, just as if the consumer was holding bank notes and coins in his pocket. This, of course, means the consumer needs to exercise particular care in order to avoid losing the card. It is unlikely that the issuers of electronic cash cards will accept any contractual responsibility for the value loaded onto a card which is then lost. To assist the consumer, Mondex has provided an electronic locking facility on the card which means that the value on the card cannot be spent until a 4 digit personal identification number is keyed in by the consumer. If a card is lost and a fraudster could conceivably have access to the consumer's personal identification number and thus have the ability to load more value onto the card, then the position with electronic cash cards is exactly the same as currently exits with traditional payment cards. The same rules in terms of limitation of the consumer's liability should therefore apply.

These fundamental differences between electronic cash and traditional payment cards and the fact that the electronic cash initiatives vary in both operational and contractual framework, makes it very difficult to apply the existing regulatory framework and legal principles. It is possible to construct these systems in such a way that they do not become subject to any existing regulatory regime. These issues give rise to the question of whether it would be appropriate to expand the functions of existing financial services regulators or to create a new regulatory regime to cover this type of product, and perhaps other aspects of electronic commerce as they affect the consumer.

Three things are perhaps clear: First, the fundamental differences which exist between electronic cash cards and traditional payment cards mean that the principles which have evolved in relation to consumer protection as it relates to existing payment cards cannot be assumed to be appropriate or indeed desirable in relation to electronic cash. Second, international payment systems operate charge-back rights in certain circumstances. The introduction of such requirements in electronic cash schemes would not be operationally feasible, would add costs and would be inappropriate bearing in mind the cash nature of the products and the low value transactions at which they are basically aimed. Third, we are dealing with the rapidly evolving marketplace which means that premature regulation would be inappropriate as this will be likely to stifle commercial and technical developments which are fundamentally in the interests of the consumer.

Electronic cash initiatives and especially Mondex represent the move to a new paradigm in the financial services industry, and one from which the
consumer stands to benefit enormously in terms of convenience, flexibility, and security. It is imperative, therefore, that governments and industry tackle the issues with an open mind and are prepared to work together to find appropriate solutions to novel questions.
Panel 2 - VIRTUAL MONEY: CONSUMER PAYMENT OPTIONS

Summary of Questions and Answers

Following the presentations in Panel 2, discussion began with an inquiry about data collection and whether or not consumers are aware of the information that is collected online and if they have control over its use and dissemination. The panellists answered that they do collect personally identifiable information, primarily for payment purposes, but that this information is not used without the consumer’s consent. It was also noted that information involved in a SET transaction is encrypted in such a way that even the merchant cannot collect the card number used in the transaction.

A questioner then introduced the subject of premature regulation and legislation of electronic commerce, wondering how and when the time would be right for such action, and who should take the lead in examining these issues. The panellists suggested that no specific system of electronic commerce has been in place on a large enough scale to provide actual evidence about how they work and what problems might exist. It was also suggested that because of the global nature of the medium, there should be an international dialogue and a partnership between business and government to review the issues.

A question was then posed about privacy aspects of the payment systems and the prospects for anonymous forms of payment for goods and services in electronic commerce. In response, it was suggested that there should be a balance between the right of the consumer to his or her privacy and the need of the payment system administrator to monitor the process for security purposes.

Finally, a question was raised regarding the problems of consumer redress. The credit card industry pointed to the very detailed dispute resolution mechanisms they have in place which allow for consumer chargebacks. They expect these rules to extend to the Internet and will retool them if necessary.
Session II
CONSUMER PRIVACY AND DATA PROTECTION

Summary of Remarks

Chairman
Mr. William P. Fagan
Director, Office of Consumer Affairs, Ireland

Panel 1 - Cryptography

Speakers
Mr. Mads Bryde Andersen, Professor of Law, Institute of Legal Science, University of Copenhagen, Denmark
Mr. Amisha Marty, Bureau du Premier Ministre, Service Central de la Sécurité des Systèmes d’Information, France

Summary of Questions and Answers

Panel 2 - Protecting Transactional Data

Speakers
Mr. Simon Davies, Director, Privacy International, United Kingdom
Mr. H. Robert Wientzen, President and CEO, Direct Marketing Association, Inc., United States
Mr. Jacques Ribs, Commissioner, Commission Nationale de l’Informatique et des Libertés, France

Summary of Questions and Answers
Session II

CONSUMER PRIVACY AND DATA PROTECTION

William Fagan
Director, Office of Consumer Affairs, Ireland

The first question we wish to pose is that if privacy needs vary from consumer to consumer, and transaction type to transaction type, how can public policy best support this degree of flexibility without leaving consumers completely unprotected.

Next we will consider the question: "How can consumer requirements for access to encryption protection best be reconciled with reasonable law enforcement concerns?" The question of reconciling reasonable law enforcement concerns with other issues is, I think, one of the great balancing acts required. Here we are not just talking about consumer law, we are actually talking about other aspects of law enforcement.

For the second session, we will address two other issues. First, what steps should be taken to better educate consumers as regards their electronic commerce privacy threats, rights, and responsibilities. This is an issue not just about data protection as such, but about protecting the economic security as well as the privacy of consumers.

The final question is: “How can privacy and encryption policies function in the borderless global electronic marketplace and yet accommodate national differences?”
Panel 1 - CRYPTOGRAPHY

Summary of Remarks

Mads Bryde Andersen
Professor of Law, Institute of Legal Science
University of Copenhagen, Denmark

Basically, cryptography is about hiding what you say so that only the people you want to share a secret with understand what you are saying. It comes down to putting a new language on top of a language that you already speak so that only the person who knows this other language understands what you are saying.

Information is converted into other languages, by taking each and every part of your words and changing them to put in other words. One of the basic and best known cryptological ciphers for computers can be found in the movie 2001, where the main character is called Hal. Hal can be seen as an encrypted version of a well known computer manufacturer. In this instance, one letter is replaced with the next letter in the alphabet, so H will become I, A will become B and L will become M. So, if we in this room are the only ones who know that this is how we should interpret Hal, we have shared the encryption algorithm.

Current technology generates codes using sophisticated mathematical formulae or algorithms. In very basic terms, encryption involves multiplying two very large prime numbers together to generate an extremely large product - a process called factoring. Prime numbers are numbers that are indivisible by another whole number, and factoring a product is finding the two numbers that were originally multiplied. The larger the number of digits in the product to be factored, the more difficult it is to find the two primes that were multiplied.

A fundamental distinction can be made between types of encryption. The first is known as private key encryption. Using this method, two parties share the same key for encryption and decryption of the information passing
between them. Private key encryption is currently used to secure personal identification numbers and account information in credit card and ATM transactions. The second method is public key encryption. Here, each user has two keys -- one public and one private. The public key is used to encrypt messages that can only be decrypted by the person holding the private key. One person can encrypt a message to another person using each other’s public keys and each of them can decrypt the other’s message using his or her own private key. Public key encryption also allows each message to contain a “digital signature” that cannot be forged.

Encryption has the potential to take on a number of problems related to security and authenticity of information on the Internet which is crucial to build consumer confidence in electronic commerce. Without confidence in the system there will be no consumers and perhaps no market at all. These payment systems are extremely important, and equally important are the underlying encryption principles and the infrastructure that will support them.

Amisha Marty
Bureau du Premier Ministre, Service Central de la Sécurité des Systèmes d’Information, France

I represent the French Central Computer Security System which is generally in charge of the security of electronic communications and specifically in charge of the security of information and cryptography. Security is a key factor in the expansion of the information highway and in particular in electronic commerce.

The cryptography market can be freely developed to satisfy the needs of both the public and of business in the framework of national legislation. Such legislation can either seek to provide internal and external security or guarantee only a minimal amount of security to consumers. It is necessary to keep political principles separate from the practical uses of cryptography so that in the end we develop a system that includes both confidentiality and integrity.

Integrity, or the authentication of correspondents, will be the most important condition for the development of electronic commerce. It must be encouraged at the international level by actively promoting standardisation and by establishing the necessary supporting infrastructures. It is the role of
government to take all requisite measures to recognise the legal value of these authentication and numerical signature techniques. Their use should be as free as possible, however, countries must be able to ensure that it is impossible to circumvent the cryptography techniques.

Confidentiality is, in principal, related to three applications: the protection of privacy, the protection of intellectual property, and the protection of the industrial and commercial rights of individual countries. The protection of privacy and the respect for the secrecy of communications are usually granted through the constitutions of all democratic countries. Obligations concerning the protection of personal data are usually contained in the laws governing data processing.

The protection of intellectual property and the protection of the industrial and commercial rights of individual countries are necessary for the development of trade and of electronic commerce. Unlike privacy rights however, these protections are not constitutional provisions. Since these three types of protection have different objectives, they do not necessarily lead to identical technical and political solutions.

Since their common objective is to conceal information, all three types of protection incur the same risk: they endanger state security by depriving enforcement agencies of one of their means of investigation. A necessary equilibrium must be sought between the undeniable need to protect privacy and the safety of electronic commerce and the equally undeniable need for governments to fulfil their mission to apply the law.

Achieving this balance makes it necessary for governments to have control over the use of cryptography tools. Export controls for these tools can also be applied. One possible solution is to establish a central key authority which would keep users’ encryption keys in order to provide them if they are lost. These certified centres could also provide the same keys to government authorities in the event of an investigation, but only under strict legal controls and pre-established conditions. The centres would also have to abide by two specific legal commitments; the private legal contract signed with their subscribers, and meeting the conditions necessary for approval by their government.

Without directly engaging any direct government liability for the relations between these centres and their clients, government approval would contribute to their credibility. Through this approval, governments could make sure that the centres respect their obligation both to enforcement agencies and
to their subscribers. This would confirm both their technical capacity to fulfil their obligation to their clients and their legal and financial stability -- necessary to merit the confidence crucial to all parties involved. Banks, which are essential for electronic commerce, are by definition a type of third party confidence centre. The approach adopted for electronic card-based payments could be applied to electronic commerce in the widest sense.

In the same way that it was necessary to have international agreements between banks to execute international card transactions, international, or at least bilateral, recognition of these key authorities would certainly be necessary. Harmonisation of the necessary approval conditions would be highly desirable.

Since the task of maintaining public order is a strictly national one, the principles governing the operation of central key authorities must respect the organisation and the prerogatives of the country. Any technically acceptable solution must be based on governmental or private centres situated within national territory and inter-operating with the centres of other countries. In order to allow nationally deposited products to circulate across the world and to allow legal access to the keys deposited by another country, the depositing of encryption products on the territory of the country which exports them is not acceptable.

For products that respect the principles of cryptography, imports and exports should be facilitated. Respecting the confidentiality of information within electronic commerce and the need to safeguard a country’s vital interests is a delicate balance of two conflicting requirements. We think this balance has been found in the framework of the cryptography guidelines recently developed by the ICCP Committee in OECD.

It is clear that national security and freedom of global electronic commerce can only thrive with international rules which we should start working on as soon as possible. We think that OECD is the most appropriate forum to achieve this goal.
Panel 1 - CRYPTOGRAPHY

Summary of Questions and Answers

Following the presentations in Panel 2, discussion began with the question of key repositories and the level of secrecy and security they should be allowed to maintain. Despite the fact that certain communications are highly sensitive (for example trade secrets) should private parties be in a position to decide for themselves to keep certain information in complete confidence using encryption techniques, even avoiding government scrutiny? It was noted that today, communications are almost completely insecure (including the Internet, cellular phones, and traditional phone lines), and that anyone with the technological knowledge can access almost any electronic communication. Encryption and other technological solutions have the potential to minimise the threat of unauthorised access to information, however these technological solutions must be balanced with government and law enforcement concerns. It was noted that maintaining the essential requirements of strong and transparent law enforcement and judicial authorities can help assure private parties that government requests for access to encrypted communications would be prudent and fair.

Another question was raised regarding encryption, key repositories and key recovery initiatives in the global arena, and what body should be entrusted with coordinating the international efforts to deal with these issues. It was noted that divergent international rules and policies related to encryption have led to a very inconsistent regulatory framework. In response there was mention of a WTO initiative tasking the Council on Trade in Goods to analyse global trade procedures.
Panel 2 - PROTECTING TRANSACTIONAL DATA

Summary of Remarks

Simon Davies
Director, Privacy International, United Kingdom

Transactional privacy is an issue which remains embryonic. It fell upon me as the first speaker in this session to find a definition which, if you thought cryptography was a tough question, you should try defining transactional data. What I have concluded is that transactional data is the fact and a piece of a communication. The fact that I telephoned is a piece of the original transactional data.

As I see it, the fundamental difference between the telephone and the Internet is that the content of a telephone conversation was always subject to some sort of warrant, interceptor warrant, with judicial oversight. The content of the Internet communications, being highly interactive and being highly specific, in most countries is not subject to those provisions. Trade organisations and companies will insist that transactional data maintains its definition over the age regardless of the technology, privacy advocates suspect that they may be wrong. Transactional data is data relating to the fact of a communication, not the facts revealed by the communication. One of the points that I have concluded is that we need to fundamentally change our definition of transactional data.

We need to explore how transactional data is dealt with. In some cases organisations will disclose information that has been given to them only where there is some sort of individual consent for its disclosure. Others don’t have that guideline.

You can infer a great deal and deduce a great deal by merging different sources of data in complex ways. Since our discussion deals with developing bonds of trust between organisations and the public, I have a deep suspicion that somebody is going to have to set leadership in this area.
It is very hard to find a voluntary code of practice that actually has teeth, where there is an enforcement mechanism that works, and where there are penalties and some form of redress for the public. Unless we see some sort of change in the heart of industry, I think legislation is the only way to go, and I have a deep suspicion that prohibition of disclosure of transactional data may have to be the only option.

Technology can be introduced where the data is completely erased from the system once a confirmation has been secured. We’ve been arguing for long time as privacy advocates that privacy enhancing technologies and certainly cryptography, is the means to achieve a technology-led privacy protection regime, but it does require some sacrifice. I’m hoping that one of the things that comes out of our discussion is that some industry groups may be able to suggest ways where technology can be used to protect the privacy of individuals.

**H. Robert Wientzen**
President and CEO, Direct Marketing Association, Inc., United States

The Direct Marketing Association is the largest trade association for businesses interested in direct marketing and database marketing. The DMA represents more than 3,000 corporations and non-profit organisations in the United States as well as more than 500 organisations from 48 other nations. Our members use all media to reach their customers and prospective members. They use mail, telephone, direct response television, radio, and, increasingly, they are using and employing the new cyber media.

The rapid emergence of the cyber media is shrinking the global market place dramatically. Among its many applications, the new media will have a revolutionary impact on commerce between consumers and marketers. While new cyber media certainly have great potential for both consumers and marketers, they also are presenting marketers with challenges. Certainly, one of these challenges relates to consumers’ privacy concerns.

As you’ve already heard, some people are concerned about how marketers collect and use personal information. This, of course, is not a new issue. For a long time, consumer privacy as it relates to the traditional direct marketing media, such as advertising mail and telephone marketing, has been a
complex issue for the marketing industry. The DMA for many years now has endeavoured to address these concerns as they relate to the traditional media.

One reason consumers have made direct marketing a $1.2 trillion business in the United States is because marketers endeavour to understand who their customers are so that they can offer these customers the products and services that they want and need. One way we can do this is by looking at the customers’ past needs and wants as reflected in past transactions. However, we realise that the use of transactional information must meet consumer expectations of privacy. Not only do our customers want it to be protected, but since this transactional data is our most valuable business asset, we have a strong interest in protecting it as well. Therefore, it is to our benefit to honour our customers’ requests for how that information is used --even if that request is that this information not be used at all.

And, of course, this has never been more important as in this new cyber era since the Internet was not created with privacy foremost in mind. Indeed, due to the sophisticated capabilities of the cyber media -- such as the ability to track not only transactions but even browsing or “cyber window shopping,” if you will -- it is all the more reason for the direct marketing industry to serve our customers:

- By developing policies and technologies that are customer-friendly, and
- By helping to educate our customers and potential customers about how information flows on the Internet as well as our individual company privacy policies.

Technological advancements will certainly help address many of these consumer concerns. The DMA has become actively involved in development of what has been referred to as handshake technologies. As an example, this type of technology would require Webmasters to clarify the information practices of their sites. Consumers set their own individual privacy preferences and then the site’s privacy preferences and the consumer’s preferences would be electronically compared. If there is a mismatch between the site’s information practices and the consumers’ preferences, the consumer would be informed of the reason for the mismatch. Then, with this information, the consumer can make an educated choice whether he or she wishes to proceed with a visit to that site. We think most consumers would rather make their own choices concerning such matters, as opposed to having the government impose a one size fits all approach.
While new technologies will surely help address consumer cyber privacy concerns, marketers can -- and should -- be pro-active in addressing these concerns. The DMA has been a long-time champion of consumer choice in conjunction with industry self-regulation and peer review. Nearly 40 years ago, the DMA initiated a self-regulatory program for ethical business practices. The concepts at the very foundation of our self-regulatory principles are the following:

− To provide the consumer notice of the marketer’s information practices,
− To provide an opportunity for the consumer to opt-out of the process, and
− To respect and honour those consumers who do choose to opt-out through the employment of both the marketer’s own in-house suppress system and the DMA’s Mail Preference Service and Telephone Preference Service.

As we enter the cyber environment, the DMA believes that industry self-regulatory guidelines, consumer education, and applications of new consumer choice technology ensure a self-regulatory regime that is flexible and second to none in protecting consumer privacy in a global marketplace. We have also adopted new online marketing principles which were developed in 1996 in cooperation with the Interactive Services Association. These new guidelines relate to the appropriate notice and opt-out the consumers have an opportunity to engage in the interactive environment.

More specifically, our new principles urge online marketers to state their privacy policies on their Web sites. These policies should be presented in a manner that is easy to find, easy to understand, and should provide consumers an opportunity to opt-out of the marketing process. Moreover, the DMA’s online marketing principles urge that unsolicited e-mail advertisement be clearly identified as such and conform to the policies of the host forum.

Regarding the online marketing to children, it is the view of the DMA that a combination of industry self-regulation and current and developing technologies in consumer education initiatives can provide parents the tools necessary to guide their children’s online activities.

However, self-regulatory and technological safeguards notwithstanding, the DMA is not hesitant to acknowledge that children are a special audience. Reflecting this, our new online marketing guidelines further
encourage marketers to take into account the ages and sophistication of children when marketing to them or collecting information from them online. Also our guidelines urge marketers to provide a means by which parents can limit the collection of marketing data about their children -- and to honour the wishes of these parents.

In addition, because of the global nature of the marketing industry and of the cyber media, the DMA and 22 other direct marketing trade associations from six continents signed an agreement in October 1996 establishing an International Federation of Direct Marketing Associations.

Among other things, the signatories to the agreement have agreed to advance and adhere to a set of professional education, ethics, self-regulatory policies along with consumer education practices. The signatories have agreed to establish self-regulatory principles.

Jacques Ribs
Commissioner, Commission Nationale de l’Informatique et des Libertés, France

The problems surrounding the of protection of personal data are not entirely new. The Internet is simply a new medium that amplifies problems that already exist. The CNIL is an ‘independent administrative unit’ which authorises processing of information concerning personal data by government or any public body. The CNIL also assesses conformity with the laws and regulations, can issue warnings, and has the power to bring legal action if any provisions of criminal law have been violated.

The rapid development of electronic commerce today, creates a number of new problems including the 'de-materialisation' of the contract, jurisdictional questions resulting from the international nature of transactions, transactional security, and the protection of personal data.

Contrary to the impression Internet has initially created it is not a 'legal vacuum' but, in fact a medium that may end up with too many rules to be observed. This should inspire us all to undertake an effort to harmonise these rules in the interest of creating a safe legal environment for everyone on the Internet, for those on the supply side as well as those on the 'receiving' end. It seems fair to say that creating this legislative security will be as important as
developing the technical security necessary to fully develop this exceptional tool. The Internet will only grow if it provides a positive response to the questions concerning the protection of personal data of consumers.

What are our legal instruments in France and in Europe? We are not starting from zero. A reasonable body of regulatory provisions currently exist, particularly in Member states of the European Union. The French system, which applies entirely to the Internet, is based first on the idea of 'fairness' in the collection of personally identifiable information. Which means that individuals must be informed about the data being collected on them. This must either be directly communicated to the individuals concerned or they must be automatically notified using existing technology that does not require any action by the user. In this respect, the use of 'cookies' which allow an individual’s online activity to be tracked (usually without that person’s knowledge or the ability to stop or escape the practice) poses a serious problem. However, in a welcome move, two of the largest browser software providers, Netscape and Microsoft, have developed technological solutions to counteract this type of data collection.

The second principle relates to the ultimate use of the data being collected. The information should not be used for purposes other than those expressed to the individual providing the information. This implies that the consumer should be kept informed of any and all use to be made of the data collected. The use of a payment card, for example, allows a site to establish a user profile without that individual’s knowledge. By connecting files containing address lists, specific purchase information, and other personally identifiable information, site operators can create a wealth of data without the users' knowledge. An online purchaser may want to stipulate that the information necessary to make such a purchase cannot be used to establish this type of user profile.

The third principle in our national law is the right to oppose the transfer of personal data. The user has the right to be informed of all recipients and uses of the transactional data that has been collected in connection with his purchase, and must be given the opportunity to object to any transmission of the data he has provided to any third party. Using technical solutions to control the type and amount of information available about a user, in either a general manner or on a case by case basis, is a welcome development.

In 1981, the Council of Europe adopted a Convention which deals with the principles of data collection including: the use of data solely for the
express purpose for which it has been collected, improved technical protection for sensitive data, and the right of an individual to access and correct his or her own personal data. At the time of its adoption, the Internet did not exist. However, the Convention provides specific provisions concerning transborder data flow, both between signatory countries and non-member countries. In the latter case, each signatory country can contest the transfer of data to countries where there is no data protection equivalent to that granted by the Convention.

There is also a European Directive from October 1995 which addresses the protection and free flow of personal data. This Directive includes most of the above principles and includes two notable differences. First, it adds a requirement to control the efficient application of these principles by obliging Member states to create an independent data protection authority which can be directly referred to by any individual.

Second, is the principle that international data transfer is only authorised if the country of destination ensures a level of data protection which is equivalent to that ensured by European rules. In this respect, the Directive constitutes a powerful instrument towards the harmonisation of data protection, a fact which should be particularly useful in connection with the development of electronic commerce.

Inspired by the G7 of 1995, the White House document for the G7 meeting of 1997 entitled 'A Framework for Global Electronic Commerce' marks a decisive step towards international co-operation in this field. It confirms the need to define a transparent and harmonised legal environment in the area of privacy protection, and advocates the creation of simple redress mechanisms. While this clear statement is highly commendable, one should also bear in mind that the status of the user of electronic commerce should not be reduced to that of 'consumer' only. The consumer is also a citizen who has a number of rights which are guaranteed by data and privacy protection laws in a more general way.

On this particular point the White House paper refers to a number of fundamental rights which we, in Europe, have been familiar with for several years. These particular rights concerning the computerised processing of personal data can be ensured today not only by judicial means, but also by appropriate technical solutions developed by software and service providers in response to pressure from users. Data protection authorities should support these efforts and have, in fact, done that by supporting the development of voluntary rules undertaken in the field of direct marketing. Past experience --
and in France this includes in particular the Minitel and the Smart Card -- has already prepared the groundwork for developing not only regulatory solutions, but technical ones as well when the parties involved work closely together.

A second interesting point emerging from the White House paper is that it advocates the development of simple redress mechanisms. Such mechanisms could, in our opinion, be developed relatively easily as soon as we have defined clear and harmonised rules.

There are different ways to achieve a global framework for electronic commerce, either through voluntary guidelines or by bilateral agreements. But I think -- and here I am not speaking on behalf of the French government but as a technician -- that if we want to offer real security to users, be they merchants or consumers, the most efficient and operational way to do so would be by developing an international convention. After having developed recommendations of a mostly 'ethical' character but without any compelling force, we should work on a worldwide convention based upon the essential principles already defined by the EU and the White House paper.

It would be equally important to develop mechanisms for international co-operation. This could be facilitated if all countries involved create offices specifically responsible for data and privacy protection. It is important to avoid having geographic areas where no such protection exists, which would become just like tax havens -- havens of non-protection for data and privacy.

The developments to date should make us rather optimistic, and it will be interesting in the years to come to follow the development and application in practice of this work based on a global consensus which should eventually emerge. Applying these new structures will certainly be difficult. However, if the Internet continues to evolve quickly, those who seek to develop a framework for this new media must move quickly as well.
Panel 2 - PROTECTING TRANSACTIONAL DATA

Summary of Questions and Answers

Following the presentations in Panel 2 discussion began with a look at the amount and type of information revealed by Internet browsers with and without the users’ consent. Technologies are in use today that allow enormous amounts of data to be collected without the users’ knowledge or consent (using “cookies” and “click stream analysis”). This data can then be merged with other information to create a very specific user profile. Information can be captured about your location, the types of hardware and software you are using and where you have been and where you will next “travel” on the net. Certain companies exist whose sole purpose is to collect this type of information and sell that information for targeted marketing purposes. Technologies also exist to alert and block this type of data collection and set their preferences as to the amount of information that can be divulged and the use of that information.

The discussion then moved to the question of whether or not a consumer (or anyone else) could have access to the information that is collected. The direct marketing representative stated that as long as there is full disclosure of a site’s policy with respect to data collection and use it would be an unnecessary burden on the system to enable consumers to access that database whenever they choose. The European consumer representative stated the contrary belief that with the new growth of processing power and data collection capabilities it should be a consumer’s right to see, correct and even delete the information if proper and necessary. It was also noted that in the United States there is no requirement that an individual have access to data collected about them -- with the exception of credit data when credit has been denied.

A question was then posed regarding the collection of data relative to children and how much information can and is collected about them as they use the Internet. The direct marketing representative noted his association’s strong directives to its members that, within reasonable boundaries, they make every effort possible to determine the age of the child and only to collect data if they are comfortable that parents are aware of such collection efforts. There was also mention made of the support in both the United States and Europe that some effort needs to be made to protect vulnerable populations such as children.
Session III

JURISDICTION IN CYBERSPACE: WHO PROTECTS CONSUMERS?

Summary of Remarks

Chairman

Mr. Pierre Gabrié
Chief of Consumer Affairs and Security Department, Directorate General for Competition, Consumer Affairs and Fraud Repression, France

Panel 1 - The Role of Business and Government in International Consumer Protection

Speakers

Ms. Christine Varney, Commissioner, Federal Trade Commission, United States
Mr. Dan L. Burk, Professor of Law, Seton Hall University, United States
Ms. Glee Harrah Cady, Manager Public Policy, NetCom, United States
Mr. Jim Murray, Director, European Consumers’ Organisation, Brussels
Mr. Atsushi Niimura, General Manager, Multimedia Business Department, JCB, Japan

Summary of Questions and Answers

Panel 2 - Protecting Consumers from Cross-Border Fraud and Misleading Conduct

Speakers

Mr. François Benveniste, Director General, Calvacom, France
Mr. John Rothchild, Federal Trade Commission, United States
Mr. Christian Huard, Secretary General, Association de l’Education et d’Information du Consommateur de la Fédération de l’Education Nationale, France

Mr. Tadahiko Fukuhara, Professor of Law, Chuo University, Japan

Panel 3 - Unsafe and Defective Merchandise: Product Liability Protection in the Global Marketplace

Speakers
Mr. Edward A. Cavazos, Senior Vice President, General Counsel, Interliant, Inc., United States

Mr. Jeffrey B. Ritter, Program Director, ECLIPS, Ohio Supercomputer Center, United States

Summary of Questions and Answers
Session III

JURISDICTION IN CYBERSPACE: WHO PROTECTS CONSUMERS?

Pierre Gabrié
Chief of Consumer Affairs and Security Department
Directorate General for Competition, Consumer Affairs and Fraud Repression, France

Yesterday’s discussion centred on the potential benefits for consumers of electronic commerce. Today we will examine who can protect consumers against its risks. The requirements of quality, truthful commercial information are not new, but we cannot deal with these questions without involving the major player in this field, the consumer. He should not only be someone who reads the label and is a target for the marketing efforts of business. He should actively participate, together with the business side, in the efforts to improve the quality of this information.

The development of virtual shopping on the Internet gives these requirements a new and fundamental importance. The undeniable benefits for consumers that come along with the widening of consumer choice and with increased competition should not be compromised by a growing insecurity in this field. Current OECD work in the area of electronic commerce is therefore of crucial importance. How can we provide security in a global market if the monitoring of markets is still in the hands of national authorities? The answer is increased co-operation, the creation of notification systems, mutual information and harmonisation of rules and solutions to the up-coming problems. I do not want to advocate the introduction of new regulations, but I do want to stress that we can rely on already existing structures of co-operation. The International Marketing Surveillance Network which functions between OECD Member countries in an efficient and informal way is a good example of co-operation between the OECD enforcement authorities, which could be used in connection with the development of the Internet.
A number of countries are developing systems of self-regulation to eliminate misleading and fraudulent content from the Internet. This is the case in France, which, although not too advanced in this field, has started making this an area for serious reflection and have chosen to include consumer representatives right from the outset. The National Consumer Council, an institution which is composed of both business and consumer representatives is currently discussing in one of its working groups the problems of Internet access, including such questions as advance information of consumers, security and confidentiality problems and, in particular, the problem of proof of transactions and has issued an initial report of its findings.

Panel 1 - THE ROLE OF BUSINESS AND GOVERNMENT IN INTERNATIONAL CONSUMER PROTECTION

Summary of Remarks

Christine Varney
Commissioner, Federal Trade Commission, United States

I believe that, in general, government should regulate only when there has been an identifiable market failure or where an important public policy goal cannot be achieved without government intervention. My own view is that government should not regulate in the absence of a market failure. Yesterday the question was raised as to how and when will we know when the market fails -- in my view, you will tell us. Entrepreneurs, business people, and consumers, will let those of us in government know very quickly when the market is failing to provide adequate privacy and adequate protection against fraud.

The pace of change in the information industry is unprecedented. Government regulation, on the other hand, moves very slowly, and the predictive skills of government agencies are notoriously limited. As a result, regulatory and legislative solutions to consumer protection issues are unlikely
to be either timely or sufficiently flexible with respect to the digital world at this juncture.

There is a wide spectrum of views in the U.S. with respect to electronic privacy. Some advocate strong government regulation to protect consumers online. Others think that it is too early to regulate electronic privacy. Still others think that industry efforts to define the ethical use of consumer information can be transferred to the online context. All of these views are reasonable. In the end I believe the rapid pace of technological development limits the effectiveness of government regulation in this area. For that reason, I support industry self-regulatory efforts. I do, however, see a strong FTC role in encouraging industry self-regulation by convening and facilitating dialogues with business and industry, working to develop a market place for privacy protection, and prosecuting those engaged in unfair, fraudulent or deceptive practices.

One role that I believe government can serve is to educate. Our colleague from the United Kingdom yesterday pointed out that many people on the Internet are not susceptible to scams -- because they're smart, sophisticated people, they're not going to be taken in by fraud. However, we have found that the same “get rich quick” pyramid scams that exist in the terrestrial world can be found all over the Internet. The FTC has brought a number of enforcement actions against these types of scams and have posted a number of consumer education “tips” to help people to protect themselves against scams on the Internet.

I think government can also encourage technological solutions to consumer privacy concerns. The collection of data on the Internet is a widespread practice. Websites have the ability to collect information about who you are and what you’re doing without your knowledge or consent. Individual profiles can be automatically assembled combining clickstream data, demographic data, and information gathered directly from the http connection such as location, domain, and the type of computer and browser you use. This information can then be used to create databases or to deliver targeted content over the Net.

There are a number of promising technological solutions that afford consumers the opportunity to set their own privacy preferences. If you can have your personal privacy preferences downloaded onto your hard drive and into your browser, you can be warned if a site does not honour those preferences and than make a personal choice about whether or not to proceed.
If we create a marketplace for privacy, perhaps people will not go to sites that collect this kind of information without their knowledge or consent.

In this information age, privacy may become a market commodity. Given adequate levels of consumer and government awareness, the demand for privacy protection could continue to increase and a robust, competitive market for privacy protection could develop. Under this scenario, the market itself could serve the same function as a government privacy bureaucracy.

These assumptions lead me to the conclusion that the government ought to move cautiously in the electronic arena, and should initially focus its attention on supporting the growth of self-regulatory efforts and online education efforts. Internet commerce won't really take off until consumer confidence in the system is established, so it makes business sense for industry to invest in self-regulation and consumer education.

**Dan L. Burk**
Professor of Law, Seton Hall University, United States

Within electronic commerce, two very distinct types of transactions are beginning to emerge. The first is a transaction that culminates in the shipment of physical or tangible goods. The consumer may select and order and even pay for the goods online, but ultimately something tangible and solid is physically shipped to the consumer.

That is quite different from another type of transaction we are beginning to see on the Internet -- transactions involving digitised goods. Here the goods are not only selected, ordered and paid for electronically, but they are also delivered electronically through the network.

These two types of transactions are very different from a consumer protection perspective. By thinking about the types of goods consumers may want to purchase from an economic perspective, we can begin to understand these differences. Economists would call the first category of goods inspection goods. These are goods which the consumer can look at and determine for him or herself first hand whether they are of good quality and whether the they want to make the purchase. So you might think perhaps of some fruit or some meat in the grocery store where you can immediately tell by sight and by touch if it is of good quality.
The second category of goods would be called experience goods. The consumer cannot immediately tell if they are of good quality, he can only measure their worth by using the goods for some period of time. For example with an automobile, you need to drive it around for a while before you learn whether or not it was a good purchase.

The final category of goods consists of what economists call credence or reputational goods. These are goods which the consumer may never be able to tell whether he has purchased good quality product or not.

Consumer protection agencies and law enforcement agencies have a great deal of experience already in dealing with many of these situations from their experiences with mail order catalogues, telephone orders, and so on. Digital goods that can be delivered on the Internet, are an entirely new type of creature that are outside the previous experience of law enforcement officials and of governments. The Internet gives very few clues or hints as to the physical location of someone using the network. Therefore, when a consumer purchases digitised goods, such as software, a motion picture, a database or other types of informational goods, it is going to be extremely difficult to locate the source of those goods if there is a defect or fraud in the sale.

Because the network is geographically indeterminent, it will be hard to decide which government or which agency has jurisdictional authority in dealing with a problem. Similarly, conflicts of laws will arise in determining whether the law of the source of origination of the goods applies or the law of source of receipt. Government agencies that attempt to deal with defective or fraudulent goods of a digital nature and attempt to locate the source of these types of goods could stretch their resources beyond the limit.

In my view, it is extremely important for governments to create an environment on the Internet where transactions become self-enforcing. This is drawn from the economics of game theory in which an agreement that is self-enforcing is an agreement that you would not expect the parties to cheat on or defect from. Why? Because it's not in their benefit to do so. The best thing that governments can do for the Internet is to create an environment in which it is not to the advantage of businesses or consumers to cheat or defraud.

I am not necessarily advocating the creation of a business coalition or other types of self-governance model. I am suggesting we create a business environment in which natural market mechanisms lead to these types of self-enforcing systems, minimising the need for government agencies to expend their limited resources to police these types of transactions.
With regard to physical goods, we already know that trademarks are extremely important. By identifying for consumers the nature and source of physical goods, consumers come to rely upon the trademark or trade name as a repository of reputation that allows them to identify trusted businesses and services with whom they can chose to interact.

Digital certificates can allow consumers and businesses to verify in their online transactions that they are, in fact, who they purport to be. If I receive something that has been encrypted with the private key of a particular businesses cryptographic code, I am certain that it in fact came from the business that purports to have sent it to me.

It is extremely important that strong cryptography be put into the hands of businesses and consumers as soon as possible. Certain government polices have inhibited the release of strong cryptography tools into the marketplace, and we need to remove these barriers as soon as possible to enhance verification on the network.

I would also suggest that certification be enhanced and fostered by governments. The process of third party auditing and certification authorities becomes extremely important, even if the consumer does not know, and cannot personally ascertain the practices of a particular business. The consumer can trust the audit that was conducted by a trusted third party.

With a combination of these three steps, identification through trademarks, verification through cryptographic methods, and finally certification through third party audits, we can begin to create the type of digital environment in which law enforcement agencies will not need to police every transaction. If you think about it, that's the type of environment we enjoy in the physical world. Government agencies cannot oversee every transaction that occurs in the physical marketplace. We trust that most consumers and most businesses are honest and forthright in their dealings and we only require the government to step in and deal with marginal business transactions. We would like to create the same situation on the Internet where the majority of transactions will be self-enforcing, honest, and forthright and where we require only occasional government intervention.
Glee Harrah Cady  
Manager Public Policy, NetCom, United States

As we all think about the future of the Internet, I would like to give you some information from the point of view of those of us who carry the packets of information from one point to another. The company that I represent, Netcom Online Communication Services Incorporated (Netcom for short), is an international direct Internet services provider. The Internet Architectural Principles are the foundation upon which all of the technology works.

The first principle is the idea that connectivity is the goal. This is a way of saying that the value of the Internet is that everyone can be connected to each other so that we can communicate. That is the goal. It is not to sell things, or to buy things, the value is that we share this environment.

The second principle is actually the tool that is the Internet Protocol Suite. This is a series of technical standards and agreed upon communication methods which allow for interoperability. This means that the machine that I operate in San Jose, California can communicate with the machine that Mr. Leroux operates here in France without regard to the operating system, the time of day, the flavour of browser one uses or the choice of e-mail clients.

The third principle is that the network itself is not intelligent. Which means, in the example that I just gave, should I send a message via an e-mail program from my home computer to Mr. Leroux’s home computer, there is no need for any piece of the network that we may traverse to know where either of those points are, to know what that packet is about, or to have any idea of its contents.

The fourth principle is fact that technical change is constant. Many of our speakers here have discussed the reasons why we hesitate to recommend legislative and regulatory matters. Among those reasons is that by the time we finish legislating or regulating or agreeing upon which we were legislating or regulating, that condition no longer exists.

Internet service providers actually carry the packets from place to place. I’m going to speak specifically about the kinds of lines of business that my company is in because those are the ones with which I am most facile. The first is that we operate networks in the names of consumers, who connect to us via a telephone line and a modem. In our second line of business, we connect large servers and large companies. Third and finally, we are in the business of
hosting of data in the form of web gopher or FTP servers in the name of our clients.

With that in mind, we have to think about what is our position in the world as a whole. That is, what do we do besides route packets? At this point in the development of the Internet, part of our charge as a business, is to educate. First, we educate ourselves, and I say that because we have a number of employees, and it’s important for them to understand the privacy needs of the data that we have about our customer set.

Secondly, we have the duty to educate our customers. We try and do that via our website, via letters to the customers, we do it with links to government education messages and we do it with links and messages about parental control software. We encourage our users to define and become comfortable with their own environment.

We also attempt to educate our suppliers. Interestingly enough, not all of the people from whom we purchase services actually understand the business that we are in or the necessity to keep information about our customers private. In this way, we can ensure that in cases where we are licensing connections to particular websites, those websites are aware of the privacy rules that protect our customers.

We also take the time to educate our elected, appointed and regulatory officials of local, state, regional, and federal organisations, to help them understand the technology upon which it is based.

Finally, we work with law enforcement personnel. We do this because we have a large community of users, and not all of them are good people. While we are not regulated in the sense that there are strict rules for how to be an Internet service provider, we are in fact both good citizens and citizens of the geographical areas in which we operate.

In our efforts educate and keep everyone informed, we address ourselves to four pivotal issues which we think of as the Four P’s. The first of those is parental empowerment, that is the ability to define the environment in which you operate if you are a parent and worried about your children. The second is intellectual property, third is privacy, and the fourth is consumer protection. We believe that education is essential to the growth, utility and the future of the Internet.
Jim Murray  
Director, European Consumers' Organisation, Brussels

I am here on behalf of my member organisations, which are the independent organisations from twenty European countries, including the members of the European Union and European Economic Area.

Could I stress, I am not going to talk at all about illegal content. We are all against frauds and scams and child pornography, but on issues of marketing practices and consumer protection, there is a difference about how much protection and privacy there should be, or what kind of rules should apply.

We really have two questions: who applies the rules and what rules are applied on the Internet? I say rules, by the way, not necessarily to mean laws, but simply rules which may be applied by government, they may be applied by international authorities, they may be applied by industry, they may be indeed applied by consumers in a self-enforcing way. However, consumers can only enforce rules when they know what’s happening. I can only refuse to give information about myself when I know I am giving information about myself. If I don’t know what information is being taken, through my browser or from my computer, clearly I can’t enforce any rules about it because I simply don’t know what’s going on.

The second question is what rules should we apply? Should they be the French rules, or the EU rules now applying to most countries in Western Europe? Should they be the American rules or should they be some WTO or OECD rules?

Electronic commerce is distance selling, and we must look to the principles which we have worked out in relation to distance selling and see how they may be applied to the Internet. Governments must be prepared to take responsibility not only for their own consumers, but for consumers in other countries with respect to electronic communication. For example, the government in Ireland, must be prepared to take responsibility for advertisements which flow out from Ireland to other countries around the world. That may sound simple but in fact in many countries it's a principle which is not well embedded in law. Laws tend to protect domestic consumers and sometimes take a rather lighter attitude towards messages which are, in effect, exported. So governments must be prepared to take responsibility for what happens on their own territory even if the message ends up with consumers elsewhere.
We also need to develop a much more sophisticated understanding of the principles of home country and host country control. Home country being the country of origin, and host country being the country where the consumer receives the final message. This is particularly important, for example, within the EU where the idea that receiving countries should be able to exert some control is given practical expression in the treaty under the principle of minimum harmonisation.

I think common rules in this area can be helpful, but they're not the complete answer. First, very few countries would be prepared to accept only those rules that can be agreed through a large number of broad international fora. Secondly, even common rules oddly may not work, unless the problems of cross-border transactions are reviewed as well. If you have two countries, each with common rules, and even with identical rules, there may still be a problem when the transaction is cross-border due to lack of cooperation, problems with jurisdiction, or problems with the enforcement of judgements cross-border.

Much of the discussion on electronic commerce on the Internet tends to focus, I think too narrowly, on the current technology. I think we need to look at what shape the market will be, in terms of concentration for example.

I think it is reasonable to ask and to expect companies doing business on the Internet to respect and to integrate into their normal business practices the standards and the norms which we have already developed and those that we expect to see in the future. A great deal can be done if we are prepared to do it and firm enough to demand it.

Atsushi Niimura
General Manager, Multimedia Business Department, JCB, Japan

I am responsible for establishing and implementing strategies on electronic commerce, smart cards, and the use of information technology to enhance our service and competitiveness.

I believe that the development of the Internet and electronic commerce will reduce the potential for unfair or deceiving commercial conduct which are commonplace in the terrestrial world. I think the Internet is now playing a vital role in reducing information asymmetry. Uninformed
consumers and the lack of balance with respect to information is one of the primary causes of consumer harm. Although many of you might think my argument is too naive, it seems to me that the growth of the Internet and the combined efforts of consumers, businesses, and governments as we look to build and fully utilise the new medium, is proving that the Internet can make the global marketplace more efficient and fair. I would like to address the topic of international consumer protection from my position as a credit card company.

Today the JCB card is held by 35 million card members and accepted at 4.4 million merchants in 160 countries around the world. While the goal of the JCB card is to provide the highest quality service, the basic function of the JCB brand is, in short, to provide our customers with a secure and convenient payment system. Thus, JCB is dedicated to focusing on customer service while working towards being the most functional payment system available.

By functional I mean that JCB can be used at any time and in any place for any purpose. By utilising the most recent technologies, we have now concretely envisioned the multifunctional “dream card.” By having this one dream card you will be able to save, spend, and invest your money very easily. Furthermore, your dream card can serve as your personal I.D., your data base, and your communication device. It's like you have your PC, cell phone, ATM, investment consultant in your wallet.

I will not go into the details of technological background of the dream card, I would instead like to emphasise that the difference between virtual and real world will mean very little soon because technology is nourished in the field of the Internet. Those of us who are dedicated to smart card technology are now looking towards the integration to a single card system. This development will, I think, blur the boundaries between the virtual and the real world. People will use the card in both arenas and will not pay attention to the technologies that make the card work.

In order to ensure a level playing field and unobstructed competition in the marketplace, some type of a common platform must be agreed upon by the major participants. Speaking from the perspective of a card company, this means that financial institutions and organisations related to the financial industry need to cooperate to ensure interoperability for the sake of the consumer.

One example of such cooperation that I am sure you are all familiar with is the discussion surrounding SET. This protocol was first proposed and
agreed upon by VISA and MasterCard, then opened for discussion before being finalised. This free and open environment, which excluded no one, is a sign of what we can achieve through cooperation in the realm of electronic commerce as well as providing a clear example of the potential for free competition.

Competition is the most reliable guarantee to protect customer's rights. Cooperation at various levels is very necessary and I believe that government's role in providing consumer protection is to first ensure free competition. Within JCB, without any laws or regulations we are very committed to serving our customers, and that is our full commitment to protect our consumers.
Panel 1 - THE ROLE OF BUSINESS AND GOVERNMENT IN INTERNATIONAL CONSUMER PROTECTION

Summary of Questions and Answers

Following the presentations by the first panel, discussion began with the issue of international law enforcement cooperation and the possibility that the Internet itself could serve as a tool in combating cross-boarder crime. An example was made of an FTC Internet mailing list connecting law enforcement personnel in the United States and Canada through which information can be easily shared between the two jurisdictions.

A question was raised about the United States view that market forces should lead the way in dealing with Internet privacy issues rather than joining in European efforts to seek a common data protection regime. Ms. Varney responded that there is a wide range of opinion in the U.S. on privacy and that some U.S. privacy advocates do support stronger government policies, noting, however, the government’s reluctance to conclude that a legislative solution is necessary at this time and the preference to see if market solutions will work. From the European perspective, Mr. Murray pointed out that European nations must adhere to and respect the privacy standards that have been set forth and asserted that consumers should always have the possibility to access the information that is being collected and held about them. The importance of compliance with existing advertising rules and standards was also mentioned.

A question was asked about the existence of technological impediments to allowing consumers to “opt-in” to data collection plans rather than having them “opt-out”. In response, it was noted that there are many different types of services and providers on the Internet. Not all of these services have a mechanism that would allow a message to go out to consumers notifying them when data collection is taking place (specifically telnet and newsgroup services).

A question was raised about the notion of self-control mechanisms and how they might be reconciled in such a rapidly expanding market. Mr. Burk replied that the reliance upon market forces in an area of explosive growth may require some limited regulation and government cooperation. But if the correct environment were created for that type of growth, the growth itself will fuel the self-enforcing mechanisms with only limited government involvement.
Panel 2 - PROTECTING CONSUMERS FROM CROSS-BORDER FRAUD AND MISLEADING CONDUCT

Summary of Remarks

François Benveniste
Director General, Calvacom, France

I realise that this is a an international forum, but I would like to dwell on a number of specifically French problems which, I believe, will also be relevant to the development of other national electronic commerce markets, including some that are developing faster than the French market.

I would like to discuss the security of transactions on the Internet and I will focus on two themes: In order to ensure transactional security on the Internet we first need a secure environment for business. If that does not exist, the business community will not make the necessary investment in electronic commerce that is critical for it to develop into a well structured environment for the Internet community as a whole. If we begin with a strong and secure environment for the Internet operators, we can simultaneously develop measures to ensure the security of users of the network.

On my first point, security measures for operators (and by that I refer to access providers, commercial or non-commercial information providers, and producers of web sites,) the French Association of Internet Professionals (AFPI) has been asking for some time for a special and clear statute for service providers -- a statute not based on self-regulation. We think that this is an emerging market, one in which the economic conditions are highly fragmented and where a variety of economic factors are very important. We also expect it will become increasingly similar to traditional markets with a number of service providers working for a large number of customers. We do not believe that there is enough common vision amongst everyone involved in the electronic marketplace and that the idea of having these fragmented interests freely agree upon certain rules is not a realistic possibility.
We think that French legislation includes provisions that would be sufficient to regulate the activities of Internet service providers. But the government has to state in a clear, unambiguous and precise manner how existing law should be interpreted with regard to these new technologies. We need a legal framework and perhaps even an institution -- appointed first on a national level and later on an international level -- whose job it is to pinpoint dubious practices on the Internet, be they cultural or commercial. We should not count on the network operators to create these structures.

Regarding security, the primary objective of Internet professionals is the simple idea that they are not presumed to be 'liable' for the information that circulates on the Net. French press law presumes that in the press, the editor of a journal, a radio or television station is liable for outgoing information. In our view, this cannot be applied to Internet service providers. The Internet is not a new type of broadcasting, a new type of television, it is not literally 'controlled' by a person or a group of people who can be held directly liable for what they are doing. The Internet represents a mass of actors, a mirror of real life and, therefore, the principle of presumed innocence should be applied until proof is shown to the contrary.

We have developed a number of principles regarding individual security on the Internet. The first is information. We have to be aware of the fact that 90 percent of the users who join the Internet do not understand the cultural and technical environment they have entered and the need for continuously updated information. Internet providers, to the extent that they themselves interact in a secure environment, can fulfil this need by providing on-line information, CD-roms and brochures, making their users aware of the problems and limits of Internet security in general and more specific problems related to transactional security.

Much has been said about the danger of credit card numbers left floating on the Net. However, the statistical risk of someone using your payment card on the Net is smaller than the risk you take in the current payment system, so that with time this should not be a major preoccupation. But sellers have a right to know with certainty the identity of their customers just as consumers have the right to know with certainty the identity of the seller. Consumers should also have the ability to seek redress if the goods or services delivered do not match their expectations.

The challenge of the Internet is a challenge of global harmonisation. We, in France, think that this will not be easy. But now is the time to begin.
According to data collected by the National Fraud Information Centre for 1996, Internet pyramid schemes are the single largest category of fraud on the Internet. They are inherently transnational in scope, as all offerings on the Internet are, and as we have seen recently, they are particularly devastating for new market economies that don't have experience with this sort of problem.

The essential characteristic of a pyramid scheme is that it involves participants paying for the right to earn commissions by recruiting new members into the pyramid, and it is destined ultimately to result in losses to the great majority of the participants. The Federal Trade Commission has brought several traditional law enforcement actions against pyramid schemes on the Internet in the past year.

Although we have had some success in shutting down these schemes and getting money back for consumers with these law enforcement actions, we felt this was not the full solution. Pyramid schemes are proliferating at such a rapid pace that it is impossible for us to sue enough of them to make a difference. In addition, these schemes can grow to their full extent and collapse before we are able to do the work to bring a law enforcement action. So we devised a supplemental approach which we called Internet Pyramid Surf Day. This was a designated day in December of last year in which investigators both at the FTC and at other law enforcement agencies on the federal and state level in the United States went on the Internet during a designated three-hour period and looked for pyramid schemes on the Internet.

A couple of days later, we sent out an e-mail message to each of the sites we found that looked like it offered an illegal pyramid scheme. It was what we think of as an educational message. I'll read part of it.

"If you do business in the U.S., you may be interested to know that pyramid schemes are illegal. Businesses can use multi-level marketing networks to sell products to the general public; however, under many U.S. federal and state laws, it is illegal to offer a program that promises profits merely by recruiting new participants."

The message goes on to say that "the FTC and its federal and state law enforcement partners are sending you this message based on a review of your Internet solicitation. We have not determined whether your solicitation
constitutes an illegal pyramid scheme. However, we have copied and preserved your solicitation for future reference."

So, in addition to the educational message, there is a little bit of a veiled threat that enforcement action could be forthcoming if the activity continues.

As a result of the Internet Surf Day we identified more than 500 sites that fit our criteria and that seemed to be illegal schemes, and we sent e-mail messages to these sites. A month later, we went back and looked at these sites to see what the effect was of sending out this educational message. We found that about 18 per cent of them had improved their site, by either taking it down or modifying it so that it was closer to being in compliance.

This model of cooperation among federal and state law enforcement for this educational purpose is a model that could be replicated easily on the international level and is one example of the sort of interjurisdictional cooperation that we need in dealing with fraud on the Internet.

Christian Huard
Secretary General, Association de l’Education et d’Information du Consommateurs de la Fédération de l’Education Nationale, France

I am in charge of a French consumer organisation and of the work on electronic commerce led within the French National Consumer Council. Contrary to much of what we have heard so far, I believe that electronic commerce needs more than merely a few regulatory provisions in order to develop and work well for consumers. Consumer organisations do not oppose the development of these new technologies. Quite the opposite, we support them but view them with caution as we continue to have reservations about their ability to fully benefit consumers without first solving a number of problems.

The problems we foresee that are most likely to be of concern to the OECD are those that arise in connection with transborder business to consumer transactions. It is interesting to note that despite more than 50 consumer protection directives, various communications and campaigns, and the current efforts to create a single European market, transborder business to consumer transactions remain a relatively marginal phenomenon. This single market has,
thus far, proven to be a market primarily for business to business transactions. In my opinion, the lack of redress mechanisms in cases of fraud or any other type of unsatisfactory contract execution is the primary contributing factor. Consequently, one of our biggest challenges today is to develop a directive allowing consumer organisations and individual consumers access to justice in other countries around the world. I believe we not only need a single European market, but a single European legal structure. Until significant progress has been made in this area, we will not make any real progress in opening up transborder distant selling to individual consumers.

Electronic commerce is not entirely new. In France we have more than ten years experience with Minitel, a national structure for electronic commerce based on an Interactive Videotex System that also includes payment facilities. These electronic consumer to business transactions have grown because the consumer protection provisions we have in place are superior to those offered in any other form of retailing. However, electronic commerce has not yet fully replaced any other form of distribution, it has simply become a complementary option for marketing certain types of goods and services.

The experience of consumer organisations, both in France and elsewhere, shows many problems arise in areas such as unfair contract terms, deficient products, and deficiencies in contract execution. So the real problem is to clarify and harmonise contract terms. As we do that, we must consider the types of consumer protection provisions that would be included in any international contract regulations. Some questions to be considered include: redress mechanisms, “cooling-off” periods, and determining what actually constitutes the execution of a contract in this virtual environment.

Language barriers also pose a problem in the distribution of information and the execution contracts in this electronic environment. What will consumer information really mean, if a contract is made in a language which the consumer does not fully understand?

My conclusion is that we cannot adequately protect consumers through self-regulation. We favour the expansion of electronic commerce in France if it proves beneficial to consumers. However, but should it become an instrument aimed at dismantling our national or international arsenal of consumer protection devices we would have to reconsider our support.
We need to keep in mind and consider the steps that need to be taken to protect consumer rights in this new global electronic marketplace just as well as we do in the real world. I would first like to address the characteristics of consumer damage suffered from fraud and misleading conduct in the global electronic marketplace. Second, what can be done to prevent consumer injury and recover damages in this new market environment. And finally, the consumer law of cyberspace, and how it should be moulded. My goal is to point out the difficulties involved in attempts to recover of consumer loss and damage in the electronic marketplace and to give some clues to help us overcome some of these difficulties.

There are a number of novel characteristics found in the types of damage from fraud and misleading conduct facing consumers in the new global electronic marketplace. First, while the amount of damage might be small for each consumer, the sum of the damage can be enormous. Second, fraudulent suppliers using the World Wide Web are often unidentified. Third, fraudulent suppliers may abuse technologies to make consumers misunderstand their products. Finally, consumer damage occurs very widely, potentially throughout the world. As a result, a consumer can meet with great difficulty in attempting to recover damages.

Both technology and the international nature of these electronic transactions have an affect on these characteristics. The international nature of these transactions brings consumers more difficulties than the technological factors I think. Needless to say, the application of damage recovery is an important aspect of consumer protection. In the global electronic marketplace, consumers must be provided with useful information about transactions in order to avoid fraud and misleading conduct. Such information could be provided by some reliable website produced in cooperation by both consumers and businesses.

Consumer remedies can be achieved in the global electronic marketplace. In accordance with the basic principle of consumer remedy, consumer damage should be recovered promptly and thoroughly through simple processes. As we consider this principle, we must again bring to mind the first characteristics of consumer damage. In these instances, a legal system, such as small claims court or class action consumer suit could be useful. However, here, the international nature of the transaction is likely to cause a
number of additional problems. If the parties involved in an international transaction consent to resolve their dispute, they are then met with problems in the area of conflict of laws such as the choice of forum, the location of the court and choice of law.

The mandatory rules included in the doctrine of forum convenience bring more difficult issues to bear in international transaction disputes and the argument of international jurisdiction arbitration is often used. However, I believe that in consumer contracts, the parties should be prohibited from choosing laws and choosing jurisdictions. Perhaps it would be best for the parties to resolve these disputes through international arbitration. In fact, in international commercial transactions, international arbitration has been used frequently all over the world and has recently been adopted as a model form of law. It may be useful for us to create a similar model law and use it to resolve disputes in the global electronic marketplace.

Regarding the need to establish an entirely new legal system beyond the existing jurisdiction to overcome these difficulties, there are a variety of opinions on the subject. One opinion presents the idea of cybercourts or cyberjurisdictions distinguished and separate from existing jurisdiction. I would like to find a feasible legal scheme, overseeing the conduct of participants in the global electronic marketplace that is based on contracts rather than on restorative consideration. I would also like to see the participants in the global electronic marketplace take this opportunity to develop their own code of conduct -- either within individual companies or as part of the Internet community as a whole -- rather than ceding that responsibility to some outside entity.
Panel 2 - PROTECTING CONSUMERS FROM CROSS-BORDER FRAUD AND MISLEADING CONDUCT

Summary of Questions and Answers

Following the panel presentations in Panel 2, a statement was made regarding the impact the Internet may have on global trade and how best to manage its effect. Noting that while harmonisation of regulations is unlikely, the harmonisation of technical standards is a distinct possibility.

A statement was made regarding the importance of the role of the contract in facilitating the development of best business practices which has been a driving force in allowing the implementation of technology to achieve efficiency in the use of electronic commerce for trade. Noting that the contract as a tool for solving legal issues and working around legal uncertainties has a proven record of success. It was also suggested that a possible role for regulators would be in partnering to develop codes of conduct, model agreements and other tools that could be useful in resolving legal uncertainties.

In one commentor’s view, if industry develops sanctions within its codes of conduct, the ability to enforce those sanctions and makes the sanctions of sufficient substance government regulation would be unnecessary. But only if those sanctions work across borders and are more efficient and effective for protecting the interests of consumers could they defer intergovernmental actions.

One response noted that self-enforcement and codes of conduct are good mechanisms and do not require government intervention when you have actors in the marketplace who are concerned about their reputation. However, these self-policing devices are ineffective in dealing with people whose only interest is in deception and fraud. One approach that provides a role for government is consumer education and enabling consumers to protect themselves and identify frauds before they fall for them.

Discussion concluded with the comment that, in the interest of promoting and encouraging a truthful electronic medium that can build consumer confidence, advertisers and governments should work together to discourage fraud and misleading information on the Internet.
Panel 3 - UNSAFE OR DEFECTIVE MERCHANDISE: PRODUCT LIABILITY PROTECTION IN THE GLOBAL MARKETPLACE

Summary of Remarks

Edward A. Cavazos
Senior Vice President, General Counsel, Interliant, Inc., United States

Sometimes, people who produce products that enter the stream of electronic commerce do not have the intent to cause harm, but we can imagine that their products will, nonetheless, do just that. Should consumers who are harmed in that way have a set of remedies available to them? The answer to this question is, I think, yes, and it can be found by examining product liability laws.

Product liability law is a distinct body of law that is different from conventional models. In the United States, as in most jurisdictions, its most distinguishing characteristic is that it is a strict liability doctrine. This means that the focus is not on whether the defendant responsible for the harmful product had the intent to harm the consumer, but rather whether or not the defendant’s product actually caused consumer harm; there is no malice required. If the defendant is making money on the product, says the doctrine, they should be held responsible should the product hurt someone.

A product liability claim must satisfy several elements that, if met, give rise to a successful cause of action. The first, of course, is that the product must be defective. The defect must also make the product unreasonably dangerous to the consumer. The product must reach the consumer in substantially the same form as when it was sold. (It is not fair to hold the defendant responsible should the product be changed somewhere in the stream of commerce.) Finally, it’s not enough just to identify a defect in a product, it must actually hurt someone in order for that person to be able to recover damages.
The first element, then, is whether or not the product is defective. I think this point raises some very interesting questions. For instance, what constitutes a product in the online world? It’s extremely important, early in the discussion of any product liability policy for electronic commerce, to make some determinations as to what qualifies as a product, and what qualifies as a service, or non-product.

Once you have crossed that hurdle, you come to the next question: what is a defect in a product? As a general rule, there are three types of potential defects. One is a design defect which occurs where a reasonable and feasible alternative safe design existed at the time of manufacture, but the manufacturer chose not to use it. Another possibility is a marketing defect which occurs when a product is properly designed but improperly marketed. For example, the product might not contain the proper instructions necessary for safe use of the product or warning labels on the product to warn about potential hazardous uses. Products can also be found to be defective if they are found to have been manufactured improperly -- the design was right, the marketing was right, but somehow in the manufacturing process something went wrong.

In the online setting, we can imagine software having a design defect if the algorithms are improperly implemented. A marketing defect might be established if the manuals that accompany the software don’t point out certain shortcomings that they should. A manufacturing defect is a little harder to imagine, but say perhaps a virus attaches itself to the product unbeknownst to the manufacturer. In this case, the product was clearly properly designed and marketed, but somehow a flaw in the process of manufacturing ends up causing harm to a consumer later on. All three possible classes of defect potentially apply to online products.

Once one has established that the product was defective, the second element of the test, requires a showing that the defect made the product unreasonably dangerous to the consumer. It’s not just enough to show that there was a problem, it must have the effect of making the product unreasonably dangerous. We analyse this element using two questions. They are: who is the anticipated consumer and, is that consumer a sophisticated party? If a website, for instance, is open to anyone on the web, the anticipated consumer base is everyone online. If a website is password protected and only after certain qualifications does a person have access to that site, then perhaps those qualifications change the picture so that the person accessing the site is a
sophisticated party. In that case, all of the safeguards that might need to be built into the product otherwise may prove unnecessary.

The third element is whether the product reaches the consumer in substantially the same condition from the time it was sold. And, finally, we need to show that the defect caused injury to the user. These final elements complete the test, and, if established, will allow the plaintiff to recover.

We are trying to anticipate issues that are clearly on the horizon, issues that demand solutions, and demand some forward-looking policy analysis. I think that it is appropriate though to keep this in mind as a caution; to focus too particularly on a specific way that the technology is manifesting itself today when analysing your overriding policy approach, is in error. After all, one of the few things we can be certain of is that the way the technology works today will not be the way the technology works tomorrow.

**Jeffrey B. Ritter**
Program Director, ECLIPS, Ohio Supercomputer Center, United States

I find the topic of product liability an appropriate issue, and perhaps the OECD provides us with an appropriate venue from which we can conclude the substantive piece of this debate regarding the question of whether, indeed, industry has the will and the fortitude to respond to the opportunity to put in place the necessary structures for regulating and protecting consumers against the risks that we have been discussing for two days.

In her presentation, Commissioner Varney indicated that one role of government as regulators is to take the necessary steps to achieve a desirable social goal when the market is unable to do so. In order to achieve this goal, the private sector needs government to define and clarify the role of business as we look to accomplish these social and marketplace goals. Self-regulation is not a label under which to create or foster an environment of no rules; rather it is an alternative to government regulation to pursue the same social goals. Business will thrive when the environment for electronic commerce is predictable, when it is stable, and when there is legal certainty as to the rights of all participants.

For cyberspace, there are two truths which have not been mentioned in our debates and discussion. First, each of us as consumers own, possess, and
control electronic assets that are not different than our car, our home, or our watch, and those information assets are entitled to be protected. When we speak of product liability we must, as a global society, value the right of individuals to maintain the integrity, the privacy and the ownership of his or her personal information assets.

The second truth which we have not addressed is the reality of commerce. It is an unsettling truth that the risk of injury and loss is an economic analysis within business. Companies calculate the possibility of injury in the development, marketing and pricing of the product. This truth will not disappear when we speak of the risks of electronic commerce and the need to protect consumers. We may think of certain defects as innocent bugs or viruses, but indeed the equation of eliminating these defects and their potential for harm to our information assets is an inherent part of the creation, introduction, marketing and service of a company’s products and services. Faced with these realities, the challenge is to be proactive and not to simply wait until the market fails to produce a solution.

I believe there is a two-step approach which may apply to more than just the product liability vacuum we face on the Internet. First, I believe that government must assert and confirm their inherent authority and responsibility to protect consumers and to assure consumers meaningful recourse and remedies in the event of product liability or in the event of criminal misconduct. I would respectfully submit that the notion of waiting for market failure is perhaps not the best approach given the velocity and investment and risk that are proceeding apace even as we meet today. Rather, the goal of government should be to step forward and assure consumers (and investors in the commercial products and services which are the infrastructure of cyberspace) that governments do not intend to relinquish their jurisdiction. Regulation, including regulation of the quality and integrity of the marketplace and of the conduct of merchant behaviour, provides the essential building blocks of consumer protection -- it is necessary and appropriate for any marketplace. However, regulation need not arise solely from government -- industry self-regulation is an important part of the solution.

We can rely upon the technologies to implement many of the protections and controls that each of us as consumers desire over our participation in cyberspace and the ownership and the control of our information. But, I would submit the industry and the private sector must commit to formalising institutions and procedures in developing self-regulatory structures in order to facilitate integrity in the marketplace.
Globally, the notion of U.S. product liability standards are beginning to be recognised in a consistent manner in Western Europe. However, they remain unfamiliar principles of law throughout much of the remaining economies of the world.

So, we have an opportunity. Do we as governments foster product liability laws in the traditional setting to be responsive to the risks of defects and injury to consumers and our information assets, or do we as governments collaborate with the private sector in fostering a global regulatory framework of product liability protections that may give greater predictability and certainty that consumers will not be harmed in cross-border transactions?

Perhaps as suggested in the recent EC directive on product liability, governments can promote for us an understanding of the common standards, principles, guidelines or minimum rules that industry must satisfy through its regulation of itself in order to provide a defence.

As a starting point, it might be useful to refer to the U.S. Bill of Consumer Rights and ask the question -- and provide to industry the guidance - - whether the right to safety, the right to information, the right to choice, the right to be heard, the right to education and the right to effective dispute resolution are indeed global rights of all consumers. If governments might confirm those as initial standards for electronic commerce, we would have a place to start. That provides the opportunity for the second step -- the genuine development of meaningful standards through self-regulatory processes.

There must be a true collaboration between government and the private sector in order to induce private sector investment in regulatory infrastructure. We must know that the results will earn the respect of government.

Therefore, I suggest that certain minimal standards must be reviewed and, hopefully, confirmed by government. These minimal standards must not only define the processes by which self-regulation is to be shaped, but perhaps more importantly, the minimum commitments industry must make for self-regulation to be meaningful.

We have learned a great deal from watching the evolution of technology standards development. Standards are rules, and whether they govern the interconnectivity of our machines, or the interconnectivity of consumers with merchants, the process that is working as we end this century is one that is market driven. It is one that is agile, where the solutions do not take
forever to be produced. It is one in which there is a sufficient critical mass participation by the stakeholders that the resulting work product will be accepted in the market.

The proper role of government is to regulate only when there has been market failure. But the market -- to succeed -- must be given leadership by government. It is a different function, but it is a function which I would encourage the members of this committee to adopt, to invest in, and to become advocates for. The private sector will then have the opportunity to compete in innovating regulatory quality.
Discussion following the presentations in Panel 3 began with a comment on liability. In the commentor’s view, the opportunity exists for industry, in collaboration with government to define liability standards and to assure that the consumer without having to assume the burden of self-education, has the confidence in using electronic means of communication that certain quality standards exist. It is an environment in which we should foster a global commitment that the use and access assures the individual regardless of the state of development of their economy or of their education of certain basic, fundamental qualities regarding the performance of the systems.

In one commentor’s view, government should not just convene dialogues to develop standards for self-regulation. And that through the articulate definition of standards as to what constitutes acceptable products and services, business would have the confidence of a safe harbour in which to conduct its affairs. Not only within the current definitions of the U.S., but as business is transacted with consumers and businesses from other nations. With sufficiently articulate standards that government can endorse them as a minimum standard which businesses can use and know that they are not engaging in illegal or fraudulent behaviour.

The discussion then moved to the subject of self-regulation and standard setting. One commentator noted the importance of developing standards that foster innovation and ensure that small businesses have the ability to compete. It was suggested this can best be achieved by developing standards using an open, transparent and accessible process and encouraging broad participation. There was also some discussion of the role of government in moving industry to create sufficient and enforceable standards for self-regulation and the areas this self-governance might be effective. It was suggested by the United States that, at this time, government might be most helpful through the enforcement of existing regulations and perhaps articulated safe harbours. It was suggested that, for example, current advertising rules and industry standards could translate well in the online world, but that any information targeted at vulnerable populations such as children may not be sufficiently self-regulated.
The discussion then turned to contracts and consent. It was noted that the United States is nearing the introduction of a new article to the Uniform Commercial Code exclusively to govern the licensing of electronic assets. In the new article, a click of button indicating the acceptance of goods and services will be equal to a signature on a contract.
I have been asked to summarise our discussion over the past two days and to outline some ideas on where we might go from here.

Speakers have referred more than once to the importance of this moment in history. This gateway or bridge or crossroads to the information age. No one is storming the Bastille, but many monuments to our industrial past are under siege.

For better or worse, the information revolution is upon us. Information technology, especially the electronic network known as the World Wide Web has already changed our lives. As several speakers pointed out, we've only just begun to grasp the significance of the changes. In recent years, previous unimagined industries have arisen. We may now use information technology to pay our bills, buy our groceries, avoid rush hour by telecommuting, and keep in touch with our friends. We see, or very soon will see, many of the benefits Professor Heckman mentioned in his background paper. For consumers, this means increased purchasing power, new products and product information, and increased competition; for marketers, nearly instantaneous, low-cost access to a global market and one on one marketing on a massive scale. This technology has enormous potential to enhance our lives.

As speakers have pointed out, however, it can also serve as a powerful tool for fraud and deception. As consumer advocates, our first response must be to keep the Internet safe, but the question is how? Some speakers have called for immediate and comprehensive government regulation. Others have warned that this instinct might prove counter-productive in light of
the speed of technological change. One of the questions on the table is whether
government should lead, follow, get out of the way, or do all three.

In order to realise the commercial and cultural potential of the
Internet, consumers must have confidence that the goods and services available
over the Internet are fairly represented, they will get what they pay for, and if
they don't recourse is available. The challenge we face as regulators is to
preserve this potential. We heard from a number of industry representatives
that they share our commitment to preserving the safety of the Internet.
Industry understands that it can build the information infrastructure, but
consumers will not come unless it is safe and sound. So how do we achieve his
goal?

In several areas it is clear that consensus will not be achieved without
additional discussion. I think, however, that consensus did emerge on a
number of important issues in the course of this conference.

First, we must recognise that we are in this together. If the Internet is
to reach its potential we, government, industry and consumer advocates must
proceed as partners. We've made an excellent start over the past two days and
we must continue to work together.

Second, we must keep in mind that there are no borders in
cyberspace. Global problems require global solutions and thoughtful
international cooperation and dialogue of the variety undertaken here is
essential.

Third, we need to reach intentional consensus on first principles
before we decide how to get there.

Fourth, we need to educate ourselves, our consumers, and our
businesses. Consumer education is not a new goal, but it takes on a different
character and is much more likely to be effective in an environment that
facilitates interaction at the point of sale, where consumers are both most
vulnerable and available for education.

Fifth, we need to use the technology itself to empower consumers to
protect themselves.

And, finally, when we've identified important concerns that require
government action, we must have simple and predictable legal tools that are
sensitive to the technology and the pace of change in the online environment.
With respect to commercial law, projects like the UNCITRAL draft Uniform Commercial Code hold tremendous prospects for resolving barriers to the formation and fulfilment of commercial contracts on the Internet.

As I mentioned, a great deal of work remains. Now we must explore global approaches to the issues that we have outlined here, including privacy protection, including the rights of consumers to know when information is being collected from them, to control its use and transfer and to correct inaccurate information. Payment systems, including security, liability limitations, refund rights and charge backs. Identity verification and appropriate uses of anonymity. Advertising rules, including control of false and misleading information and special rules concerning vulnerable groups or reflecting societal values. Control of misrepresentation deception, and fraud, especially cross-border fraud. International codes of conduct and self-regulation. Legal frameworks including contract formation, product liability, dispute resolution and enforcement. Finally, consumer and business education.

It seems to me that this committee has its work cut out for it.
<table>
<thead>
<tr>
<th>Country</th>
<th>Main Sales Outlets</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSTRALIA – AUSTRALIE</td>
<td>D.A. Information Services 648 Whitehorse Road, P.O.B 163 Mitcham, Victoria 3132</td>
<td>Tel: (03) 9210.7777 Fax: (03) 9210.7788</td>
</tr>
<tr>
<td>AUSTRIA – AUTRICHE</td>
<td>Gerald &amp; Co. Graben 31 Wien I</td>
<td>Tel: (0222) 533.50.14 Fax: (0222) 512.47.31.29</td>
</tr>
<tr>
<td>BELGIUM – BELGIQUE</td>
<td>Jean De Lannoy 1010 Brussels</td>
<td>Tel: (02) 538.58.08.41 Fax: (02) 538.58.08.41</td>
</tr>
<tr>
<td>CANADA</td>
<td>Renouf Publishing Company Ltd. 1294 Algoma Road Ottawa, ON K1B 3W8</td>
<td>Tel: (613) 741.4333 Fax: (613) 741.5439</td>
</tr>
<tr>
<td>CHINA – CHINE</td>
<td>China National Publications Import Export Corporation (CNPIEC) 16 Gongti E. Road, Chaoyang District P.O. Box 38 or 50 Beijing 100704 PR</td>
<td>Tel: (01) 506.6688 Fax: (01) 506.3101</td>
</tr>
<tr>
<td>CHINESE TAIPEI – TAIPEI CHINOIS</td>
<td>Good Faith Worldwide Int’l Co. Ltd. 9th Floor, No. 118, Sec. 2 Chung Hsiao E. Road Taipei</td>
<td>Tel: (02) 391.7396/391.7397 Fax: (02) 394.9176</td>
</tr>
<tr>
<td>CZECH REPUBLIC – RÉPUBLIQUE TCHÈQUE</td>
<td>National Information Centre NIS – projekta Konviktiska 5 Praha 1 – 113 57</td>
<td>Tel: (02) 24 23.09.07 Fax: (02) 24 22.94.33</td>
</tr>
<tr>
<td>DENMARK – DANEMARK</td>
<td>Munksgaard Book and Subscription Service 35, Nære Søegade, P.O. Box 2148 DK-1016 Kobenhavn K</td>
<td>Tel: (33) 12.85.70 Fax: (33) 12.93.87</td>
</tr>
<tr>
<td>EGYPT – ÉGYpte</td>
<td>The Middle East Observer 41 Sherif Street Cairo</td>
<td>Tel: 392.6919 Fax: 360.6804</td>
</tr>
<tr>
<td>FINLAND – FINLANDE</td>
<td>Akateminen Kirjakauppa Keskusrank 1, P.O. Box 128 00100 Helsinki</td>
<td>Subscription Services/Agence d’abonnements : P.O. Box 23 00371 Helsinki Tel: (358) 0 121 4416 Fax: (358) 0 121 4450</td>
</tr>
<tr>
<td>FRANCE</td>
<td>OECD/OECD Mail Orders/Commandes par correspondance : 2, rue André-Pascal 75775 Paris Cedex 16 Tel. (33-1) 45.24.82.00 Fax: (33-1) 49.10.42.76 Telex: 600082 OCDE Internet: Compte:<a href="mailto:PUBIS@oecd.org">PUBIS@oecd.org</a> Orders via Minitel, France only/Commandes par Minitel, France exclusivement : 36 15 OCDE OECD Bookshop/Librerie de l’OCDE : 33, rue Octave-Feuillet 75016 Paris Tel. (33-1) 45.24.81.81 Fax: (33-1) 45.24.81.67</td>
<td></td>
</tr>
<tr>
<td>GERMANY – ALLEMAGNE</td>
<td>OECD Bonn Centre OECD Bonn Centre</td>
<td></td>
</tr>
</tbody>
</table>