

The

IPTS

March/2000

42

ISSN: 1025-9384

5 EURO
BYPO

REPORT

EDITED BY THE INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS)
AND ISSUED IN COOPERATION WITH THE EUROPEAN S&T OBSERVATORY NETWORK



SPECIAL ISSUE: TECHNOLOGY & POLICY FRAMEWORKS FOR E-COMMERCE

2 Technology & Policy Frameworks for E-commerce
Bernard Clements & Ioannis Maghiros

25 E-commerce and the Encryption Debate
Stuart J. D. Schwartzstein

5 Technologies and Regulatory Frameworks
for Network Access: A Delicate Balancing Act
Eric Van Heesvelde

31 Alternative Paradigms for European
E-commerce
Andrew McMeekin, Ian Miles & Jason Rutter

12 New Rules to Deal with Old Problems in
Internet Commerce
Morten Falch & Anders Henten

38 The Need for an International Infra-
structure for Low-value Payment Systems
Michael Rader, Knud Böhle & Ulrich Riehm

18 Frameworks for Privacy in the On-Line
Environment
Jos Dumortier & Caroline Goemans

EUROPEAN COMMISSION
Joint Research Centre



ENGLISH VERSION

ABOUT THE IPTS REPORT

The IPTS Report is produced on a monthly basis - ten issues a year to be precise, since there are no issues in January and August - by the Institute for Prospective Technological Studies (IPTS) of the Joint Research Centre (JRC) of the European Commission. The IPTS formally collaborates in the production of the IPTS Report with a group of prestigious European institutions, forming with IPTS the European Science and Technology Observatory (ESTO). It also benefits from contributions from other colleagues in the JRC.

The Report is produced simultaneously in four languages (English, French, German and Spanish) by the IPTS. The fact that it is not only available in several languages, but also largely prepared and produced on the Internet's World Wide Web, makes it quite an uncommon undertaking.

The Report publishes articles in numerous areas, maintaining a rough balance between them, and exploiting interdisciplinarity as far as possible. Articles are deemed prospectively relevant if they attempt to explore issues not yet on the policymaker's agenda (but projected to be there sooner or later), or underappreciated aspects of issues already on the policymaker's agenda. The multi-stage drafting and redrafting process, based on a series of interactive consultations with outside experts guarantees quality control.

The first, and possibly most significant indicator, of success is that the Report is being read. The issue 00 (December 1995) had a print run of 2000 copies, in what seemed an optimistic projection at the time. Since then, readership of the paper and electronic versions has far exceeded the 10,000 mark. Feedback, requests for subscriptions, as well as contributions, have come from policymaking (but also academic and private sector) circles not only from various parts of Europe but also from the US, Japan, Australia, Latin America, N. Africa, etc.

We shall continue to endeavour to find the best way of fulfilling the expectations of our quite diverse readership, avoiding oversimplification, as well as encyclopaedic reviews and the inaccessibility of academic journals. The key is to remind ourselves, as well as the readers, that we cannot be all things to all people, that it is important to carve our niche and continue optimally exploring and exploiting it, hoping to illuminate topics under a new, revealing light for the benefit of the readers, in order to prepare them for managing the challenges ahead.

EDITED BY THE INSTITUTE FOR PROSPECTIVE
TECHNOLOGICAL STUDIES (IPTS)
And Issued in Cooperation with
the European S&T Observatory Network

PUBLISHED BY THE EUROPEAN COMMISSION

Joint Research Centre
ISSN: 1025-9384
Catalogue Number GK-AA-00-002-EN-C
DEPOT LEGAL: SE-1937-95

DIRECTOR

Jean-Marie Cadiou

EXECUTIVE EDITOR

Dimitris Kyriakou

EDITORIAL BOARD

G. Fahrenkrog, P. Fleissner, J. Gavigan,
M. González, H. Hernández, D. Kyriakou, I. Maghiros
(Production Manager), P. Sorup, A. Soria, C. Tahir.

PRODUCTION

CINDOC-CSIC/L&H Spain

PRINT

Graesal

TRANSLATION

CINDOC-CSIC/L&H Spain

COPYRIGHT

The views expressed in this publication do not necessarily reflect those of the European Commission
© ECSC-EEC-EAEC Brussels-Luxembourg, 1997
Reproduction is authorised, except for commercial purposes, provided the source is acknowledged.
The EC may not be held responsible for the use made of the information.

THE IPTS REPORT

is published in the first week of every month, except for the months of January and August. It is edited in English and is currently available at a price of 50 EURO per year, in four languages: English, French, German and Spanish.

SUBSCRIPTIONS

For a subscription to The IPTS Report, or to amend an existing subscription, please write with full details to:

The IPTS Report Secretariat
IPTS, JRC Sevilla
World Trade Center
Isla de la Cartuja
E-41092 Sevilla, Spain
Tel: +34-95-448 82 97
Fax: +34-95-448 82 93
E-mail: ipts_secr@jrc.es

Web address: www.jrc.es/iptsreport/subscribe.html

C O N T E N T S

2 Editorial. Technology & Policy Frameworks for E-commerce

5 Technologies and Regulatory Frameworks for Network Access: A Delicate Balancing Act

The success of e-commerce will depend on affordable, high-quality network access being made available to residential and small-business users. With a variety of technologies and players overlapping in the market, regulators need to balance long- and short-term interests carefully.

12 New Rules to Deal with Old Problems in Internet Commerce

Although the need to protect consumers against unscrupulous sellers is not new, national approaches differ and the cross-border nature of e-commerce makes it necessary to find new ways of providing unsatisfied customers with redress.

18 Frameworks for Privacy in the On-Line Environment

The use of personal information is an intrinsic part of successful e-business. Thus ways need to be found to balance the needs of e-businesses with concerns about privacy. The relation-building aspect of the standardization approach could help create the right privacy-protection environment.

25 E-commerce and the Encryption Debate

Encryption is finding increasing use as a means of protecting sensitive data passed over the all-too-public Internet. Arrangements intended to ensure governments continue to exercise their traditional control over this technology face a number of problems.

31 Alternative Paradigms for European E-commerce

It is generally assumed that the Internet will be the dominant paradigm for e-commerce in Europe, as it is in the US. However, mobile telephony, digital TV and EDI offer other alternatives, which may have interesting ramifications.

38 The Need for an International Infrastructure for Low-value Payment Systems

While credit cards can be used for on-line transactions above a certain value, there is as yet no widely accepted system for small-value payments. Such a system could give a boost to e-commerce, all the more so in view of the projected path towards the digital economy.

EDITORIAL

2

Technology & Policy Frameworks for E-commerce

Bernard Clements & Ioannis Maghiros, *IPTS*

Over the last year or so electronic commerce (e-commerce) has shown itself to be a strategy for success for some and an implementation minefield for others. Not all those adopting this new distribution channel have found it financially rewarding, yet it has allowed newcomers in certain sectors to raise their stature to the point where they threaten incumbent giants. Predictions about the volume of e-commerce and its rate of growth vary widely (and are frequently distorted by economic interests). But in reality so far it has remained small, accounting for less than 1% of retail trade. Although the figures suggest Europe is lagging behind the United States, many believe it will close the gap and expect growth rates to be as high as 100% a year over the next three years (assuming that PC penetration increases and that telephone tariffs decrease further - Forester Research 27/12/99).

Whatever its current usage, which is strongly influenced by the overall active number of Internet users, e-commerce will bring with it a range of transformations. It is a source of new wealth, new business organization paradigms, new methods of work, and could bring a shift in social patterns. It offers convenience of use and time and cost savings to the end-user, in addition to stressing the differences that exist at many social and economic levels. The main reason for its growth is attributed to its enhancing both the supply and the demand chains (e.g. impact on inventories, sales, distribution) which are quickly

translated into cost reductions, although not necessarily immediately into price reductions.

A very much "hands-off" regulatory approach has been crucial to the growth of e-commerce so far. Fundamental to ensuring that this growth continues are issues of (a) developing a sufficiently large infrastructure and ensuring affordable access to it; (b) enhancing trust and confidence of both citizens and businesses alike; (c) coping with the lightning pace of technological evolution; as well as (d) identifying where, what and how rules should be applied. In addition, the impact of e-commerce on international trade, taxation and operation of global financial markets is only now starting to be assessed. Moreover, the ability to measure precisely the composition and growth of e-commerce (especially the widely diffused business-to-business segment), as well as the ability to educate and train the necessary human resources required for its long-term operation (probably the first step towards a digital economy), will become essential properties of the expected growth.

Against this backdrop Governments and businesses everywhere seem to agree that a predictable, stable legal environment, even if not globally uniform, is a necessary condition for continuous growth, provided interoperability is ensured. Current thinking takes the line that enhanced competition and consumer choice should be the main driving force, while the

privacy and security issues raised should be dealt with under sectoral self-regulatory regimes that provide a safe environment without establishing extra barriers. Yet, technological evolution, which is both solving problems and creating new ones, can only mean that a new approach to developing a policy framework needs to be considered. One that defines globally accepted principles, allows market forces to develop their own tools and procedures to address any emerging problems and concurrently develops the means to validate market-led instruments and educates users so that they themselves may handle any negative consequences.

The IPTS has been analysing the socio-economic implications of e-commerce since 1998. In order to achieve this it has conducted studies and organized a series of workshops¹ which have sought to establish comparative perspectives on regulations, so as to inform European policy-makers on current developments in other regions and provide an open forum for debate. As a further step in this ongoing process, the IPTS is co-financing, with Directorate General for Enterprise, the development of a European Observatory on electronic payment systems (see: <http://www.jrc.es/pages/projects/e-business.html>).

This special issue of the IPTS Report aims to present just some of the aspects raised in defining the required technology and policy frameworks. The main questions are centred on identifying the best process needed to achieving a policy

framework that encourages rather than stifles growth, and at the same time on setting commonly accepted standards and rules reflecting technological evolution. The following are the main aspects presented in the 6 articles of this issue:

The first of the articles presents the role of the national regulatory authorities in **ensuring affordable universal access**, the circumstances under which unbundling the local access network might prove to be advantageous, how to deal with the interconnection problem, and finally how to tackle the risk of oligopolies in provision of backbone capacity.

The second article analyses some of the existing regulatory problems in the area of consumer protection in the light of the fresh challenges created by the emergence of e-commerce. It then goes on to describe the international/regional and public/private initiatives being developed for their solution, the optimal solution probably being a **mix of state and self-regulation**.

In our third article, the authors deal with some of the issues regarding the **protection of privacy**. They explore the differing environment for data protection in the U.S. and the EU and how the public/private sector is dealing with this. They go on to propose general guidelines for the establishment of a "standards-approach" process that would aim to balance the needs of the business world and those of the individual consumer.

Note

1. A workshop in June 1999 to explore the limits and opportunities of self-regulation from primarily a European perspective; and one in October 1999 to discuss the relationship between policy objectives, self-regulation and the role of standardisation in the area of privacy policy; and one in January 2000 to examine responsive regulatory frameworks and processes that may be applied to Internet commerce on a global basis. This last workshop also addressed the theme of taxation in an electronic world. (web address <http://www.jrc.es/pages/projects/e-business.html>)

In the fourth of the articles, **encryption** is discussed as a means of protecting the confidentiality of transmitted data over a public Internet. The potential misuse of encryption raises a series of issues that governments, industry and the public will have to solve if e-commerce is to flourish. In addition when addressing these issues it may well be worth considering that not all disparate needs may be met at the same time and especially the aim to regulate encrypted content.

The authors of the fifth article suggest that, considering Europe's economic and cultural identity, it is unlikely that the pattern of technological uptake will be identical to that of the U.S. with the only difference being that of a time

lag. In this case it would be worthwhile to prepare for the possibility of **alternative technological platforms becoming a significant paradigm for business to consumer e-commerce in Europe**. It is suggested that their ramifications should be studied and appropriate scenarios developed.

The last article deals with a relatively modest issue with far-reaching implications. The authors present the need for developing a **widely accepted system for small-value payments** and the boost this could bring to trade in intangible goods and services as well as the completion of monetary Union. For this to happen, a set of technological issues, as well as various political and cultural issues, will have to be addressed.

Contacts

Bernard Clements, Head of Unit

Life Sciences & Information and Communication Technologies, IPTS

Tel.: +34 95 448 84 49, fax: +34 95 448 82 08, e-mail: bernard.clements@jrc.es

Ioannis Maghiros, IPTS

Tel.: +34 95 448 82 81, fax: +34 95 448 83 39, e-mail: ioannis.maghiros@jrc.es

Technologies and Regulatory Frameworks for Network Access: A Delicate Balancing Act

Eric Van Heesvelde, *BIPT*

5
Information and
Communication
Technology

Issue: The cost of access to data and multimedia services is a key factor for the diffusion of electronic commerce in Europe. Greater competition in the context of "convergence" is likely to push down prices and weed out inefficient network solutions.

Relevance: As well as the need to ensure that market rules keep pace with changes in technology, regulatory bodies are faced with three fundamental problems that need to be solved in the short term; universal access at affordable tariffs (related to the question of competition in the local loop), interconnection and the risk of oligopoly formation in the backbone market.

Universal access

Is there enough choice in the local loop?

Despite the liberalization of the telecommunications market, users have yet to enjoy the full benefits due to the lack of competition in the local loop (i.e. the connection from the user's home or premises and the network). It emerged early on that the level of investment alternative operators needed to reach all end users via adequate infrastructure was much too high to permit full competition in this segment. In response many European Member States have either started to introduce local loop unbundling (LLU) or have at least begun a consultation process to discuss the options for bringing competition into the local loop. The fact that xDSL services (x Digital Subscriber Line, where the "x" stands for one of a number of

access methods) can also make use of the local subscriber telephone link means it is not just would-be telecoms operators who have a stake in unbundling. Nevertheless, the process is a complex one and EU Member States may take different approaches depending on national circumstances and preferences.

When defining their approaches National Regulatory Authorities (NRAs) need to take into account the phenomenon of convergence. This convergence not only concerns the blurring of the limits between fixed and mobile telephony but also the phenomenon of integration all along the value chain, bringing together access providers, network operators, service providers and content producers. The second essential consideration is that, in most European countries, although effective competition has reached the mobile telephony market, and there

Liberalization of telecommunications markets in Europe has yet to bring effective competition to small-business and residential users. Local-loop unbundling (LLU) is one solution being put forward

is growing competition in the business market (where corporate users usually have a choice of alternative operators or leased lines), there is clearly still insufficient competition in the residential and small-business market. Thus it is here that the question of unbundling is most relevant.

These phenomena imply a new role for NRAs: not only to stimulate competition, but also to facilitate change by fostering innovation and thereby creating added value for industry and consumers. From the regulatory perspective, solutions have been put in place to help overcome many of the obstacles, such as interconnection, Significant Market Power (except perhaps for mobile-fixed relations and mobile-mobile relations), frequencies, number portability, etc. Nevertheless, the issue of customer access has still to be resolved.

At present the access market offers a variety of possible technical options:

- Copper (the incumbent's Public Switched Telecom Network) with :
 - upgrading (e.g. xDSL)
 - Carrier Select and Carrier Preselect
 - Value Added Services for competitors (in collecting or terminating model)
- cable
- leased lines

- wireless local loop
- satellite
- powerline (although not yet fully proven)
- convergence (fixed & mobile) :
 - GSM 2nd generation-upgrading
 - UMTS : network + services + content
- unbundling of the local loop

The table below, which indicates the potential capacities, the timing for market introduction and the cost of investment (and so ultimately the cost to the end user) clearly shows that diversity on the supply side does not necessarily mean that there is optimal competition in the market.

Is unbundling of the local loop a viable alternative?

NRAs' decisions regarding unbundling should be based on the criteria of timing, demand for bandwidth and the cost of the alternatives. Moreover, they should take into account supply and demand for new services in both the short and medium term. Unbundling is possible in the very short term, whereas competition in UMTS (Universal mobile telecommunications service) is to be situated in the longer term. Weighing up several technologies and analysing whether a decision does not, in one sense or another,

Table 1. Access technologies

	BITS/SEC	TIMING	COST OF INVESTMENT/ COST PER SUBSCRIBER
COPPER X DSL			
ADSL	± 1 Mbps	NOW	± CHEAP
HDSL	several Mbps	VERY NEAR FUTURE	± EXPENSIVE
CABLE	VARIABLE, from Kbps to several Mbps	VARIABLE	± VARIABLE / EXPENSIVE
WLL	64 kbps - 155 Mbps	NOW	± EXPENSIVE
GSM:HSCSD	57,6 kbps	NOW	± CHEAP
GPRS	115 kbps	VERY NEAR	± CHEAP
EDGE	384 kbps	VERY NEAR FUTURE	± CHEAP
UMTS	2 Mbps	(NEAR) FUTURE	± EXPENSIVE

undermine the future possibilities of a new technology, is obviously hazardous in the telecoms market given the pace of change. Nevertheless, it could be argued that unbundling might limit the future potential of UMTS given that users may be reluctant to buy new terminal equipment after having invested in Asymmetric Digital Subscriber Line (ADSL), for instance. Will operators be inclined to make risky investments in UMTS when they find that upgrades of GSM (i.e. GPRS) and unbundling of the local loop can provide an adequate (if not optimal) service? On the other hand, past experience seems to suggest that when a new technology is sufficiently attractive users will tend to adopt it.

More difficult, however, is the question of the extent to which unbundling might have a negative impact on cable investments. This is definitely an essential part of the question in countries where cable penetration is very high and where these operators have made and are still planning huge investments (e.g. Telenet and UPC in Belgium). Generally speaking, LLU should be carried out in a way that avoids undermining incentives to invest in broadband networks. Moreover the NRA is obliged to take account of the need for consistency and transparency in the regulatory framework. Technological and commercial factors already bring more than enough uncertainty to the sector, and legislation should avoid adding to it.

In view of this, the policy of certain NRAs to introduce sunset clauses (i.e. clauses which set in advance the date at which the regulatory instrument is to become ineffective) may be an option in some cases. This offers the advantage of responding smoothly to specific market developments. For instance, this could be used to introduce unbundling in specific regions for a certain period, for example if the incumbent fails to introduce new technologies, does so badly or at

too high a price. Or, alternatively, when the cable operator, as a duopolistic player in the customer-access market fails to introduce enough real competition in the market.

There may also be other options, however, such as partial base-band leased circuit technology, bitstream access, permanent virtual circuit access, indirect access. One option that could be considered, for instance, would be to force the incumbent to offer service plans via leased lines for ADSL access to alternative service providers and operators. This would certainly have a positive impact on the supply of higher bit rates to companies and users with sufficient demand for them.

With all these considerations one should not lose sight of certain key issues upon which the ultimate success of both unbundling and other medium-term developments rests:

- The correct definition of costs. It is a highly complicated matter to determine the right compensation for the incumbent; it is also fraught with dangers given its close links with a number of fundamental economic problems on the boundary between the short and longer term. Getting the tariff balance right is a decisive factor in stimulating effective market entry. In some cases (especially in remote regions) it can bring to the fore the question of the local access deficit and consequently the need for rebalancing the tariffs. Finally, the introduction of LLU must not erode the incumbent's incentive to build or upgrade infrastructure;
- A number of technical problems have yet to be solved. These include uncertainty about the length of individual lines that can be served. The suitability of lines has to be studied case by case, which means there is sometimes the need for efficient spectrum management. This in turn influences overall capacity possible while avoiding mutual interference.

Local loop unbundling could be implemented quickly, but may undermine the prospects for other solutions that will only become available in the longer term

One option would be for local loop unbundling to be used to encourage competition in specific areas and for specific periods

One way of stimulating e-commerce might be to introduce different pricing structures for data than for voice traffic, although from the operator's point of view the cost is basically the same

Many Internet services providers are able to offer free connection thanks to the way collecting costs are calculated. Lowering retail tariffs could jeopardize this business

- The problem of collocation and other logistic issues have also to be solved.

In the meantime regulators need to be aware of the danger of network operators re-establishing a monopolistic position in the absence of LLU, e.g. with xDSL. The incumbent could sign an exclusive contract with certain suppliers, thereby denying other suppliers access to that terminal equipment market. This situation's arising could be sufficient reason for unbundling.

The interconnection issue is the existing interconnection model suitable for lower tariffs?

It is not enough to provide universal access to all users; they should also be able to enjoy Internet access under sufficiently advantageous conditions so that electronic commerce can develop in the business-to-customer segment. Therefore regulators will have to answer the question whether it is justified for retail tariffs for data communications to be lower than retail tariffs for telephony. Unless infrastructures have been specifically adapted for data communications right down to low levels of the network, this option may not be easy to implement. Nevertheless, it is safe to say that from a strategic point of view it is not unjustified to differentiate between voice and data, considering the need to stimulate electronic commerce and internet access and the specific user profile of this kind of communications, which on average have a much longer duration.

The question is, however, how to make these retail tariffs substantially lower than the other tariffs, when one assumes that the cost price elements for the use of the network, at least as far as access to the last mile are concerned, are basically still the same.

In general the financial flow is as follows: Retail = Collecting + Terminating + the costs of the internet service provider (ISP) for peering (i.e. direct interconnection agreements between ISPs) and/or transit. As the incumbents' interconnection conditions have been determined by the NRA and are cost-oriented, this simple formula clearly shows that the margins for lowering the retail tariffs are not very big. The problem is more complicated still, in fact, because the terminating revenues paid by the incumbent to the other licensed operators (as part of the specific interconnection terms) are used by these operators to pay opportunity costs to the internet service providers, thereby enabling the ISPs to offer their customers free access. Lowering the terminating tariffs could therefore put this under pressure, so that lower retail tariffs could lead to the disappearance of free internet access paid for in this way. Thus, in the existing terminating context, the margins are fairly tight.

This model also holds two additional risks that put a heavy burden on optimal economic efficiency. First of all there is no pressure whatsoever either on the incumbent, who sets the retail tariffs, nor on the other operators or the Internet service providers, to intervene either in the collecting costs, or in the terminating price. Everyone is comfortable with the situation, since the retail tariffs – in a monopoly for the incumbent – are the same for everyone anyway. A second risk is that by changing the terminating aspect the door is left open for the incumbent to squeeze retail pricing, thus making it harder for other operators to compete.

Efforts to lower the retail tariffs drastically in the short term could therefore upset certain financial balances and the short term advantages could strengthen the incumbent's hold over the data market and remove any incentives to make further investments in that market.

Box 1. Glossary: Telecommunication terminology

CPS	Carrier Pre Select
Collecting	CSC-based conveyance of calls generated by end users of a network operator to a point where another operator is interconnected with this network
CS	Carrier Select
EDGE	Enhanced Data rates for GSM Evolution Evolution of the GSM standard using a new high-level modulation process on the radio interface of a GSM network = 384 kbit/s
Extra access area	Collecting or terminating service requested by interconnected operator crosses the boundaries of the access area where the call was handed over to, respectively by the interconnected operator
GPRS	General Packet Radio Services Evolution of the GSM standard transforming a GSM network into a packet switched data network = 115 kbit/s, or even 170 kbit/s
HSCSD	High Speed Circuit Switched Data Evolution of the GSM standard allowing to combine several time slots on the radio interface in order to achieve a higher bit rate = 57,6 kbit/s
Intra access area	collecting or terminating service requested by interconnected operator remains within access area where the call was handed over to, respectively by the interconnected operator
LLU	Local Loop Unbundling, i.e. allowing competitors direct access to the local loop by forcing the incumbent to sell or lease the links to homes or business premises to competing telecoms operators.
NRA	National Regulatory Authority
Powerline	line that is part of a network used to convey electrical energy
Terminating	conveyance of calls by a network operator handed over by an interconnected operator to destinations on the network of the network operator (e.g. identified by geographic numbers)
UMTS	Universal Mobile Telecommunications Systems Third generation of radio systems for mobile communication. UMTS will be the European variant of a family of standards named IMT-2000 ("International Mobile Telecommunications") recognized by the International Telecommunication Union (up to 2 Mbit/s), with an intelligent architecture achieving fixed-mobile convergence.
xDSL	A method of transmitting digital data at high bit rates using advanced modulation and signal processing techniques over the existing installed twisted pairs of the access network
ADSL	Asymmetric Digital Subscriber Line, xDSL family member
HDSL	High bit rate Digital Subscriber Line, xDSL family member
WLL	Wireless Local Loop (also known as Fixed-Wireless Access, FWA)

Introducing a specific series of numbers for Internet access might lead to tariff innovations, as well as making the cost of access more transparent for users

Is there an alternative?

Supposing that internet access were considered as a **wholesale market**, the internet service provider having to hold both on the tariffs per unit time and on the access subscription conditions, it might be possible to work out some alternatives. This would first of all mean that specific series of numbers for Internet access are introduced. In general this would also make the costs of connecting to the Internet more transparent for users because the service is provided as a whole by the Internet service provider. Furthermore, it would make room for tariff innovations. Finally, and most importantly, any gain in efficiency would be passed on to the end user. This is basically the same as the collecting model described above, but although the formula $\text{Retail} = C + T + \text{ISP costs}$ remains unchanged, competitive pressure would be introduced at each level of costs, causing tension between competitors for retail prices too. In such a situation one can no longer talk about a collecting fee for the incumbent, but about a withholding. In this context it is essential to fix this withholding correctly, in relation to the collecting costs the incumbent has to bear.

However, a number of problems will persist, such as the distinction between the intra access area (IAA) and the extra access area interconnection conditions, since at this moment there is sometimes not enough competition on the level of the backbone segment. ISPs are then faced with a difficult choice, either face high charges for leased lines or the high cost of IAA access investments. So, intervention of the NRAs is also needed here. A second problem is that care has to be taken that the various models (collecting and terminating and the use of geographical and non-geographical numbering) co-exist for some time, in order to allow all market players to go from one system to the other in a fair way.

These considerations –although only briefly stated– make it amply clear that it definitely would be advisable to proceed with caution where interconnection is concerned so as to avoid short term interests standing in the way of the balanced development of the sector over the longer term. Moreover, miraculous reductions in retail tariffs cannot be expected. The need for the necessary investments to make data transmission more efficient over the “last mile” to the end user, should not be overlooked.

The Risk of Oligopolies

The third problem in the electronic commerce market is also very complicated and the solutions may well be even less apparent. Internet service providers are forced, both nationally and internationally, to reach agreements for the extension of ways of terminating traffic. On the domestic market they have to appeal to other operators, which makes them subject to the general price level of leased lines, internationally they have to conclude peering agreements or transit agreements with ISPs or operators that may or may not apply accounting rates themselves. In general, there is a lack of transparency in the international market and this may also favour oligopoly formation. At the same time some experts point to a risk of over-investing, leading to over-capacity. In any case entry in this market is not easy. Also, not unsurprisingly given the cost of infrastructure, many internet service providers have a privileged link with certain network operators.

This gives rise to a number of risks, in particular the disappearance of smaller ISPs who are pushed out of the market because they lack that privileged link. Also it can force integration in the value chain of operators, service providers, backbone operators (and for reasons having to do with convergence, also content providers), to the extent of severely limiting competition in this


segment. Another possible repercussion is that in countries with small markets and consequently smaller access players, these small players are likely to be absorbed in this worldwide battle.

The problem of the cost price of national leased lines may still seem solvable for the Member States, supported by the European Commission and its analysis of cost-orientation for this market, but on the international level the problem is much harder to solve. This is largely due to the fact that this market is highly opaque, but also because it is not clear which bodies are to regulate these problems and on what legal and strategic basis they should do so.

Conclusion

The first two problems (universal access, i.e. competition in the local loop and interconnection) have made it clear that the NRAs have to make tough decisions about the short and the long term, while bearing in mind the need not to undermine the incentives to make investments and to guarantee fair compensation of all market players

involved. At the same time, the regulatory system must apply sufficient competitive pressure to ensure the market evolves in a way beneficial to consumers. Whereas the problem of competition in the local loop may seem solvable in the short term by means of LLU –possibly including sunset clauses or specific rules where there is already some competition in the local loop– the interconnection debate is still some way from being concluded. The key here is to rethink the interconnection problem, but with due caution in order to avoid the short-term advantages of lower internet tariffs harming competition in the longer term.

As for the backbone problem and especially the risk of oligopoly formation, the solution seems to lie in the general rules of fair competition rather than in sector specific rules. Apart from that, it is all too clear that the major part of the problem will have to be handled at the international level. The European Union would benefit from a common position in order to lay down enforceable and fair rules in the competent international bodies such as the ITU (International Telecommunication Unit) or WTO (World Trade Organization). 

The opaqueness of the market and the big differences in size between players create a risk of oligopoly formation

Keywords

local loop unbundling, interconnection, oligopoly formation

Contact

Prof. Eric Van Heesvelde, General Administrator BIPT (Belgian Institute for Postal Services and Telecommunications)

Tel.: +32 2 226 87 63, fax: + 32 2 223 24 78, e-mail: eric.van.heesvelde@bipt.be

About the author

Eric Van Heesvelde

is a lawyer by training and is currently General Administrator of BIPT and a guest professor at the University of Ghent.

Other past and present responsibilities include working as a legal advisor for a private firm, membership of the Belgian Planning Office responsible for the communications and transport sector, the post of head the Cabinet of the Minister of Science Policy, and the post of deputy head of the Cabinet of the Minister of Cooperation Development.

New Rules to Deal with Old Problems in Internet Commerce

Morten Falch & Anders Henten, *CDI/DTU*

Issue: The emergence of an electronic market has created a range of new regulatory problems relating to authenticity, quality and security, cancellation and consumer redress, contractual issues, payments, marketing practices and privacy. These issues apply in particular to cross-border transactions. Common minimum rules need to be established to increase trust and confidence levels, since suppliers do not always live up to desirable standards.

Relevance: Lack of transparent legislation protecting consumer rights could prevent the electronic market place from reaching its full potential as consumers may be reluctant to engage in transactions on the Internet if they are unsure of their rights and obligations. This applies in particular to European countries with a long tradition of legislation on consumer issues. Regulation may be rule-based or market driven, but needs to be transparent to consumers and sufficiently flexible and dynamic to meet the demands of an ever-changing environment.

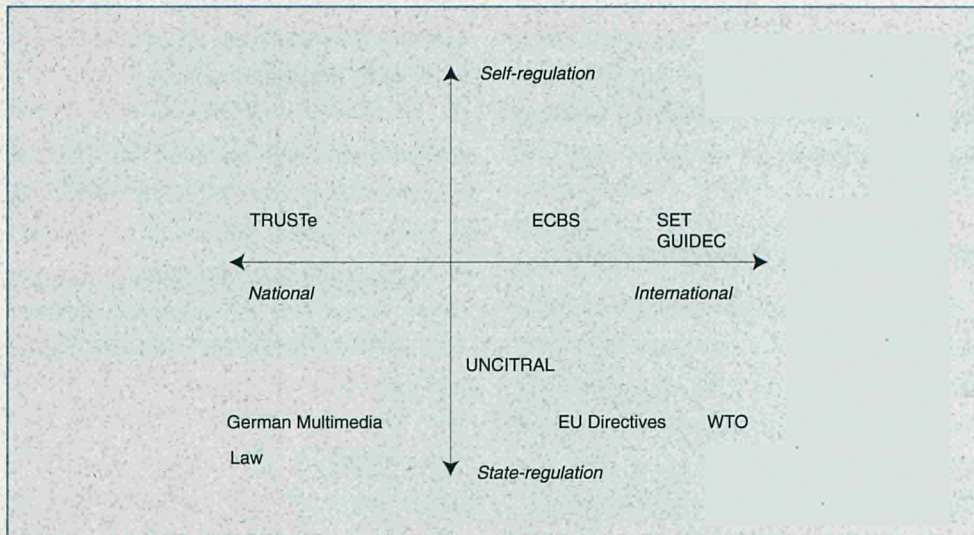
Although the Internet has developed fairly successfully so far without much regulatory intervention, there is a general recognition that some sort of regulation is necessary where consumer protection is concerned; this could take the form of self-regulation or regulation by some national or international authority

Regulatory frameworks

So far the Internet has developed very successfully in a basically unregulated environment. There are, however, a number of issues related to consumer protection where some type of regulation may be desirable. This is recognized both by national governments and international bodies such as the Organization for Economic Cooperation and Development (OECD) and the World Trade Organization (WTO). The question is how regulation of international transactions on the Internet can be enforced in a world where regulation is defined and enforced within national borders.

A number of regulatory models have been proposed to solve this issue. These models can be characterized by their location on a two dimensional continuum defined by two different parameters: The degree of international orientation and the degree of government intervention (Figure 1).

In the bottom left-hand corner we have national legislation, which is the dominant form of regulation in the physical world. One example is the German Law on Multimedia, which also addresses electronic commerce. In the bottom right-hand corner we have international agreements such as WTO treaties. In between we have EU Directives, e.g. the directive on electronic commerce.

Figure 1. Dimensions of regulation

Model laws from the United Nations Commission in International Trade Law (UNCITRAL) can be seen as a mixture of international and national regulation. UNCITRAL has prepared an international model law on electronic commerce, and the idea is that elements of the law should be adopted in the national legislation in the different countries. Individual countries will not adopt the whole model law, as they will take existing national laws and environments into account. However, the initiative contributes to a certain degree of international harmonization. The model law may also serve as an inspiration for a code of conduct and has, therefore, also a slight element of self-regulation.

The very top of the figure represents a situation with an entirely unregulated market where each actor is free to define his own set of rules. Below we have a market where a number of organizations define their own set of rules or a code of conduct to which actors can adhere on a more or less voluntary basis (self-regulation). These organizations can either be national, regional or global in their reach. TRUSTe is one out of a number of organizations that have been

set up on private initiative to regulate behaviour on the Internet without government intervention. A service provider can, if he follows certain rules on privacy protection, receive certification from TRUSTe, which can be made visible on his website. In principle such services can have a global reach. So far TRUSTe has tended to aim its services at the US market, but is now beginning to create a foothold in Europe.

The European Committee for Banking Standards (ECBS) and Secure Electronic Transaction (SET) are examples of standard setting for electronic payments. ECBS is developing European standards for electronic payments over the Internet, e.g. the European Electronic Purse, and SET is an example of an international standard which can be used to secure payments on the Internet. SET is backed by most of the major credit card companies and has created a framework for a hierarchy of trusted third parties that can guarantee the validity of the payment.

GUIDEC (General Usage for International Digitally Ensured Commerce) is an example of an international initiative that intends to establish an

The United Nations Commission in International Trade Law has prepared an international model law on electronic commerce, with the intention that it be adapted to the national legislation of individual countries

One approach to self-regulation would be for national, regional or international organizations oversee behaviour and issue certification. A number of initiatives of this type are underway

The argument most frequently levelled against state regulation is that it stifles innovation. On the other hand, some form of regulation may be necessary to inspire confidence in consumers

The problems associated with self-regulation should not imply state regulation is the only option, the optimal solution is probably a mix of state regulation and self-regulation

international code of conduct for electronic commerce. GUIDEDEC is an initiative of the International Chamber of Commerce (ICC) providing a set of common definitions and business-generated best practices for certifying electronic commerce.

Self-regulation vs. state-regulation

The issue of consumer protection is often discussed in terms of consumer trust and confidence. The fact that some suppliers may not live up to desirable standards makes rules necessary to secure the trust and confidence of users. It is frequently argued that self-regulation ensures adequate control as suppliers have an interest in delivering good quality at acceptable prices as otherwise they will not survive in the market. However, it is clearly not always the case that enlightened self-interest alone is enough, as it leaves the door open for the unscrupulous players, uninterested in long-term survival in the market, to make a quick profit through cheating, fraud or other kinds of malpractice. Clearly some form of regulatory framework is required, not least in order to create the necessary trust and confidence for the market to develop. If consumers are to use it, the system not only needs to be trustworthy it needs to be seen to be trustworthy.

The primary argument against state regulation – apart from it ostensibly being impossible in an international Internet environment – is that it tends to stifle development and innovation. This is a well known argument against almost any state intervention in markets, but it is here reinforced with arguments concerning the inherently international, distributed and unregulated “nature” of the Internet. The counter-argument is also well known, namely that there has to be a stable regulatory framework for markets to grow and develop. Debates of this type have frequently been rehearsed in the standardization field, for instance.

In the area of e-commerce, the argument is that lack of information and security for consumers constitute market failures that require governmental (or inter-governmental) intervention.

Nevertheless, self-regulation also has its difficulties. One problem lies in the definition of the group or groups that are to be regulated (which may be different in the case of business-to-business e-commerce and business-to-consumer e-commerce) and the players who are to have a say in the process.

Even if there is no state governance of a market, there will still be some kind of governance structure. The governing parties will then not be the state but generally business representatives, and probably representatives of the larger corporations. Even if some consumers may favour this approach, it can represent a problem in terms of public democratic procedures in governance structures.

Self-regulation does not provide the same basis as state regulations in terms of accountability. It is true – as argued, for instance, by the Secretary General of ICC, Maria Livanos Cattai – that rules that are freely incorporated into contracts also are enforceable in court. However, most consumer “contracts” with sellers are not based on large voluntary bodies of provisions. Furthermore, very few consumer cases are taken to court. The costs both economically and otherwise may be too high.

But these arguments in favour of state regulation do not exclude self-regulation. Probably the best solution is a mixture of self and state regulation. Therefore, the question is not whether there should be self-regulation but where its limits should be set. It would be foolish to reject positive self-regulatory measures. A situation with an industry that reluctantly abides by the minimum rules laid down by the state is in

no way desirable. As, for instance, in the field of social insurance (life insurance, pensions and health insurance, etc.) where there is presently much interest in the social responsibility of industry, positive initiatives should not be rejected. The two types of regulation are by no means mutually exclusive.

National vs. international Regulation

In the EU the European Commission has proposed a new directive on electronic commerce in order to ensure harmonized rules within the EU on authenticity, contractual issues and marketing practices such as spamming. According to this directive, the official place of e-business will be where the operator is registered for tax or company law purposes irrespective of where web-sites, mail boxes or servers are situated. Furthermore operators will be obliged to disclose basic information such as name, address, trade register number, etc. In order to avoid spamming, commercial communication by e-mails must be made clearly identifiable so they easily can be deleted. A political agreement on this directive was reached in December 1999 and will contribute to a more transparent consumer protection regime within the EU.

In the EU and EFTA (European Free Trade Agreement) countries, the Lugano/Brussels Convention allows consumers to raise cases either on the basis of their home country laws or on the basis of the appropriate laws in the home country of the seller. This rule has obvious advantages for consumers and is generally recommended by consumer organizations. However, such a solution raises a number of problems in terms of technical trade barriers and extra-territorialism including enforceability of decisions. It is, therefore, unlikely that this convention can be extended beyond European borders.

However, one should be cautious about the mixture of arguments dealing with desirability and feasibility at the same time. International regulation is not an entirely new thing. International regulation is already practised in other areas through binding agreements, e.g. through the WTO. While international business representatives and the US government have opposed any mandatory international public rules in the areas of consumer protection and privacy, they have been strongly in favour of establishing an international regime for the protection of intellectual property rights.

This in itself should not be criticized, but it shows that it is not primarily a question of the difficulty of establishing an international legal regime. The intellectual property rights field is perhaps one of the more difficult areas in which to enforce international rules. The reason that international business representatives, in spite of these difficulties, still want to install an international legal regime is that they have crucial interests at stake here. This illustrates that it is not only a question of difficulties but also a question of desirability and political will. Often arguments consist of a mixture of feasibility and desirability.

There is no easy solution to the problem of establishing international rules in the e-commerce area. The initiatives of ICC with regard to international guidelines and model contracts, etc. are highly commendable. Very important is also the UNCITRAL model law on electronic commerce. Initiatives in the OECD will, furthermore, have a large impact. The OECD is not an organization, where binding agreements can be taken. Nevertheless, it is often used as a forum in which member states can develop common political positions. A Global Action Plan for Electronic Commerce prepared by business with recommendations for governments was presented at the Ottawa meeting in October

A proposed EU directive on e-commerce aims to clarify issues such as the place of business of electronic commerce firms, and proposes harmonized rules on authenticity, spamming, etc.

Agreements are now in place to allow consumers to take up cases either on the basis of the laws in their own country or those of the seller, although there are doubts about the applicability of this in practice


1998. A revised version of this plan was issued in October 1999. The plan is very much focussed on self-regulation, and includes a survey of self-regulating initiatives taken on the electronic market place.

However, none of these organizations have the competence to establish legally enforceable rules. The WTO could be such an organization, although its recent travails would need to be kept in mind before charging it with more tasks. It should be possible, as in connection with the basic telecommunications deal, to have a regulatory model attached to an agreement on electronic commerce setting out the basic minimum requirements for (among other things) consumer protection.

Conclusion

The regulatory problems created by the Internet are not entirely new. International transactions, of course, already took place before the Internet was born. However, in the physical market, it is always easy to distinguish between domestic and cross-border transactions. Moreover, cross-border transactions are mainly

business-to-business transactions, while business-to-consumer transactions are far less frequent. The international electronic financial market is a good example of this. Electronic transactions have played a role in the development of more liberalized currency markets, but the actors dealing in the market are all professionals and consumer protection is not an important issue. While professional dealers can be expected to have knowledge about different types of national regulations, it will be difficult to demand the same knowledge from private consumers.

National borders are related to control over physical space. Lawmaking requires some mechanism for law enforcement, which depends on the ability to impose coercive sanctions on law-breakers. International institutions do not exercise the same physical control and international law making can only be done with the consent of national states. This makes international lawmaking a very complicated and slow process, in sharp contrast to the dynamic Internet market. Even at the national level, national legislation may find it difficult to keep pace with technical developments, making control at international levels yet more elusive. 

Keywords

electronic commerce, electronic market, consumer protection, national and international regulation, self-regulation

References

- Cattai, M.L., (99): *Let commerce shape the future of the Net*. CommunicationsWeek International, No.1, February 1999.
- CEC, *A European Initiative in Electronic Commerce*, COM(97) 157, 1997.
- CEC, *Commission proposal for European Parliament and Council Directives on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions*, 1988.
- CEC, *Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market*, COM (1998) 586 final, Brussels, 1998.
- Danish Ministry of Business and Industry, *The Legal Protection of Consumer Rights in Relation to Transnational Digital Network*. Copenhagen, 1997.
- Falch, M., Henten, A., and Skouby, K.E., *Consumer related Legal Aspects of the Information Society, the Case of Denmark*. In Human Choice and Computers, IFIP-TC9 5th World Conference. Geneva, 25-28 August 1998.
- OECD, *Business-to-Consumer Electronic Commerce, Survey of Status and Issues*. OCDE/GD(97)219. Paris, 1997.
- OECD, *Gateways to the Global Market – Consumers and Electronic Commerce*. OECD, Paris, 1998.
- OECD, *Electronic Commerce: Prices and Consumer Issues for Three Products: Books, Compact Discs, and Software*. DSTI/ICCP/IE(98)4/Final, Paris, 1998.
- OECD, *A Global Action Plan for Electronic Commerce Prepared by Business with Recommendations for Governments*. Ministerial Conference, Ottawa, Canada, 7-9 October 1998 (2nd edition, October 1999).
- OECD, *A Borderless World: Realising the Potential of Global Electronic Commerce*. Ministerial Conference Ottawa, Canada, 7-9 October 1998.

Contacts

Morten Falch, CTI/ DTU

Tel.: +45 45 25 51 77, fax: +45 45 96 31 71, e-mail: falch@cti.dtu.dk

Anders Henten, CTI/ DTU

Tel.: +45 45 25 51 76, fax: +45 45 96 31 71, e-mail: henten@cti.dtu.dk

About the authors

Morten Falch has a Master degree in economics and a bachelor in Mathematics. He holds a Ph.D. and is an Associate Professor at the Center for Tele-Information (CTI) at the Technical University of Denmark. His main areas of research are: Telecommunication regulation and policy, telecommunication economics, internationalisation of telecommunications, socio-economic implications of information and communication technologies and trade in services.

Anders Henten has a Master degree in communications and international development studies. He holds a Ph.D. and is an Assistant Professor at the Center for Tele-Information (CTI) at the Technical University of Denmark. His main areas of research are: Regulation, internationalisation and standardisation of telecommunications, socio-economic implications of information and communication technologies, trade in services, and development policy.

Creating a personal relationship with customers is an essential part of e-commerce; electronic business is therefore unthinkable without the processing of personal data

Frameworks for Privacy in the On-Line Environment

Jos Dumortier & Caroline Goemans, *ICRI*

Issue: The absence of legal security for business and the lack of transparency for consumers may hinder the development of a global digital economy. The European data protection directive of 1995, which is currently being transposed by the Member States into their national law, provides a general legal framework for the protection of individuals with regard to the processing of their personal data. Yet, there is still an urgent need for well-balanced and practical rules on this issue.

Relevance: Any such rules would benefit from self-regulation and consensus among all interested parties. Over the years a whole set of mechanisms for such a consensus-building process have been developed and refined in the context of standardization. In considering the standardization tool-set in the discussion about privacy and electronic business, particular attention needs to be paid to certain conditions that any successful self-regulatory regime will have to fulfil.

Introduction

Electronic business is unthinkable without the processing of personal data. Despite the explosive increase in the number of Internet users, according to Forrester Research, on 70 percent of Web sites only 2 percent of the Web surfers turn into buyers (Anwang, 1999). The main challenge for an online merchant is therefore to establish a personal relationship with the Web site visitor and to adapt the goods or services offered precisely to what the potential customer is likely to be interested in. To quote one editorialist: "The battle is not for eyeballs; it's a battle for trust, hearts and minds" (Miller 1999).

Personalization and privacy protection: keys to successful electronic business

The success of electronic business largely depends on the potential to present the right products and services to the right person. Modern Web technology makes it possible to create a customized environment for every individual customer. The online store displays only commercial messages perfectly matching the customer's profile.

So far we have probably only just scratched the surface of Web personalization's potential. In the near future, we can expect more *integrated* personalization, where the customer profile is maintained across all sales channels, and where

improved techniques are used for managing customer and product categories and for offering real-time incentives and promotions.

This kind of customization will only be possible if the customer is satisfied that any personal data communicated by him or collected in the background will not be misused for other purposes. A serious impediment to the further development of electronic commerce is the fear of consumers that the information they communicate (or generate) will be used in ways they would not authorize. Almost eighty-seven percent of U.S. respondents in a recent survey of experienced Internet users stated that they were somewhat or very concerned about threats to their privacy online (Cranor, 1999).

Personal data protection law in the European Union

It is clear that the processing of personal data in the context of electronic business has to remain within the limits of the law. In the European Union the principal legal text on this issue is the European Data Protection Directive of 1995. The directive contains a series of general rules that had to be transposed by the Member States into their national law before the end of October 1998 (EC Directive 1995).

The Directive pursues two closely linked objectives: on the one hand to ensure the rights of the individual with regard to the processing of his personal data and, on the other hand, to enable business to benefit by ensuring that such data can move freely within the EU. It has to be taken into account in this respect that the Directive only provides a framework and that much of the effectiveness of the protection of personal data will depend on the various implementation mechanisms.

The consequence of the European Directive is that data protection principles have to be

embodied in comprehensive law. These principles are applicable to all sectors of economy and need to make it possible for non-compliance to be penalized and for individuals to have a right of redress. The law has to incorporate additional procedural mechanisms, such as the establishment of independent supervisory authorities with monitoring and complaint investigation functions.

For a commercial Web site owner in Europe, it means that personal data of potential customers cannot be processed without taking into account his national data protection legislation. In this legislation he will find a comprehensive set of general rules and procedures, directly derived from the European Directive. It remains, however, a delicate matter to translate this general legal framework into specific guidelines directly applicable to the context of electronic business.

Therefore the Directive itself states that the Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct in order to facilitate the application of the Directive. These codes should take account of the specific characteristics of the processing of personal data carried out in certain sectors, and respect the national provisions adopted for its implementation. In the philosophy of the Directive, the particular rules on personal data protection with regard to online commerce have to be developed into a specific code of conduct.

The U.S. approach

The United States has approached the regulation of the use of personal information in a different way. European laws attempt to protect individual rights more or less in a preventive manner, and give the state an active role as the overall authority, at least as far as the general legal

In the future online stores will make increasing use of profile information to customize the environment to individual customer

The 1995 European Data Protection Directive seeks both to ensure the rights of the individual concerning his or her personal data and to enable the free movement of such data within the EU

The Directive intends codes of conduct to be used in a way that takes into account the differing national and sectoral practices

In the US the approach taken to the privacy issue has opted for low levels of state intervention

The Federal Trade Commission has been carrying out surveys to assess the effectiveness of self-regulation of on-line privacy. These have shown that in many cases widely accepted fair information principles are not being addressed

framework is concerned. In contrast, US regulatory philosophy is based more on a philosophy of minimal state intervention. In order to minimize state intrusions in information flows, the United States approaches the regulation of personal data processing more through attention to discrete sector and sub-sector activity. Comprehensive law is fairly rare (Schwarz & Reidenberg, 1996). Nonetheless, the practical effects of the contrast between the approaches on both sides of the Atlantic should not be overstated.

A number of US trade associations have promulgated fair information practice guidelines to promote standards for the treatment of personal information in specific industries. Companies have established policies and practices, including internal codes of conduct and procedures offering supplementary protection. A growing number of Internet Web sites display a button referring to one or more pages explaining the site's privacy policy.

In 1998, the Federal Trade Commission (FTC) asked trade associations and industry groups to voluntarily submit copies of their on-line information practice guidelines and principles. Examination of those guidelines proved that they did not address all the core fair information practice principles that are widely accepted in the US (FTC, 1998).

The FTC also examined the practices of commercial sites on the World Wide Web to determine whether self-regulation is an effective means of protecting consumer privacy on the Web. The survey, conducted in 1998, of over 1400 Web sites revealed that industry's efforts to encourage voluntary adoption of the most basic fair information principle – notice to the customer that the personal data collected on the Web site will be shared with others for direct marketing purposes – had fallen far short of what is needed to protect consumers. Consequently, the FTC concluded in its

1998 Report that in the light of its findings, substantially greater incentives were needed to spur self-regulation and ensure widespread implementation of basic privacy principles.

In its 1999 Report the FTC stated that the results of two new surveys of commercial Web sites suggested that online businesses were providing significantly more notice of their information practices than they were in 1998. However, the new results showed that, despite these efforts, the vast majority of even the busiest Web sites had not fully implemented certain fair information practice principles. Problems concerned mainly the provision of reasonable access for online consumers to personal data collected from and about them, and the maintenance of adequate security for that information (FTC, 1999). Therefore the FTC decided to establish an Advisory Committee on Online Access and Security (ACOAS). The purpose of the Committee is to provide advice and recommendations to the FTC regarding implementation of these practices by domestic commercial Web sites. An issue to debate in the context of ACOAS is whether the implementation of all the fair information practice principles will be enforceable without the enactment of comprehensive legislation (FTC, ACOAS).

International flow of personal data

One of the further objectives of the European Data Protection Directive is to prevent the abuse of personal data of EU-origin in third countries where adequate protection is not ensured. Thus, the Directive not only regulates processing personal data in the EU but also includes provisions on the transfer of data to third countries. The basic principle is that Member States should permit this type of transfer only when the third countries concerned ensure an "adequate" level of protection. Because the US

relies largely on a sectoral and self-regulatory approach, rather than on comprehensive legislation for effective privacy protection, many US organizations have expressed uncertainty about the impact of the "adequacy" standard on personal data transfers from the EU to the US.

To provide a more predictable and cost-effective framework for such data transfers, the US Department of Commerce therefore issued "safe harbour principles" under its statutory authority to foster, promote and develop international commerce. The principles were developed in consultation with industry and the general public. They are intended solely for use by US organizations receiving personal data from the EU and only for the purpose of qualifying for "safe harbour" status and the presumption of "adequacy" this creates. US companies could come within the safe harbour by self-certifying, on an entirely voluntary basis, that they adhere to these privacy principles.

At present, the safe harbour principles are still under discussion. One of the main issues remaining to be clarified is the precise role that the various US bodies involved will play in enforcing the safe harbour principles. For the European Commission, a prerequisite under the safe harbour principles is that the mainly self-regulatory approach is enforced effectively. Another issue is the US request for a grace period during which US organizations would have time to prepare themselves for entry into the *safe harbour*.

Seals and other privacy protection tools and services

Even in the US there is a growing understanding that the mere publication of some self-developed privacy policy principles on the Web site is not enough to increase the confidence of the online

consumers about the protection of their personal data. An average individual consumer is generally unable to evaluate the quality of a company privacy code and doesn't have any means of ensuring the company actually complies with its stated principles.

One possible answer to this concern is to issue "seals" certifying the Web site's information policy for users' personal information. Companies can submit their privacy policy to a more or less neutral third party and receive a "trustmark" if this policy meets certain criteria. What is less clear, however, is how effectively the compliance of the company with its privacy principles will be systematically controlled. The companies themselves also remain responsible for the development of their own privacy policy. In practice some of these policies are very obscure and difficult to evaluate by an ordinary Web user.

Some Web-based services therefore offer e-commerce businesses the ability to outsource the creation of a customized privacy policy. Other services deliver not only seals or trustmarks but also include an online mediation service to which customers can address complaints in case of non-compliance.

Little by little privacy protection tools and services are developing into a real e-business of their own. A service on the Web, for instance, screens privacy policies for a vast array of websites and assesses them according to a four-star system. A site with four stars – *contact (only) with permission* – means that this site does not contact you without your explicit permission and does not share your personally identifiable information with third parties. On the other hand, if a Web site receives only one star, consumers know that this site may share their personally identifiable information without their explicit permission.

The European Data Protection Directive also seeks to control the flow of personal data to third countries, only permitting transfers when the country concerned offers adequate safeguards

Differing standards for data protection in the US and EU may be tackled by individual organizations being able to qualify for "safe harbour" status to satisfy EU requirements

One approach to the problem of public confidence in on-line privacy is the issuing of "seals" or "trustmarks" independently certifying a site's compliance with a code of practice

Other approaches include users managing their own profiles and keeping their data private. For those wishing to disclose nothing at all there is a burgeoning range of anonymity services

Another recently launched service seeks to enable consumers to own their own profile and to keep their consumer data private and use it for their benefit, convenience and profit. A first phase in the rollout of the system gives the provider the authority, on behalf of the customer, to order direct marketers to remove the customer's name and personal information from their databases. After this opt-out process, the service starts to act as a personal broker for the online distribution of profile information on behalf of the individual customer.

There is also an increasing range of anonymity services on offer, combining the use of pseudonyms, strong encryption and network facilities. One recent proxy-based service lets users both block information that typically gets sent to a Web site and create aliases for site registration. Another service sends the user's Internet traffic through a series of privacy-enhancing detours and invites the user to create several pseudonyms to use for different online interests. The user alone decides how much - or how little - personal information to disclose with each pseudonym and how many different pseudonyms to create.

To summarize, a new industry is springing up with services helping online consumers to get better control of the use of their data. Practically every week new privacy protection services or tools are announced. The wide variety of services and the constant development of new creative ideas in this domain is undoubtedly a very positive development. However, as privacy becomes an industry of its own competing standards, guidelines, and systems may make consumers and Web publishers alike throw up their hands in frustration. As in every other sector creativity, innovation and competition could benefit from a certain degree of standardization (Lemley, 1996).

The role of standardization

More than in any other area, electronic business has come to depend on standards to ensure the interoperability and ubiquitous adoption of the technology used. Clearly, both businesses and users can participate more effectively when systems work together, and the standardization process can make a significant contribution to achieving this success. Individual consumers will feel more confident when systems operate seamlessly, efficiently, securely and effectively through common approaches. This objective is the driver for one of the standardization initiatives in the context of the Internet, referred to as "P3P". The Platform for Privacy Preferences (P3P) is an initiative of the World Wide Web Consortium (W3C) enabling users to negotiate with a Web service on the use of personal information. The negotiation is steered by a standardized procedure (W3C, 1999).

This kind of standardization is not necessarily an obstacle for *innovation or competition*. On the contrary, one has only to look at the highly competitive mobile telephony market in Europe to

Box 1: What is P3P?

As the first step towards reaching an agreement, a service sends a machine-readable proposal in which it declares its privacy practices. The set of statements that may be made in a proposal is defined by the harmonized vocabulary, which is a core set of information practice disclosures. The statements are automatically parsed by the user's Web browser and compared with privacy preferences set by the user. Thus, users need not read the privacy policies at every Web site they visit. If a proposal matches the user's preferences, the Web browser may accept it automatically. If the proposal and preferences are inconsistent, the browser software may prompt the user, reject the proposal, send the service an alternative proposal, or ask the service to send another proposal.

see how standards and competition can go hand in hand. Standardization could create a more transparent market for privacy protection services for the consumer. It would improve their capability to compare the various offers and make it easier for them to move from one provider to another. This could even lower the cost of access to the market and stimulate competition.

The standardization approach places emphasis on the strong networking capabilities of the "standards community". The aim is to take full advantage of these capabilities.


Conclusion

To make any standardization initiative successful, a certain number of conditions have to be fulfilled. A first condition for success is to invite all the interested parties to join in the discussion. This includes not only business and consumers, but also government representatives and data protection supervisory authorities. Secondly, a standardization initiative has to start with an open agenda. The discussion should not be fixed on one particular deliverable. Standardization has to be considered primarily as a working method.

Thirdly, it is important for all the parties to bear in mind at all times that everybody should always have something to gain. Each of the participating parties must have an incentive to continue the

discussion. Fourthly, and more specifically with regard to personal data protection and electronic business, the standardization initiative has to be considered as a complement to the existing regulatory framework (Swire 1996). It should help business to implement the legal rules more effectively and increase security for consumers.

In the fifth place, reducing complexity and facilitating privacy protection while enabling competitive electronic business should always remain the objective. Increasing complexity and introducing more bureaucracy is not a desirable outcome. Last but not least, standardization has to be considered as a continuing process. Standards are living documents and their flexibility is one of the main advantages in comparison to other forms of regulation.

Standardization is certainly not a "cure all" for privacy protection in the context of electronic business. It has to go together with privacy-enhancing technology and services and with government regulation or legislation. Any privacy-protection regulatory system should always have a fourfold aim: a) substantive rules guaranteeing the individual data subjects a high level of protection; b) a good level of compliance with the rules; c) sufficient support and help to individual data subjects in the exercise of their rights; and, d) appropriate redress to the injured party where rules are not complied with. 

Standardization could create a more transparent market for privacy protection services for the consumer. One initiative in this direction is P3P, the Platform for Personal Privacy

About the authors

Jos Dumortier is a full professor in law at the University of Leuven (Belgium) and the director of the Interdisciplinary Centre for Law and Information Technology (ICRI). As a consultant for the Belgian federal government, he has been very intensively involved in the transposition of the European data protection directive into Belgian law.

Caroline Goemans has been a practising lawyer and is currently working as a full-time researcher at the Interdisciplinary Centre for Law and Information Technology. With Jos Dumortier she authored a background paper on personal data protection and standardization on behalf of CEN/ISS.

Keywords

privacy, personal data protection, electronic commerce, self-regulation, codes of conduct, standardization

References

- Anwang, G., *The Stuff You Want*, PC Magazine, Vol. 18, N° 17, October 5, 1999, p. 103.
- Cranor, L.A., Reagle, J., and Ackermann, M., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, AT&T Labs Research Technical Report TR 99.4.3, 1999.
<http://www.research.att.com/projects/privacystudy>
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281, 23/11/1995 p.0031 – 0050.
http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html
- Federal Trade Commission (FTC/ACOAS), *Establishment of the Federal Trade Commission Advisory Committee on Online Access and Security and Request for Nominations*.
<http://www.ftc.gov/acoas/index.htm>
- Federal Trade Commission, *Self-Regulation and Privacy Online*, Report to the Congress, 1999.
<http://www.ftc.gov/reports/privacy3/index.htm>
- Federal Trade Commission, *Privacy Online: A Report to Congress*, 1998.
<http://www.ftc.gov/reports/privacy3/index.htm>
- Lemley, M., *Antitrust and the Internet Standardization Process*, 28 Conn. L. Rev. 1996, p. 1043.
- Miller, M., *E-Relationships Are Vital*, PC Magazine, Vol. 18, N° 20, November 16, 1999, p. 4.
- Schwartz, P., and Reidenberg, J., *Data Privacy Law. A Study of US Data Protection*, Michie Law Publishers, Charlottesville, 1996.
- Swire, P., *Self-Regulation and Government Enforcement in the Protection of Personal Information*, Report submitted to the National Telecommunications and Information Administration (NTIA), 1996.
<http://www.acs.ohio-state.edu/units/law/swire1/psntia6.htm>
- US Department of Commerce, *Elements of Effective Self-Regulation for Protection of Privacy*,
<http://www.ecommerce.gov/staff.htm>
- World Wide Web Consortium, *Platform for Privacy Preferences (P3P)*, Working Draft 26 August 1999.
<http://www.w3.org/p3p>

Contacts

Jos Dumortier, K.U. Leuven, ICRI

Tel.: +32 016 32 51 49, fax: +32 016 32 54 38, e-mail: jos.dumortier@law.kuleuven.ac.be

Caroline Goemans, K.U. Leuven, ICRI

Tel.: +32 016 32 52 73, fax: +32 016 32 54 38, e-mail: caroline.goemans@law.kuleuven.ac.be

E-commerce and the Encryption Debate

Stuart J. D. Schwartzstein, *LSE*

25
Information and
Communication
Technology

Issue: Although the development of electronic commerce requires means of protecting the integrity of transmitted or stored data, one of the most important means of protection, encryption, is controversial. The potential misuse of encryption means it raises a complex set of issues related to questions of regulation of electronic means of communication and content, to privacy and the role of government.

Relevance: Much of the future of electronic commerce will depend on how encryption is dealt with by governments, the public and industry. The security of communications and of operating systems will also depend to a considerable extent on how well a range of concerns are addressed.

Introduction

The future of both electronic commerce and electronic communications and computer storage of data will depend to a large extent on the ability of systems to protect information and control access, ensure the integrity of communicated or stored data and provide assurances of authenticity. These needs existed in the pre-computer age and appropriate solutions were developed for them. However, the speed and global reach of the digital economy makes these issues more pressing. In particular, if electronic commerce is to flourish, users must trust the systems and be confident that they are not running unacceptable risks (the issue of quantifying risks is itself, however, beyond the scope of this article). It should be underscored that the very high speed of electronic systems and their ability to send large amount of data quickly further exacerbates the need for protection.

Encryption

Although some regulation to protect information and limit access, when consistent with law and widely applicable (such as that regarding fraud), can be of great value, regulation alone, whether by government or by industry (self-regulation), cannot address data protection and information infrastructure protection needs adequately. Encryption is the most practical means of preventing unauthorized or unwanted access to data and information stored on computers or communicated over computer networks and telecommunications systems. Encryption is also a means of ensuring the integrity of data or information and the authenticity of the source. Perhaps most importantly, encryption permits individuals to protect their own data and information, rather than relying on others or relying on legal systems to deal with problems. In addition, as encryption can be integral to the data/information, –rather than a peripheral

If electronic commerce is to flourish users must trust the systems and feel confident that personal data is safe

*Encryption is a means
of ensuring the
integrity and secu-
rity of data and the
authenticity of
its source*

*Once the preserve
of governments,
encryption has now
become common in the
private sector and
this trend is likely
to continue*

defence— it is in some ways more reliable than “firewalls” and gives greater guarantees. Encryption, of course, can also be used to protect systems operating over private networks.

In parallel with the information revolution, encryption has undergone revolutionary changes in recent years¹. These changes include:

- Use of encryption is no longer limited to military, diplomatic and intelligence purposes but is now used widely by both businesses and individuals. Indeed, it is now recognized as being critical to the use of computer and communications technologies for a wide range of purposes – including, of course, those necessary for electronic commerce.²
- Expertise in encryption is no longer nearly entirely found within military and government agencies. Government is no longer the sole possible employer for cryptographers –and, indeed, it seems that for present-day cryptographers and experts in encryption, government positions are considerably less attractive than those in the academic world, software firms and other businesses.³
- The development of public-key cryptography has made use of encryption both easier and more practical for a variety of applications
- *Strong* cryptography (i.e., encryption which cannot, feasibly, be cracked⁴) is widely available, despite the best efforts of a number of governments –most notably that of the US government –to place restraints on its proliferation. A recent study⁵ indicates that there are at least 805 hardware and software products incorporating encryption capabilities produced in 35 countries outside the United States; of these 167 were found to use strong encryption. The study further noted that in

general the quality of US and non-US products is comparable.

Given the importance of encryption for a wide range of uses, including electronic commerce, it is likely that there will be strong commercial demand for encryption in the future. This will likely result in more progress in the encryption field being made in the private sector than in government in the future. As with advances in most ICT-related fields, now that we are well beyond the “infant,” high-risk stages of development, it will be the commercial sector which will be responsible for new developments in encryption technologies and, indeed, other means of data protection. Furthermore, in addition to the private sector being better able to attract the best, brightest and most innovative cryptographers, software programmers and thinkers in the field, there are now vast amounts of capital available for ventures, including some which entail considerable risk.⁶ This includes, of course, technologies for the protection of systems and information. The dramatic growth and development of electronic commerce, which we are witnessing now, and keen interest by the business sector⁷ makes it clear that what is needed in this sector, including (most importantly) encryption, will become available. The strength of market forces and the proliferation of skills and products make that certain.

Proposals for “Key escrow”

The widespread availability of strong encryption has and will continue to have implications for government and, within governments, particularly those areas dealing with law enforcement and national security. For a number of governments it remains difficult to envisage both loss of control over encryption as well as loss of abilities – such as interception – which they have enjoyed for a number of years. There

are real and important concerns about the use of encryption by criminal groups and the implications of the inability to intercept communications relevant to threats to national security –and to national economic well-being.

As a consequence of governmental concerns over unimpeded use of strong encryption, several governments –again, most notably, the US Government– have made attempts to restrict and regulate its use (in particular so as to retain an ability to intercept communications and access stored data). Export controls on encryption are widely seen as an important tool in restricting the use of encryption both outside the US and domestically.⁸ But the US Government has also attempted to gain acceptance of crypto systems which permit access by government (the “Clipper Chip” proposal was perhaps the best known). This was seen by those advancing such proposals as providing government with the means of access when deemed necessary while, at the same time, permitting the public (most importantly, the business sector) with the necessary means of protection of communications, data and systems. Such attempts, however, have failed to gain acceptance either in the United States or elsewhere. Over the last three or four years there have emerged a number of proposals for “key recovery,” “key escrow” and “trusted third party” encryption. These are schemes which would permit government access to encrypted communications or stored data, through the holding of encryption keys by a special agency or a third party or through another mechanism permitting decryption. The proposals have not only failed to gain acceptance in the US, the UK and elsewhere, but have been the subject of an at times acrimonious debate.

However sympathetic one might be towards the objectives of government in this area – and it must be said that government seems to get little sympathy from most of those who have been engaged in the

debates over encryption – it has become clear that “key recovery,” “trusted third party” and other similar schemes are not likely to succeed, for political, economic and technical reasons.

The political reasons include the fact that – particularly in the US – government has come to be seen as more an adversary than representative of the interests of those most concerned with encryption (and data protection). There is widespread distrust of government and there remains a sense on the part of most that the government (again, mostly, in the US, but elsewhere as well) is interested in restricting or controlling use of encryption. Trust, which is critical to any kind of government or government-sponsored key recovery scheme, does not exist at this time. Nor, in the case of the US, has the current approach to data protection by government been one which is seen as engendering trust.⁹ There exists what one might call a “social/political gap” or different architectures, with stark differences in views on encryption between most individuals familiar with it outside government circles.

The difficulties of setting up and operating schemes for trusted third party or key escrow across national borders are both technical and political. The needs and uses of encryption are not easily contained (or contained at all!) within one country’s borders and thus any scheme would have to entail a high degree of international co-operation, some of which may be lacking given the nationally-based activities of various intelligence agencies. Differing views, too, of privacy, the role of government and rules of evidence are also likely to complicate international cooperation in this area.

As noted in an important report on the subject published last year, “No one has yet described, much less demonstrated a viable economic model

Over the last few years a number of proposals have emerged for “key recovery,” “key escrow” and “trusted third party” schemes which would permit indirect government access to encrypted communications or stored data

Nevertheless, it has become clear that “key recovery”, “trusted third party” and other similar schemes are not likely to succeed, for political, economic and technical reasons

Apart from the complexity and costs of such schemes, one of the main objections is the potentially damaging consequences of the theft or disclosure of the keys

to account for the true costs of key recovery.”¹⁰ The report went on to note that “key recovery as envisaged by law enforcement will require the deployment of secure infrastructure involving thousands of companies, recovery agents, regulatory bodies and law-enforcement agencies world-wide, interacting and co-operating on an unprecedented scale. This, of course, would be very expensive.” Other costs, including design costs and end-user costs would also have to be considered, making for what would likely be an extraordinarily expensive venture.

The technical objections to such key recovery schemes, as set forth in the report, include a high degree of risk and their sheer complexity. As noted by the report: “The failure of key recovery mechanisms can jeopardize the proper operations, underlying confidentiality and ultimate security of encryption systems; threats include improper disclosure of keys, theft of valuable key information or failure to be able to meet law enforcement demands. It also notes that “A fully functional key recovery system is an extraordinarily complex system with numerous new entities, keys, operational requirements and interactions. In many cases, the key recovery aspects of a system are far more complex and difficult than the basic encryption functions themselves.”

While key recovery, key escrow or trusted third party schemes are likely to be abandoned, it is also likely that debates over encryption will continue at least for some years more. The use of encryption will become much more common, but it remains unclear how governments will come to terms with it and adapt to their inevitable loss of the ability to intercept communications.

Apart from its impact on governments, it is likely that widespread use of encryption will also have implications for a number of areas which are subject to national laws and regulation –primarily

civil, rather than criminal codes— including intellectual property rights, product safety and liability, contractual obligations, privacy, libel and competition/anti-trust issues.

However, although we can expect the battle over encryption to continue over the next few years, efforts to control it are unlikely to succeed. Moreover, the increasing realization that the extensive use of encryption is essential if electronic commerce is to prosper is shifting the focus of the debate, given national stakes in this emerging business sector.

Concluding remarks

If the issues of access and data protection are inherently complex –necessitating consideration of systems architectures, as well as social, political and economic issues– the issues raised by strong encryption are no less so. The debates over encryption are at the heart of a number of larger questions, including privacy, protection of data and information, regulation by government, security and those issues over content and access to various kinds of content. When addressing the issues it may be worth bearing in mind that it may ultimately prove impossible to reconcile all possible viewpoints. Nor can we expect to be able to construct systems that can meet all the disparate needs at the same time. Moreover, these needs will change in unpredictable ways as technology advances and the economic, cultural and political context evolves. Perhaps the most important first step we can take is to delineate and re-think our goals and objectives and then give thought to what architectures are most appropriate and effective.

By its very nature encryption is difficult to regulate, and even its prohibition under the strictest regimes may be circumvented by steganographic¹¹ techniques which can elude

detection where cryptography may raise suspicions (and are not themselves considered cryptographic techniques). Attempts at regulation –such as proposals for mandatory key escrow arrangements– have not only met with opposition, but have been judged highly impractical by those with the requisite technical expertise to make informed judgements. Those who would regulate have, therefore, sought recourse to stratagems such as restrictions on exports of encryption software and hardware. But basically it is not so much encryption itself which governments wish to regulate, but the encrypted *content*. It is not likely that many would care if encryption were used exclusively as a means of protecting operating systems or hardware. But there is

concern, particularly by governments, that the content that is encrypted is either dangerous to society or to governments –and the concerns range from those over sexually explicit material (particularly where children are concerned) to material that is deemed seditious or part of criminal activity to that which is seen as inimical to national interests.

Given the importance of protection of information and restrictions on access for electronic commerce and much use of networked systems, the problems posed by encryption will, if anything, become more prominent over the next decade. Governments, businesses and individuals will have a tough challenge in reconciling interests.

Keywords

encryption, electronic commerce, key recovery, key escrow, trusted third party

Notes

1. For example, Schwartzstein, "Export Controls on Encryption Technologies," SAIS Review, Winter-Spring 1996.
2. This point has been made and re-stated in any number of places. The importance of cryptography is noted, for example, in the June 1999 report on "Cryptography and Liberty 1999" published by the Electronic Privacy Information Center of Washington, D.C.
3. In the view of this writer, it will be the effects of expertise in cryptography going primarily to non-government sectors that will have the most profound effects. For the best and brightest cryptographers, employment with government agencies like NSA (in the US) and GCHQ (in the UK) is likely to be considerably less attractive than the private sector, not only because of salaries, but because government employment in this area requires in-depth security checks, imposes constraints on behaviour and offers little flexibility.
4. Or, if it can be cracked theoretically, cannot be done with resources or technologies currently available.
5. Hoffman, Balenson, et al. "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations, June 10, 1999, Cyberspace Policy Institute, George Washington University, Washington, D.C. (<http://www.seas.gwu.edu/seas/institutes/cpi>)
6. Interestingly, the CIA, aware that it is having difficulties in keeping up with the rapid pace of technological development, has set up an organisation called "In-Q-It, Inc." which is to provide some funding for ventures in Silicon Valley, as well as participate in others – as a means of giving the CIA something of a "window" on information technologies.

About the author

Stuart J. D. Schwartzstein

is a Fellow of the European Institute of the London School of Economics and Political Science and a consultant on a range of international relations issues. Until recently he was Associate Director for Science and Technology Policy at the US Office of Naval Research.

7. One has only to look at the market demand for shares of "internet" or electronic commerce businesses, the high price-earnings ratios and the extraordinary demand for initial public offerings to get an idea of the strong interest and, indeed, confidence that this will be an important area in the future.
8. But the actual effectiveness of export controls is open to debate. As the Balenson/Hoffman study confirms, the availability of encryption products continues to grow. It is arguable that the net effect of US export controls has been to stimulate the growth of encryption technology production outside the US.
9. The "safe harbour" principles for data protection, which the US has wanted accepted by the EU, are not seen by many in the US as providing adequate protection of personal data.
10. From "The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption" by the Ad Hoc Group of Cryptographers and Computer Scientists (which included Whit Diffie, Peter Neumann, Ron Rivest and Bruce Schneier amongst others).
11. Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present (<http://www.thur.de/ulf/stegano/announce.html>)

Contact

Stuart J. D., Schwartzstein, The European Institute, London School of Economics and Political Science
Tel.: +44 (0) 20 795 568 15, fax: +44 (0) 20 795 575 46, e-mail: S.Schwartzstein@lse.ac.uk

Alternative Paradigms for European E-commerce

Andrew McMeekin, Ian Miles & Jason Rutter, *PREST*

31
Information and
Technology

Issue: A new paradigm for e-commerce is being created not only around Internet and the Web but also around smart household technologies. However, the diffusion of new consumer technologies (such as digital TV and mobile telephones) and persistence of EDI systems suggest the importance of other access paradigms.

Relevance: As Internet and e-commerce use has largely been led by the United States it is tempting to assume a "catch-up" model for both business-to-business and business-to-consumer e-commerce. However, this is not the only scenario, and policymakers and entrepreneurs need to be informed about the socio-economic impacts of the alternatives.

Introduction¹

Electronic commerce involves the mediated purchases of goods, services, or other financial transactions, using digital information technology at both ends of the interchange. These two ends of the interchange are, furthermore, locationally separate. In **Business-to-Consumer E-commerce** the client is a member of the public; though this has attracted considerable media attention, currently the largest volume of activity by far is believed to be accounted for by **Business-to-Business E-commerce**. While there have long been experiments with teleshopping, and a steady growth of business interchanges using EDI (Electronic Data Interchange), it is the explosive growth of the World Wide Web that has finally

opened the floodgates for e-commerce. Despite security and speed concerns with the Internet, the Web has proved more amenable to use by new entrants, small firms and consumers than were earlier e-commerce formats like videotex and EDI.

In the late 1990s a remarkable explosion of stock market interest in Internet-related companies excited the financial community (particularly in the US). Market forecasters also responded by predicting that huge volumes of consumer and business purchasing would be transacted online within a very few years. However, these forecasts are largely based on extrapolating the recent Web successes, and we must be cautious about assuming that Web-based e-commerce will provide the universal, or even the dominant, framework, for future e-commerce.

Despite security and speed concerns with the Internet the Web has proved more amenable to use by new entrants, small firms and consumers than were earlier e-commerce formats like videotex and EDI

In the early 1980s Videotex services, like the UK's Prestel and the much more widely diffused French Minitel system were already providing a form of e-commerce

EDI has been in use for over two decades but adoption has been slower than anticipated.

The next generation will probably be web-based and integrated with other web services

Box 1: What is EDI?

EDI is computer-to-computer exchange of structured data between two or more companies, sent in a form that allows automatic processing, with no manual intervention.

It is relevant to any business that regularly exchanges information such as client or company records, but is especially relevant when they send and receive orders, invoices, statements and payments.

EDI remains the dominant term in the UK for electronic trading, although some people consider the term electronic data interchange to be too narrow to describe the full potential of electronic trading. Electronic Commerce (EC) encompasses techniques such as PC-based fax and e-mail, as well as EDI.

Source: (Department of Trade and Industry, 1997, p3)

EDI and the Internet

Businesses have for some time been proceeding with a range of efforts to institute inter-firm communications. In the US there was automated transfer of large routine transactions in the automobile industry as early as the 1960s. A number of bodies were established to deal with issues of exchanging trade data – e.g. the TDCC (Transportation Data Coordinating Committee), and the well-known SWIFT (the Society for Worldwide Interbank Financial Telecommunication). As business use of computer-communications grew, there was an emergence from the 1970s of Value Added Networks (VANs), offering sophisticated computing and data transmission services. In the early 1980s Videotex services, like the UK's Prestel and the much more widely diffused French Minitel system - were already being used for not just to access information or chat to like-minded people, but also

to make bookings and reservations, ordering goods and services, and the like. This period also saw the first major expansion of EDI, with government promotion and intergovernmental standardisation efforts underway in many industrialized countries.

The diffusion of EDI has, however, been considerably slower than most of its proponents ever anticipated, even in those sectors for which the technology seems to be particularly suitable. The number of companies using EDI has risen steadily over two decades: estimates diverge, but suggest that the number of worldwide users in 1996 probably falls between 80,000 (Fletcher, 1997) and 150,000 (Gartner Group). In business-to-business transactions, EDI is likely to retain significant

Box 2: Forms of Internet EDI

At present, there are two main forms of "Internet EDI":

- **Mail-based EDI.** Here, the functions of the traditional VANs are substituted by Internet email, reducing the need of "intermediaries" for EDI communication, and allowing for more flexible solutions which could move toward the concept of an "open" EDI to which much more users could have access (ISO, 1994). In practice, for new users ISPs may be substituting for established VANs - and they are often far cheaper.
- **Web EDI.** This represents a more novel approach to EDI communication. It is particularly suitable for connecting a (large) partner to small firms which cannot (or do not wish) to integrate the EDI application into their internal systems, and for outreach to consumers. In such applications of the Web, EDI "documents" (typically orders) are manually entered onto user-friendly Web forms, and then directly translated into EDI messages.

Source: Senn, 1998

importance, not least because of the scope for standardized messaging and compatibility of database architectures. However, for business-to-business electronic commerce, Internet and related technologies may well be the key infrastructure of the future EDI, and the driving force for the further (and more rapid?) diffusion of that technology.

The major benefit of Web EDI is improved flexibility and user-friendliness but its development is likely to be accompanied by the diffusion of other new Web services (e.g. electronic catalogues and other applications integrated into the EDI transaction system). We can expect Internet and Web EDI to be more thoroughly integrated with other e-commerce and traditional EDI, implying development of more completely computerized transactions using Web pages or their analogues, though this will remain incomplete for a long time for a variety of practical reasons.

E-commerce Users and User Technologies

The emergence of the Web as a common platform for presenting and exchanging information has had a major impact on practically all telematics services. Online databases and news services, computer conferences and groupware systems, bulletin boards and messaging services, have widely recognized and "migrated to" Web formats. Even information services like Reuters, which only a few years ago was content to rely on its proprietary system and to argue that the Internet was an insecure playground for techno-freaks, is now offering Web-based services (and in the process developing new lines of business). The new media are even having an impact on electronic services more generally, as Internet telephony, music downloads, along with video and radio broadcasts and narrowcasts demonstrate.

To date, a major factor in the success of Web-based commerce and information supply has

been the fact that only part of the process is automated - i.e. that at the service supplier's end. At the consumer end, the PC effectively serves as a text-entry mouthpiece for a human agent, who is almost always acting in real time (or at best, preparing inputs offline that will be transmitted rapidly). Thus, the common language interface is familiar and organized in ways that draw on familiar experiences (like the "shopping basket" metaphor used in several Web sites). Neither party has to reorganize their knowledge of the product area to any great extent. This makes uptake of the services that much easier; and means that retailers are free to use their own frameworks for classifying and describing products, rather than having to use a standard scheme or protocol as in conventional EDI.

Despite the transformative importance of the Web, with its demonstrated potential for revolutionizing both business-to-consumer and business-to-business transactions, it may well be short sighted to see this Web-based paradigm for e-commerce as a stable one. Even before the eventual emergence of virtual reality systems, e-commerce could be revolutionized by the emergence of other, perhaps non-computer based, modes of access. Among these contenders are developments centred on already existing household technologies: the advent of WAP (Wireless Applications Protocol) standards for mobile telephony, and the rapid diffusion of digital TV, indicate paths available for the uptake and use of *e-commerce media*. Figure 1 shows the levels of mobile phone dissemination among Europe's top adopting countries. These levels of diffusion contrast sharply with Datamonitor's predictions that it will be 2003 before one in three households in Europe have internet access via a PC.

The non-PC media may use Web or Web-type interfaces. However, this is not the case for early developments in mobile phone e-commerce and

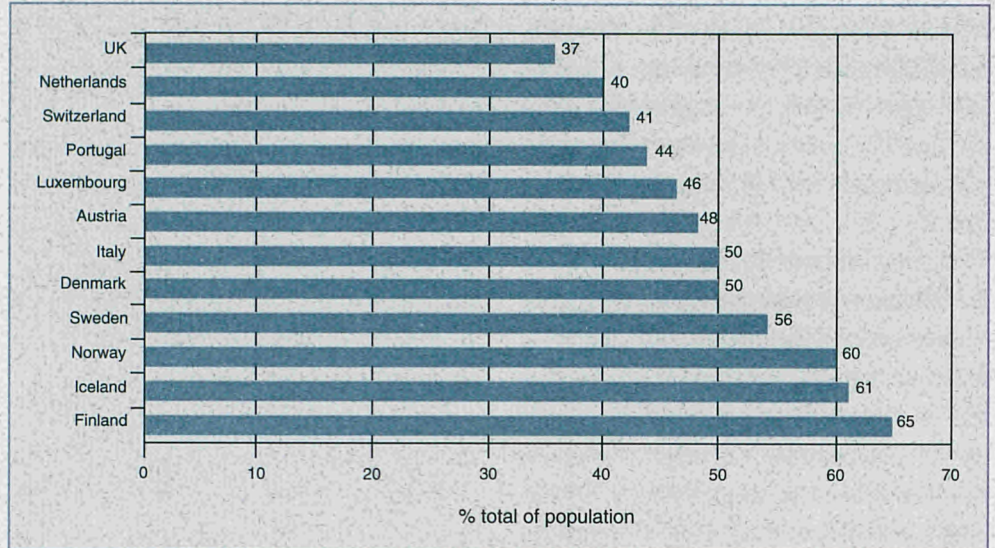
The flexibility of the Web means that retailers are free to use their own frameworks for classifying and describing products, rather than having to use a standard scheme or protocol as in conventional EDI

E-commerce using mobile phones and digital TV is not likely to have the same format as the PC-based variety

In addition to worries about security breaches and viruses, the crashes and outages to which the Internet is prone are a further cause for concern to users

Digital television providers are creating protected areas for their users, which they are populating with well-known and trusted retail organizations

Figure 1. Top European Mobile Phone Users: Dec 99



Source: FT Mobile Communications

digital TV (DTV) "Internet" services. Neither the handheld device nor the TV set is ideal for displaying Web pages à la PC. Further, increases in compression technology and bandwidth along with direct connection services point towards competing front ends for e-commerce access. In short, consumers and businesses are liable to have a range of choices about the interfaces to use to take part in e-commerce.

Decisions about whether to buy and from whom are based not solely on rational, technologically supported discourse. Factors like trust, status, and aesthetic and social sensibilities are involved in decisions about what technology to use, alongside considerations of access, convenience, usability and cost. Further, the integration of e-commerce facilities into existing household technologies will affect the relationship users have with the technology and the firms they buy from. For example, the continued development of e-commerce relies not only on the development of technology and production of information but the facilitation of online relationships. This has been

recognized by the more successful online retailers (and Internet Service Providers), who have developed a range of added-value attractions to encourage consumer involvement and attract people to visit their sites frequently. Discussions of trust often slip into arguments about security. The decentralized and open structure of the Internet means that it has been notorious for security breaches, ranging from computer viruses to hacking. Such problems are of obvious concern for e-commerce users, and there are thus major efforts to develop security mechanisms. Some of these mechanisms operate at the level of communication protocols, based for instance on encryption and return receipts. Others directly operate at the level of specific applications, such as specific systems for credit card payments. In addition to worries about the security of the Internet, there are concerns about its performance (especially its speed, but also its vulnerability to "crashes" and outages).

However, there are profound differences between security seen as a predominantly

technical issue, and the more social dimensions of trust. It is arguable that digital television will (in the short term at least) have the advantage when compared to the management of trust in Web-based e-commerce. DTV providers are creating "walled gardens" for their users – essentially large Intranets with little or no breakout to the larger Internet. These they are populating with well known and largely trusted retail organizations such as large high street retail outlets and banks. This brand recognition, together with the familiarity of the television and the assurances implied by their DTV provider, is intended help build a shopping environment which is more like a mall rather than the perceived chaos of broad Web-based e-commerce. The diffusion of e-commerce will also be driven by word of mouth as individuals share experiences (both positive and negative) with one another. In consequence it is also likely that social networks will provide a basis through which trust and confidence are improved. In other words, whilst access to the networked hardware is essential for e-commerce participation, it is not sufficient, without trust and confidence spread through interaction between consumers. This will be particularly important for sections of society with little or no experience in using information and communication technologies.

E-commerce: Beyond the US Model

Many commentators and research studies assume (whether implicitly or explicitly) that European countries will follow the US-model in e-commerce diffusion. This is particularly argued to be the case for the UK, which exhibits greater similarities to the US than the rest of Europe. The apparent received wisdom is that the USA is typically a few years ahead of Europe and that as our economic growth continues we should "catch up" with the US. For example:

"The UK has been experiencing growth rates comparable to growth rates in the US. With 15%

of the UK adult population having ever accessed the Web, penetration in the UK is at the same level now as in the US two years ago. The UK's Web penetration is growing at a faster rate than [both France and Germany]."

Lisbet Sherlock, European Marketing Services Director,
Ziff-Davies

However, numerous differences between US and European economies make identical take-up patterns unlikely. These include:

- different demographics
- different geographies
- different economic structures, including divergent retail sectors
- different historical experiences with other distance shopping modes, such as mail order, telephone-based commerce, the persistence of Minitel in France, etc.
- different systems of regulation of retailing,
- telecommunications and broadcasting systems, and infrastructures

The assumption of similar growth patterns for e-commerce also implicitly assumes that e-commerce in Europe will involve similar media to the US, especially the use of PCs and the Internet. However, European patterns of technological uptake can differ from those in the US, and not always in ways suggesting a European lag behind the US. For instance, several European countries are well in advance where it comes to the use of mobile phones. There are good reasons to believe that Europe's DTV markets will develop more rapidly than those in the US – and, as suggested above, this could ultimately be a greater driver of e-commerce than the Internet alone. Already, according to Market Tracking International (1998), more Europeans than Americans use interactive e-commerce applications specifically developed for digital TV.

Many commentators assume that Europe will follow the US-model in e-commerce and that the only difference is one of a time lag. However, European patterns of technological uptake could differ from those in the US

Conclusions

Dynamic change is underway, and there is no reason to assume that this will rapidly halt. A new paradigm for e-commerce may have been rapidly forged around the Internet and Web, but this could well be challenged by alternative technological platforms. The ramifications of these changes are yet to be thoroughly explored although scenarios can be constructed which help focus the issues raised here (including issues of social exclusion as well as those of technological adoption – see McMeekin, Miles & Rutter: 1999). What can be confidently predicted is that there will be continued demand for a wide and expanding array of supporting services, and that the rate and sophistication of their use will remain very uneven across sectors, regions and applications. Given this state of affairs the following points encapsulate the main issues that will effect changing paradigms for European e-commerce.

- Web presence and active e-commerce strategy are essential in most markets, and specific programmes may be necessary to raise awareness in lagging sectors and regions. Given the limited time and resources of many small firms, novel forms of business support may be needed if they are to participate actively in e-commerce, or respond to the challenges posed by larger firms that already have a foothold here.
- DTV, mobile telephony and other non-Web methods of access will become increasingly important, offering opportunities for European technology and service entrants. There is likely to be a continuing flurry of acquisitions and mergers here, across sectoral and national boundaries, which may pose challenges for industry and competition policy.
- Action and investment must be made on *Europe-specific* data rather than assuming patterns of development similar to the US.
- There may be entry barriers in the new media (especially DTV with its “walled gardens”) which are very different from those confronted in the free-for-all Internet environment, and competition and media policy will have roles to play here.
- A variety of consumer policy issues will become prominent, including data protection and confidentiality concerns, product liability, fair trading and advertising regulation. At present, there is wide divergence across EU members regarding consumer policy, which runs the risk of confusing potential consumers and retailers.
- There are opportunities for public services, voluntary organizations, and supporters of social inclusion and international development to make an impact on the world of e-commerce.
- It is likely that policy action will be required for organizational innovation aimed at providing training and other infrastructural support for SMEs and the socially excluded. For example, small traders and less affluent, disabled, elderly or geographically remote consumers that could benefit most from e-commerce, may miss out without such organizational innovation. 

Keywords

e-commerce, EDI, e-business, digital television, Internet, WAP

Note

1. This paper draws on studies recently carried out for the Retail and Consumer Services Panel of the UK's Foresight Programme (<http://www.foresight.gov.uk>)

References

- Bolisani, E., Scarso, E., Miles, I., and Boden, M., *Electronic Commerce Implementation: a Knowledge-Based Analysis*, International Journal of Electronic Commerce, vol. 3, n. 3, Spring 1999, p53-69.
- Department of Trade and Industry, *How EDI can work for you: a guide to implementing EDI in your business* London: DTI (URN 97/586), 1997. Available online at <http://www.isi.gov.uk>
- McMeekin, A., Miles, I., and Rutter, J., *Exploring the Effects of E-Commerce*, Report for Retail and Consumer Services Foresight Panel, 1999. Available online at <http://les.man.ac.uk/cric/e-commerce>
- Miles, I., "Cyberspace as Product Space" *Futures* vol. 29 No. 9 November 1997, pp769-790.
- OECD Working Party on the Information Economy, *France's Experience With The Minitel: Lessons For Electronic Commerce Over The Internet*, Paris, OECD, **DSTI/ICCP/IE(97)10/FINAL**, 1998.
- Senn, J.A., "Expanding the Reach of Electronic Commerce. The Internet EDI Alternative", *Information Systems Management*, vol. 15, n. 3 (Summer), 1998, p7-15.

Contacts

Andrew McMeekin, Ian Miles, Jason Rutter

ESRC Centre for Research on Innovation and Competition (CRIC), The University of Manchester & UMIST

Tel.: +44 (0) 161 275 7368, fax: +44 (0) 161 275 7361, e-mail: Ian.Miles@man.ac.uk

About the authors

Andrew McMeekin is Research Fellow at CRIC. Previously, he worked at Manchester School of Management and Science Policy Research Unit (SPRU). His work has focused on environmental innovation; the organisation of innovation in firms; national foresight and firm level foresight; patterns of consumption and new technologies.

Ian Miles is Professor of Technological Innovation and Social Change at the Victoria University of Manchester, where he is also co-director of the two research centres, PREST (Policy Research in Engineering, Science and Technology) and CRIC (Centre for Research on Innovation and Competition).

Jason Rutter is Research Fellow at CRIC. His research both at CRIC and previously at The University of Salford has focused on social aspects of computer-mediated communication both in recreational and practical activities. Current interests include web-based dissemination of social science research, micro-sociology of e-commerce, and, construction of trust and sociability on the Internet.

The Need for an International Infrastructure for Low-value Payment Systems

Michael Rader, Knud Böhle & Ulrich Riehm, Forschungszentrum Karlsruhe, *ITAS*

Issue: Predictions indicate that trade in "intangible" goods and services is probably the area of e-commerce with the greatest growth potential. While credit cards can be used for Internet transactions above a certain value, there are currently no widely accepted or diffused payment systems for small sums of money.

Relevance: There is a need for an infrastructure to enable the interoperability of a broad variety of small-value payments over the Internet. Such an infrastructure comprising standards, settlement and clearing agreements and arrangements in addition to technological components could give a boost to e-commerce. The results of this initiative could also help to fulfil European citizens' expectations that the completion of monetary Union will simplify conventional business in countries other than their own.

Introduction

There is widespread agreement among European politicians and industrialists that e-commerce is a key factor for competitiveness and economic growth in an increasingly global marketplace. Most observers feel that Europe is trailing behind the U.S. in terms of e-commerce, although it has also been argued that the European Internet lag is largely an American fabrication to excuse the failure of American companies to meet their own expectations in Europe (Guissani, 1999). A white paper by the Interactive Media in Retail Group published in 1998 demanded "that governments and industry should be doing more to back on-line commerce in Europe" (Rouf, 1998). Several

European governments have committed themselves to creating conducive environments for business, and the underlying concerns are not restricted to Europe. Canada has embarked on an ambitious programme to support Canadian e-business to staunch the flow of Canadian e-dollars across its border (Friedman, 1999).

Despite a great deal of encouragement from the U.S. Government, including a broadcast announcement by President Clinton that he would buy online for the first time, even some of the major players in e-commerce are facing problems. While it was argued that Americans doing their Christmas shopping from their own living rooms could avoid the problems traditionally encountered in the bricks-and-mortar environment, many online shop-

pers were unable to visit web sites due to heavy Internet traffic, web merchants were unable to provide the desired goods due to lack of inventory or inadequate logistics, shopping was abandoned due to poor design of web sites, or customers were unable to contact customer services. It has been estimated that the volume of custom could have been double the actual figure, had it not been for such shortcomings.

Even if this were not so, many American citizens are reluctant to participate in e-commerce for reasons of insufficient privacy or lacking security of personal data. Typical examples are that credit card information could fall into the wrong hands, or that personal data could be used for other purposes than that for which it was collected.

As in conventional mail-order, customers ordering physical items using e-commerce must provide some kind of delivery address, so that complete anonymity is difficult to achieve. However, predictions show that up to 40 percent of future e-commerce is expected to be in intangible goods which can be delivered on-line, such as software, information or services. For such goods, there is no genuine reason why the customer should reveal his or her identity. Some kind of receipt could be provided to enable complaints. Even for tangible goods there is the possibility of involving some kind of trusted third party, such as collection at post offices, to enable anonymous delivery.

The State of E-Commerce and Payment Systems in Europe

A recent study for the European Parliament (IPTS, 1999), followed by a country synthesis report (Böhle, et al., 1999) by the European Science and Technology Observatory (ESTO) has revealed a number of facts concerning e-commerce in Europe.

As this study focused on the inter-relationship between monetary union and electronic payment systems, it examined factors such as payment culture, national frameworks, payment cards, electronic purses, Internet payment systems and e-commerce in ten European countries (Denmark, Finland, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden, and the United Kingdom).

There are vast national differences and peculiarities which will have considerable impact on the diffusion of electronic payment systems and e-commerce in the individual countries. The use of electronic money is only at the experimental stage and traditional national "access products" are finding use on the Internet for domestic transactions. While Internet commerce at the national level is growing impressively, transborder commerce is only just starting.

Payment Systems

In everyday life, the use of cash has been declining steadily in all ten countries. Even so, it continues to be the most important single means of payment for everyday transactions. In fact, a recent study by the British research company, Retail Banking Research, has shown that cash will continue to be important in the new millennium, arguing that its benefits for customers are frequently under-rated. It concludes: "...before rushing to replace cash, it is vital to ensure that costs will be decreased by its substitution, which in turn means that the costs of non-cash payments need to be brought down" (RBR, 1999).

In the past, some countries have tended to make greater use of cheques for non-cash payments, while others have made greater use of debit or credit transfers. Today, with the spread of new electronic payment instruments based on payment cards, this distinction is getting weaker: recent years have seen the spread of debit and credit cards

E-commerce is being hampered by a lack of net capacity, poor logistics and concerns about security

A recent study conducted by the IPTS and ESTO has revealed vast national differences and peculiarities which will have considerable impact on the spread of electronic payment systems and e-commerce in the individual countries of Europe

Although the use of cash has been declining it will continue to be used well into the foreseeable future for small everyday transactions

Electronic purses have yet to receive widespread acceptance and despite the advent of the single currency, their use is generally restricted to a single country

The vast majority of international retail payments on the Internet are made using credit cards, generally using the safety features coming with standard browsers (e.g. SSL), but also unencrypted or by means such as fax or telephone

in all of the countries covered, although to varying degrees and following different patterns. National "preferences" may be due to payment culture, pricing structures, or to familiarity with the payment instrument concerned.

During the past few years there have been enormous increases in the numbers of automated teller machines (ATMs) and electronic devices enabling direct funds transfers at points of sale (EFTPOS). Although in some countries, there were several networks for such devices, sometimes incompatible with each other, strong tendencies towards interoperability are prevailing.

Of special interest to Internet commerce are the smart card-based electronic purses, a technology where Europe is widely felt to be leading. In most of the countries covered, electronic purses are now available on a regular basis or in pilot schemes. All in all, few electronic purses have yet achieved widespread acceptance. At least in Spain and the Netherlands, there was more than one purse scheme, and these were originally not interoperable. Most significant in view of the single currency is the fact that the use of each purse is still restricted to a single country. This is true even for the electronic purses of Finland and Sweden, although they can be loaded via Internet and in the case of Avant, the Finnish purse, may even be used for payments on the Internet.

Is there a need for new payment systems?

The vast majority of international retail payments on the Internet are made using credit cards, generally using the security features coming with standard browsers (e.g. SSL), but also unencrypted or by means such as fax or telephone. While there is interest in the SET protocol from the credit card organisations and some merchants, adoption has been

very slow and it is presently difficult to convince customers of its benefits.

For domestic purchases, Internet buyers tend to use those "national access products" which are also used most frequently for other purposes, in particular for conventional mail-order purchases. There is an astonishing variety of ways to pay within Europe and there are remarkable differences between countries.

There is a lack of widely diffused and accepted payment systems for small amounts (micro-payments). In some countries Internet service providers operate schemes to collect such small payments with the monthly bill and to distribute these to the merchants involved in return for a commission. Beyond this, small value goods and services can be delivered free to customers if sponsoring schemes, such as banner advertising, can be set up to off-set the costs.

At the present stage of e-commerce, payment systems are not a major barrier. However, surveys indicate that greater use would be made of e-commerce if it were perceived as "safer" for the transmission of information on credit cards or bank accounts, or if alternative, simpler methods of payment were available.

The availability of widely diffused payment systems other than credit cards could provide small businesses or private citizens wishing to sell something across the Internet sporadically but unwilling or unable to accept the investment needed to accept credit cards, with a means of participating on the selling side of e-commerce. There is also probably a lack of suitable small-value payment systems to cope with the volume of "intangible" e-commerce predicted for the future. Finally, there are no systems in routine application with which to make payments without revealing the identity of the purchaser. Clearly this does not

apply only to low-value payments, suggesting that there could also be demand for an alternative to credit and debit cards in other contexts.

While there have been many pilot schemes for secure, and in some cases, anonymous, "electronic" money, none has yet met with any great measure of success. A major problem is their lack of compatibility or interoperability, forcing users to make choices or to invest in a broad range of alternatives. At present, it is therefore very much a matter of chance whether a merchant and a prospective customer both happen to have subscribed to the same payment scheme. Schemes involving smart-cards have been held up back by a lack of diffusion of suitable devices for use with PCs, although Windows 2000 will be smart card-ready (Kotadia, 1999). Finally, existing schemes for low-value payments all have the disadvantage of fairly high costs per transaction, which currently makes them unsuitable for very small payments.

The need for an infrastructure for interoperability

Although the immediate benefits of establishing a common European payment infrastructure for "national" retail payment instruments are said to be moderate, it appears to be the appropriate strategic decision.

Experts are calling for regulation and responsible policies in the area of a common security infrastructure and a common payment infrastructure. Against the background that the international credit card organisations are already operating world-wide and have started to conquer the Internet, it has been argued that it would be important to make the "national" payment products interoperable and establish a common infrastructure for them within the European Union. This demand refers to "access products"

like credit transfers, direct debits but especially to "electronic money" (electronic purses).

The implementation of interoperable payment instruments in Europe would strengthen the competitive position of European financial institutions by offering alternatives to credit card payments. Banks in Europe, which have been established in a national context, could adopt suitable inter-bank agreements to be used for payments across borders. The infrastructure should enable competition to maintain consumers' freedom of choice and may also imply all in all a less risky structure of payment systems, because the risk is distributed and potential damage reduced.

Since European Monetary Union, there has been pressure on European banks to move towards such a common infrastructure. National actors afraid of competition from abroad might be reluctant to accelerate this process. In view of the lack of acceptance of electronic purses in real life at the national level, the perspective of international deployment and use on the Internet could offer the opportunity to achieve a "business case" for "electronic money products". It is also possible to use smart cards for anonymous payments, for example by means of "white card" electronic purses which have no direct link with a bank account.

Although there is competition and there is a divergence of strategic interests between "national/European" and "international" actors this should not lead to an overall notion of opposition to such an infrastructure. In the field of "electronic money" as well as in the field of secure payments over the Internet there are already important cooperative efforts.

Conclusions

There is a general consensus that policy-makers should not try to impose standards top

There is a lack of widely diffused and accepted payment systems for small amounts (micropayments). While there have been many pilot schemes for secure, and in some cases, anonymous, "electronic" money, none has yet met with any great measure of success

The implementation of interoperable payment instruments in Europe would strengthen the competitive position of European financial institutions by offering alternatives to credit card payments

About the authors

Michael Rader holds a doctorate in sociology. He has been with ITAS and its predecessor, AFAS, since 1979. His work has been mainly on the impacts of information and communication technologies. Recent work includes leading projects on the feasibility of a European Infrastructure for technology assessment and integrative technology assessment. He is a member of the executive committee of the European Science and Technology Observatory (ESTO).

Knud Böhle has degrees in both sociology and information science. Following activities in publishing, he joined ITAS' predecessor, AFAS, in 1986. He has led several projects on electronic publishing, electronic books, and, most recently, on electronic payment systems. Recently, he has participated in several European projects on a European Infrastructure for technology assessment, electronic commerce and electronic payment systems.


Box 1: Initiatives Toward An Infrastructure

The European policy of stimulating, moderating and complementing a process of self-regulatory efforts by the principal actors is already underway in shape of the work of the FIWG (Financial Issues Working Group) and its influence on the work of the ECBS (European Committee on Banking Standards). Most conspicuously the work of the ECBS has led to the concept of a multi-currency European Electronic Purse. Work on this topic was continued by the CEPS (Common Electronic Purse Specification) group which includes Europay, Visa International, Proton, ZKA Germany, Sermepa Spain, and American Express. In December 1998 it agreed on a common specification to enable the interoperability electronic purses. In the field of micro-payments, there has recently been an initiative to establish an IETF (Internet Engineering Task Force) working group on certain aspects of standardisation.

down, rather their main task should be to act as a catalyst in the process of bringing together convergent interests and technical options and then ensure compliance with the framework created. There might also be a role for policy-makers to encourage the involvement of not only the banking sector in standardisation activities with regard to payment systems, but to bring together players from various other industries (e.g.

smart card industry, networking) and application fields (e.g. digital TV, traffic, health, telecoms operators, financial services) involved in payment technologies.

Most observers agree that in the future several payment systems may co-exist, each satisfying different needs. The strategic point concerning standards is to distinguish payment products from the payment infrastructure. At the level of the payment infrastructure, interoperability is the main aim and co-operation the way to reach it. At the level of payment products and services, competition is desired. The expression "co-competition" has been coined for this approach. Some compare the situation to the deregulated telecommunications market, where any company fulfilling certain basic requirements has free access to the infrastructure. It has even been suggested that the infrastructure could be of public nature and leased to its users.

Finally, an interoperable infrastructure has its significance with respect to European integration: people expect all familiar payment instruments to work throughout the European Monetary Union and not to grind to a halt at their own country's border. While it is more of a political and psychological task to fulfil these expectations and to avoid frustration than a short term economic necessity, it could also have the added benefit of improving European chances in e-commerce. 

Keywords

e-commerce, electronic money, electronic purse, payment systems, privacy, standardisation, infrastructure

References

- IPTS, Study on Electronic Payment Systems for the Committee on Economic and Monetary Affairs and Industrial Policy of the European Parliament, EUR 18753 EN.
<http://www.jrc.es/pages/projects/docs/Final-Eps.Vol.1.pdf>
- Böhle, K., Rader, M., Riehm, U., (eds): Electronic Payment Systems in European Countries - Country Synthesis Report. Contributors: Anna Arbussà, Anna Backlund, Knud Böhle, Morten Falch, Charles Goldfinger, Philippe Herbin, Jos Leyten, Michael Rader, Ulrich Riehm, Oliver Seeley, Mildo van Staden, Jaume Valls. Seville and Karlsruhe (in print).
- Financial Issues Working Group: Stimulating Electronic Finance Within the European Union. Brussels: Global Finance Management S.A., 1999.
- Friedman, M., Canada's E-Commerce Edge. *Wired*, 10 November 1999.
<http://www.wired.com/news/politics/0,1283,32447,00.html>
- Giussani, B.: Europe's Internet Lag: An American Fabrication? *New York Times*, 14 September 1999.
- Kobrin, S., Johnson, E.: We Know All About You: Personal Privacy in the Information Age. Wharton: draft MS. 27 February 1999. (Available from the Wharton School, University of Pennsylvania).
- Kobrin, S., Johnson, E.: IBM survey reveals worldwide concerns about privacy. IBM Press Release, Hamburg, 5 October 1999.
- Kotadia, M., IT Week: Smartcards Set for growth. *Zdnet News*, UK 1 March 1999.
<http://www.zdnet.co.uk/news/1999/8/ns-7128.html>
- Retail Banking Research Ltd.: The Future of Cash – It's cheap, efficient and here to stay.
<http://www.rbrldn.demon.uk/cash.htm>, based on "The Global ATM Market to 2002", Richmond (UK), 1999.
- Raouf, A., E-Commerce Focus: Europe lags behind U.S.
<http://www.zdnet.co.uk/news/1998/27/ns-4950.html>

Contacts

Michael Rader, Knud Böhle, Ulrich Riehm, Forschungszentrum Karlsruhe
Institut für Technikfolgen-Abschätzung und Systemanalyse (ITAS)
Tel.: +49 (0)7247 82 2505, fax: +49 (0)7247 82 4806, e-mail: rader@itas.fzk.de

About the authors

Ulrich Riehm holds a diploma in sociology and has additional qualifications in computing. Previous employment was with a major manufacturer of agricultural machinery. He has been with ITAS and its predecessor, AFAS, since 1979. His work has been mainly on the impacts of information and communication technologies. This has included leading a project on electronic publishing and work for the German Bundestag on multimedia.

All three authors are at Karlsruhe Research Centre's Institute for Technology Assessment and Systems Analysis (ITAS), which is a founding member of ESTO. They recently coordinated an ESTO project on European Monetary Union and electronic payment systems.

IPTS publications

- Gameson, T. Natural Resources and The Environment Panel Report EUR 18970 EN Jun-99
- Scase, R. (J. Gavigan, ed.) Demographic and Social Trends Issue Paper: Mosaic Living EUR 18969 EN Jun-99
- Mercer, D.(J. Gavigan, ed.) Demographic and Social Trends Issue Paper: The Future of Education in Europe until 2010 EUR 18968 EN Jun-99
- Coomans, G. (J. Gavigan, ed.) Demographic and Social Trends Issue Paper: Europe's Changing Demography Constraints and Bottlenecks EUR 18967 EN Jun-99
- Kyriakou, D., Císcar, J.C., Lievonen, J., Salo A. 1998 Techno-Economic Analysis Report EUR 18964 EN Jun-99
- Papameletiou, D. Study on electronic payment systems EUR 18753 EN Jun-99
- Münker, T., Sorup, P., Schmitt, A., Rosén, K. Life Sciences and the Frontier of Life Panel Report EUR 18743 EN May-99
- Fahrenkrog, G., Scapolo F. The Futures Project: Overview EUR 18731 EN Apr-99
- Ducatel, K. Information and communication technologies and the information society panel report EUR 18730 EN Apr-99
- Gavigan, J., Ottitsch, M., Greaves, C. Demographic and social trends panel report EUR 18729 EN Apr-99
- Bobe, B., Bobe, A.C., Gavigan, J. (ed.) Benchmarking innovation practices of European firms EUR 18726 EN Mar-99
- Bontoux, L. The incineration of waste in Europe: Issues and perspectives EUR 18717 EN Mar-99
- Heller, C. Tracking & tracing in trans-European combined road/rail freight transport: A comparison of the basic technological options: AEI, GPS, GSM and train-integrated systems EUR 18716 EN Mar-99
- Hemmelskamp, J. Wind energy policy and their impact on innovation - An international comparison EUR 18689 EN Dec-98
- Zoboli, R., Leone, F. (ed.) Implications of environmental regulation on industrial innovation: The case of End-of-Life vehicles EUR 18688 EN Dec-98
- Riesco, P., Zwick, A. (ed.) The challenge of climate change for water technologies: an institutional perspective EUR 18687 EN Dec-98
- Sørup, P., Romero, L., Tils, C., Wolf, O. (editors) Biocatalysis: State of the art in Europe EUR 18680 EN Dec-98
- Weber, M. , Board, A., Craye, P., Mathieu, M. Strategic management of sustainable transport innovations EUR 18679 EN Dec-98
- Gameson, T. Private sector methods for weighting environmental indicators EUR 18655 EN Nov-98
- Kyriakou, D., Císcar, J.C., Luukkanen, H., Salo, A. Technoeconomic Analysis Report - Baseline EUR 18134 EN Sep-98
- Aguado, M.A. Use of bibliometrics as a technology watch technique. Application to the analysis of the recent developments of the photocatalysis EUR 18131 EN Aug-98

A B O U T T H E I P T S

The Institute for Prospective Technological Studies (IPTS) is one of the eight institutes making up the Joint Research Centre (JRC) of the European Commission. It was established in Seville, Spain, in September 1994.

The mission of the Institute is to provide techno-economic analysis support to European decision-makers, by monitoring and analysing Science & Technology related developments, their cross-sectoral impact, their inter-relationship in the socio-economic context and future policy implications and to present this information in a timely and integrated way.

The IPTS is a unique public advisory body, independent from special national or commercial interests, closely associated with the EU policy-making process. In fact, most of the work undertaken by the IPTS is in response to direct requests from (or takes the form of long-term policy support on behalf of) the European Commission Directorate Generals, or European Parliament Committees. The IPTS also does work for Member States' governmental, academic or industrial organizations, though this represents a minor share of its total activities.

Although particular emphasis is placed on key Science and Technology fields, especially those that have a driving role and even the potential to reshape our society, important efforts are devoted to improving the understanding of the complex interactions between technology, economy and society. Indeed, the impact of technology on society and, conversely, the way technological development is driven by societal changes, are highly relevant themes within the European decision-making context.

The inter-disciplinary prospective approach adopted by the Institute is intended to provide European decision-makers with a deeper understanding of the emerging S/T issues, and it complements the activities undertaken by other Joint Research Centres institutes.

The IPTS collects information about technological developments and their application in Europe and the world, analyses this information and transmits it in an accessible form to European decision-makers. This is implemented in three sectors of activity:

- Technologies for Sustainable Development
- Life Sciences / Information and Communication Technologies
- Technology, Employment, Competitiveness and Society

In order to implement its mission, the Institute develops appropriate contacts, awareness and skills for anticipating and following the agenda of the policy decision-makers. In addition to its own resources, the IPTS makes use of external Advisory Groups and operates a Network of European Institutes working in similar areas. These networking activities enable the IPTS to draw on a large pool of available expertise, while allowing a continuous process of external peer-review of the in-house activities.

The IPTS Report is published in the first week of every month, except for the months of January and August. It is edited in English and is currently available at a price of 50 EURO per year in four languages: English, French, German and Spanish.

S.PI.00.02



The European Science and Technology Observatory Network (ESTO):

IPTS - JRC - European Commission

W.T.C., Isla de la Cartuja s/n, E-41092, Sevilla, Spain

tel.: +34-95-448 82 97; fax: +34-95-448 82 93; e-mail: ipts_sec@jrc.es

GK-AA-00-002-EN-C

- ADIT - Agence pour la Diffusion de l'Information Technologique - F
- ARCS - Austrian Research Center Seibersdorf - AT
- CEST - Centre for Exploitation of Science and Technology - UK
- COTEC - Fundación para la Innovación Tecnológica - E
- DTU - University of Denmark, Unit of Technology Assessment - DK
- ENEA - Directorate Studies and Strategies - I
- INETI - Instituto Nacional de Engenharia e Tecnologia Industrial - P
- ITAS - Institut für Technikfolgenabschätzung und Systemanalyse - D
- MERIT - Maastricht Economic Research Institute on Innovation and Technology - NL
- NUTEK - Department of Technology Policy Studies - S
- OST - Observatoire des Sciences et des Techniques - F
- PREST - Policy Research in Engineering, Science & Technology - UK
- SPRU - Science Policy Research Unit - UK
- TNO - Centre for Technology and Policy Studies - NL
- VDI-TZ - Technology Centre Future Technologies Division - D
- VITO - Flemish Institute for Technology Research - B
- VTT - Group for Technology Studies - FIN

ENGLISH VERSION