Interorganizational Networks :

the Issue of *Global Sovereignty*

IFSAM/Track10:Global and Local Networks

Dr COLLIN Paul Marc

Associate Professor

MAGELLAN- IAE de Lyon-France

18 rue Jean Perret

F-69630 CHAPONOST

Mail : pmcollin@univ-lyon3.fr

Interorganizational Networks :

the Issue of *Global Sovereignty*

Abstract

One of the most striking phenomena of the past decade has been the internationalisation of service firms (Tersen and Bricout, 1996). Previously considered "un-exportable" (Segal-Horn, 1993), they have proven day after day that they have the necessary characteristics to undertake an international development, and even a globalization of their offering systems (Vandermerwe, 1989 ; Campbell and Verbeke, 1994 ; Gadrey, 1994 ;). Retail banking and financial services are remarkable illustrations of this phenomenon (Michalet, 1985 ; Andreff, 1995). And bank cards in the first place. However, management scholars have been slow in reacting to this challenge. Focused on industry (and surprisingly enough on the automotive industry), the scholars have rather neglected the emerging field of international service firms. This Research gap has motivated our project on the international deployment of services. The field study we have selected is relative to the bank card organizations. This industry illustrates the functioning of service firms as political institutions. A striking example relates to the emergence and development of international standards bodies, specifically in the area of Internet payments. We are faced here with the construction of a transnational regulation.

This paper brings twofold a contribution. On one hand, it enriches the interpretation of a very important, peculiar and potentially generic research object, through the lenses of the translation theory. On the other hand, it has key managerial implications regarding « political » strategies with regard to positioning as a regulatory institution. Discussion follows on the consequences of these agencies' activities for business enterprises.

Key words: interorganizational networks, strategic management, SET, bankcards

Interorganizational Networks :

the Issue of *Global Sovereignty*

Introduction

One of the most striking phenomena of the past decade has been the internationalisation of service firms (Tersen and Bricout, 1996). Previously considered "un-exportable" (Segal-Horn, 1993), they have proven day after day that they have the necessary characteristics to undertake an international development, and even a globalization of their offering systems (Vandermerwe, 1989 ; Campbell and Verbeke, 1994 ; Gadrey, 1994 ;). Retail banking and financial services are remarkable illustrations of this phenomenon (Michalet, 1985 ; Andreff, 1995). And bank cards in the first place. However, management scholars have been slow in reacting to this challenge. Focused on industry (and surprisingly enough on the automotive industry), the scholars have rather neglected the emerging field of international service firms. This Research gap has motivated our project on the international deployment of services. The field study we have selected is relative to the bank card organizations. This industry illustrates the functioning of service firms as political institutions. A striking example relates to the emergence and development of international standards bodies, specifically in the area of Internet payments. We are faced here with the construction of a transnational regulation.

The detailed case study we present and interpret is the SET scheme of Internet security and its localizations in multiple countries of operation. Interoperability is questioned in the context of industry globalization. The role and behaviour of transnational agencies such as Cybercomm are scrutinized. One of the originalities of our paper lies also in its epistemology and methodology. After a phase of interpretation of case data through the translation theory (Callon, 1986 ; Latour, 1989; Czarniawska, 1996; Sahlin-Andersson, 1996), we undertake a step of "framework" construction (Porter, 1991;

Claveau, Martinet and Tannery, 1998; Folger and Turillo, 1999; Tsoukas, 1996), in order to offer managers an "ex ante" strategic decision tool.

The translation school seems to offer a sensitivity for hybrid methodology (content and process), very useful for the analysis of transnational firms. The introduction of the notion of "actant non humain", the technical objects which build socio-technical networks, has enormous potential in management science. This concept includes all the stakeholders of transnational networks of standardization.

We have then started with the interpretation of case data with translation theory concepts We present detailed case studies in the area of transnational bankcard networks. For example a coalition between banks to create a *de facto* standard for transnational electronic payment security on the Internet. The case study is eye-opening. After a step of protecting its political interests and well-known technological solutions, the coalition understands that its mission becomes a matter of life and death for its members: brand new currency has been invented on the Web and one could develop business and monetary transactions without the banks!

This interpretative stage, while broadening our horizon and the relevance of our observations, has taught us much on the transnational mechanisms of regulation and standardization (participation in ISO meetings ; creation of proprietary bodies ; lobbying,…).But also on the « translation » steps regarding these transnational organizations. However, an additional step has to be added to this interpretative step. A step of "framework construction" (Porter, 1991, 95). The aim is to help managers of the transnational firms involved in regulations and standardization to anticipate the evolutions and make relevant decisions. The "framework" has three distinctive characteristics : the ability to help conception, the ability to help conceive problems « ex ante », and the ability to facilitate collective conception of strategic manoeuvers (Claveau, Martinet et Tannery, 1998, 70 ; David, 1998, 44).

This paper brings twofold a contribution. On one hand, it enriches the interpretation of a very important, peculiar and potentially generic research object, through the lenses of the translation theory. On the other hand, it has key managerial implications regarding « political » strategies with regard to

4

positioning as a regulatory institution. Discussion follows on the consequences of these agencies' activities for business enterprises.

1- Presentation and Genesis of Internet payments (cyberpayments)

1.1-   Presentation of cyberpayments

<u>1.1.1- Definition and challenges of cyberpayments</u>

In this article we will deal with the concerns around cyberpayments and their impact on the emergence of transnational regulation. What are the challenges of cyberpayments? Cyberpayments are an emerging new class of instruments and payment systems that support the electronic transfer of value. These transfers may take place via networks, such as the Internet, or through the use of stored-value type smart cards. Because of the efficiency and ease with which they transfer value, these systems may also present new challenges to law enforcement. Technology exists which could permit these systems to combine the speed of the present bank-based wire transfer systems with the anonymity of currency. As a result, there are issues that must be addressed as these systems are being developed to ensure the prevention and detection of money laundering and other illegal financial transactions.

Internationally, cyberpayment systems have also received extensive attention. Multilateral discussions and studies have been undertaken by both the G-7's Financial Action Task Force (FATF) and the G-10's Working Party on Electronic Money. For example, in June 1996, recommendation #13 was added to the FATF's 40 Recommendations. It states that "countries should pay special attention to money laundering threats inherent in new or developing technologies that may favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes".

What is the current state of cyberpayment technology? Progress toward technical and commercial standards in the cyberpayment industry has been steady and the emergence of cyberpayment systems is gathering momentum. A number of stored-value type smart card and network-based products have undergone pilot testing. These tests have taken place on a global basis, thus underscoring the international nature of the emerging cyberpayments infrastructure.

Some cyberpayment instruments features such as peer-to-peer value transfer and payer anonymity offer to the consumer an instrument with much of the flexibility and convenience of cash together with an enhanced ability to conduct purchases on an almost global basis. This technology suggests that law enforcement must begin to consider the potential implications of an environment where the wide availability of cyberpayments instruments could substantially reduce the use of physical currency in consumer-level transactions.

In considering potential cyberpayments-money laundering, it should be noted that the same technologies underlying cyberpayment products could also be used as new information gathering tools by law enforcement and payment system regulators. The privacy implications of enhanced government surveillance of information networks is an issue. Any policies in this area would have to be carefully crafted so as to meet constitutional protections of individual privacy and governmental concerns with critical infrastructure protection.

If we take the posture of a cardholder for a moment, the issue is materialized the following way (imagine you surf for Internet shopping): "Safe Shopping at Walmart.com: We want you to feel completely secure when ordering from Walmart.com. We use a technology called Secure Sockets Layer (SSL), which encrypts (or encodes) sensitive information before it is sent over the Internet. For more information, read more about how we protect the security of your personal information.". This is an example of what cyberpayment is all about: the choice of a few technologies (SSL, SET, …), the management of trust between the company (Walmart) and the customer, and the risks involved (counterfeiting, loss of card, …).

1.1.2- Recent history of Internet payment systems

The market potential seemed tremendous, and payment systems started to advertise their ability to react to this new challenge. We propose to move back to 1994-1995 to re-construct the Genesis of Internet payment systems, with the help of one of the gurus in the field at the time:

6

"New emerging network payment and Smart Card Purse schemes will make buying and selling quicker, easier and more convenient for merchants and consumers, while reducing cash handling costs for banks and retailers. " (Vandenengel, 1995).

In a time of Genesis, it proves useful to define the words used by the stakeholders of the situation: "The electronic commerce that is being widely discussed deals with the consumer or "retail" commerce of main street, as opposed to the "wholesale" electronic commerce of Wall Street. Wholesale electronic commerce has been prevalent for at least ten years, and relates to the trillions in electronic funds transfer between banks, international currency trading, and other institutional transactions. The "retail" electronic commerce field can be roughly categorized into two general types: network cash or payment schemes, and Smart Card electronic purse systems, although many programs cross these boundaries.

The Actor-Network (Callon, 1986) 'cannot wait'. He has to build a structure (a consortium, for example), so as to take advantage of an anticipated "gold rush". "The Commerce Net consortium was started to allow companies to conduct almost all their business through the Internet, from browsing multimedia catalogues to submitting bids and placing purchase orders." Some actors prove faster than, more pragmatic and more visionary than others: "Digicash envisions its electronic cash being used to pay for anything sold on the Internet, from software to pizza. Based on the RSA public-key cryptosystem, the user's equipment (a PC or a Smart Card) generates a random number or "note". The equipment then "blinds" the number and transmits it to the user. The user's equipment can then "unblind" the note and transmit it electronically for payment in cyberspace.

On the merchant side, the payee checks that the note's digital signature is authentic, then forwards it to a bank to have this account credited by the same amount. The underlying technology is described at length in an August 1992 Scientific American article by David Chaum." What is striking in this citation is the coupling between a fair understanding of the market needs (in terms of service) and the articulation of what seems to be a technological fit. Companies and institutions are active in searching appropriate solutions in Internet payments: "Interest in network cash isn't limited to eager entrepreneurs and theoreticians. Many major companies and institutions are active in the search of the

7

holy grail of Electronic Commerce, including Apple Computer, BankAmerica Corp are funding a company called CyberCash. Cybercash is working on both secure Credit/Debit card transactions and electronic money transfers for the Internet, AmericaOnline, Compuserve and other private networks.

There were-and there still are an avalanche of announcements in this area: "Wells Fargo has contributed to the avalanche of Internet Commerce announcements. In December 1994 they announced an agreement to work with CyberCash Inc to provide Internet payment services. They will initially support credit card only, but also believe that here is an opportunity for debit and cash payments. " The announcements haven't stopped till then.

Some work on the development of "standardizable" solutions: "Customers envision a cash equivalent being stored on pre-paid smart cards which can be used for network payment transfers as well. The Moneta-Europay-Mastercard (EMV) is working on joint standards for smart card protocols to be used in electronic commerce. These smart-card efforts go beyond the many methods that are being discussed that allow for secure credit card transactions over open networks, such as First Data's joint program with Netscape Communications Corp. First Data, a credit card transaction processor, will have a system that encrypts credit card numbers for customers making purchases on the Internet."

The pursuit of a de facto standard accessible to the entire profession operates as a signal that the major players are eager to create a Common Good for the industry. However, It is noticeable in our example that they use this opportunity to act as partners with their competitors to impose a point de passage oblige (Callon, 1986), namely the use of the smart card technology they have been pioneering without success for many years. Hence this "translation process" (Callon, 1986; Czarniawska, 1996) could be analysed as a mean of "recycling" existing technologies in techno-political projects with high visibility and potential marketing gains for each of the Networked organizations. Subsequently, opportunistic pilot projects help "discipline" the stakeholders (suppliers, customers, national public authorities, while actual physical deployment (including ATMs[1] and EFTPOS[2] materials) provide the basis for durable networking and standardization.

---

[1] ATM : Automated Teller Machine
[2] EFTPOS : Electronic Fund Transfer at The Point of Sale

Security became a concern very early in the process:

"Current estimates of credit card fraud are more than \$50 billion a year[3], and counterfeiters are now able to produce hologram credit cards with encoded magnetic stripes with little effort. It is unreasonable to expect that a number of resourceful people are not already trying to crack some of the new payment schemes, and it is perhaps inevitable that some of the less robust methods will be compromised by hackers. Anyone who has never had to deal with bugs in new software should also realize that there is no absolutely foolproof technology. The goal then, is to make the cost of breaking the system much greater than the potential returns, so that spending hundreds of thousands of dollars in computer time and labour would yield a few thousand dollars or less in illegal gains.".

In terms of innovation process, we could propose the following typology: When analysing the range of electronic commerce propositions, it may be useful to further categorise them as either "technology extensions" of current financial practices, or alternatively, as true electronic cash, although it is not always simple to make the distinction. Technology extensions can be thought of as tools and technology that allow us to operate the present financial instruments of checks and credit cards more quickly, securely, and accurately. Beyond the enthusiasm, we observe a growing concern around the issue of security of payment.

1.2- The concerns over cyberpayments

1.2.1- The trend toward deterritorialization: cyberpayments in the Cyberspace

The first dimension of the cyberpayment concern relates to geopolitics and globalization. We are told that we face an era of radical changes. One of them is the "deterritorialization" (Toal, 1999). Quoting Paul Virilio (1983), we could say that, beyond some words like globalization, translocality, glocalization, transnational, cyberspace, what is being described is the re-arranging and re-structuring of spatial relations as a consequence of the technological, material and geopolitical transformations of the late 20th century.

---

[3] already in 1994

To speak of deterritorialization in contemporary discourse, according to Toal (1999) is to speak of a generalized dismantling of the complex of geography, power and identity that supposedly defined and delimited everyday life in the developed world for most of the 2Oth century. It is to speak of a new condition of speed and 'informalization', of the transgression of inherited borders, the transcendence of assumed divides, and the advent of a more global world. Though regimes of territoriality are constantly in flux and under negotiation, discourses of deterritorialization tend to ascribe a unique transcendency to the contemporary condition, defining it as a moment of overwhelming newness.

Economically deterritorialization is held to be a consequence of an unstoppable globalization of previously discrete national markets and economies. Reich's work (1991) is a strategic response to such deterritorialization, a "work of nations" agenda emphasizing educational training, infrastructural investments, and skills development for state administrators to promote and cultivate upon their territorial patch of the global economy. Kenichi Ohmae's work suggests organizational strategies for transnational business managers to take advantage of what he sees as the coming borderless world and the death of the nation-state (Ohmae, 1990, 1995). In Ohmae's idealized world "multinational companies are truly the servants of demanding consumers around the world". "Old-fashioned bureaucrats", however, keep trying to hinder the natural development of a borderless world. "They create barriers and artificial controls over what should be the free flow of goods and money."

This striking disillusionment with the state and dis-enchantment with national territory and soil is evident also in the digital culture that has grown up around the spread of informational technologies in the advanced industrial world. According to some authors, Cyberspace is a land of knowledge with a "bioelectronic frontier" demanding discovery. Like Ohmae, they see state bureaucraties, old-fashioned border builders, as a threat to progress on the bioelectronic frontier. Governments in the cybernetic knowledge age need to get out of the way of the pioneers of the information age. Their industrial policy should focus on "removing the barriers to competition and massively de-regulating the fast growing telecommunications and computing industries" (Dyson and al., 1994). Freed from the constraints of the old spatial order, cyberspace promises to open up closed markets and liberate repressed peoples, to unify an increasingly free and diverse world. We don't mean to go that far in the

10

diagnosis. We simply aimed at presenting a quite extreme view of the opportunities, challenges and impediments inherent to cyberspace. We present now the relation which could be drawn between deterritorialization and financial markets.

1.2.2- Disintegration of sovereignty

With the Global Information Infrastructure initiative (GII), for example, territorial borders disintegrate as key paradigms for regulatory governance (Reidenberg, 2000). Transnational information flows on the GII undermine the foundational borders and erode state sovereignty over regulatory policy and enforcement. Physical borders become transparent and foreign legal systems have local relevance. With electronic cash and new means of electronic stored value, such as those developed by Cybercash and Mondex, Internet transactions may take place entirely on the network without the physical delivery of goods and services and without resort to any national payment system. Yet the GII creates simultaneous 'global' rightholders. A given activity may be subject to differing rights at the same time, such as trademark or antitrust protections, because the activity transcends the borders of any single nation. In addition, the temptations to apply national laws and standards extraterritorially further compound the legal uncertainty.

Network borders have a strong tendency to replace national borders. The visible network borders are contractual ones. For example, the demarcation lines among network service providers such as America OnLine, CompuServe, EUNet, or Prodigy create important boundaries. Network architecture also creates a significant type of border. Gateways between different systems establish fundamental rules of conduct. In effect, technical standards exert substantial control over information flows. Technical standards set default boundary rules in the network that tend to empower selected participants. These visible network borders arise from complex rule-making processes. Technical standardization may be the result of a purely market-driven process or alternatively may be adopted through a standards body. The classic example of a market-promulgated standard is the QWERTY keyboard. Once the now famous keyboard configuration became popular, public acceptance of other, more user-friendly configurations was unlikely. In contrast, standards bodies seek to identify and

11

recommend technical specifications for particular network needs such as security. These organizations, such as the American National Standards Institute (ANSI) and the International Organization for Standards (ISO), play a critical role in the development and promotion of technical standards. In essence, these organizations assure and reinforce the contours of network borders (Reidenberg, 1996).

In this context we are faced with the incongruity of traditional regulatory policymaking. In the USA, for example, national regulators compete with each other for jurisdictional power. In Europe, though, 'data protection' agencies have played a significant role in the formulation of information policy. The European Union, too, has established an Information Society Project Office to coordinate a number of wide-ranging European Commission activities.

The development of a new model for governing networks is crucial for effective policy leadership. The new paradigm must recognize all dimensions of network regulatory power. For global networks, governance could be seen as a complex mix of state, business, technical, and citizen forces. Rules for network behaviour will come from each of these interest centres. Within this framework, the private sector could become a driving force in the development of the information society and governments could be involved in protecting public interests.

Also, the recognition of new network borders opens new instruments for the achievement of regulatory objectives. Standards now contain significant policy rules. The debate over encryption standards and key escrow mechanisms reflects the critical new instrumentality of standards-setting.

Should we recognize network systems as semi-sovereign entities? Networks have key attributes of sovereignty: participant/citizens via service provider membership agreements, 'constitutional' rights through contractual terms of service, and police powers through taxation (fees) and system operator sanctions. In effect, network users become stakeholders in transnational political and economic communities. Nevertheless, where networks develop parallel to physical society, traditional governments retain crucial public responsibilities and significant interests. The European principle of subsidiarity could fit a new model of governance, where state governments would not attempt to expropriate all regulatory power from network communities. States can even provoke the creation of

network standards, but without interfering with each detailed item. The role of the state could shift toward the creation of an incentive structure for network self-regulation.

1.3- Cyberpayments' specific concerns

A particular law enforcement concern regarding the enhanced ability to move funds, is the peer-to-peer payment facility being offered by some schemes. At least one card vendor, and several e-cash schemes, plan to offer consumers the ability to anonymously transfer purchasing power from one electronic purse to another; such payment transactions would eliminate the need for clearing procedures and may provide no audit trail, providing opportunities for criminal abuse.

Another concern relates to the ability of financial transactions and monetary value transfers to 'escape' from the regulated banking industry where regulators have some level of visibility. The issue of non-bank involvement in the provision of electronic purse services was explored by European Economic Community policymakers. A 1994 report from the working group on European payment systems proposed that only banks be allowed to issue electronic purses. At the November 1994 Financial Action Task Force (FATF) meeting in Paris, it was noted that laundering operations were spreading outwards from the banking to non-banking sector as launderers become more aware of the various directives, legislation and conventions requiring banks and financial institutions to follow the standard requirements of identification and reporting. These non-bank institutions, ranging from large to small less-traditional financial intermediaries, are subject to fewer regulatory requirements and examinations, making them potentially more vulnerable to money laundering.

2- Cyberpayments' regulatory initiatives

2.1- A landscape of multiple initiatives

We can cite the G-7 Financial Action Task Force (FATF). It is an intergovernmental body which began in 1989. The main purpose of FATF is the development and promotion of policies to combat money laundering and specifically to prevent proceeds of crime from being utilized in future criminal activities and from affecting legitimate economic activities.

13

Another initiative is the one by the OECD. It considers that "as a matter of urgency, public and private sector institutions should re-evaluate many of the economic, legal and political frameworks that currently govern commercial activities and the technological and social environments in which they take place". They recommend regulation of the information infrastructure: "Electronic services infrastructures must be permitted and encouraged to converge in order to reflect the rapid convergence of networking technologies employed in Electronic Commerce applications." They recommend also standardization: "The Group urges governments to adopt a pragmatic approach that does not discourage the development of widely accepted proprietary solutions becoming adopted as if they were standards for Electronic Commerce, but which nevertheless monitors standardization developments closely to ensure that proprietary standards do not become barriers to market entry or impediments to further innovation (oecd.org/fatf/1998).

3- The SET Initiative (Secured Electronic Transaction)

3.1- Presentation

We present now an interpretation of cyberpayments' issues and solutions in terms of the Translation Theory (Callon, 1986; Latour, 1989; Sahlin-Andersson, 1996).

What is SET? "The SET Specification is an open technical standard for the commerce industry developed by Moneta and MasterCard as a way to facilitate secure payment card transactions over the Internet. Digital Certificates create a trust chain throughout the transaction, verifying cardholder and merchant validity, a process unparalleled by other Internet security solutions. Software vendors whose products pass SET Compliance Testing are eligible to display the SET Mark on their products. SET participants are merchants, financial institutions, and promotional sites that utilize or advertise licensed software. " (Moneta EU Region, Informations Presse, October 24th, 2000).

The concepts of Systems' openness and of trust chain act as vehicles and metaphors of the necessary cooperation within the network. They pave the way for actors (human and non human) (Latour, 1989) to negotiate commonly accessible solutions. The stakeholders reside in differentiated settings: the merchant on a Pacific Island, the cardholder bank in a large European city, the network in the USA,

14

for example. Service providers can be traced along this 'trust chain', ensuring quality and reliability of data transfer.

What is the Genesis of the SET network? On February 1, 1996, Moneta International and MasterCard International announced, with others in the industry, the development of a single technical standard for safeguarding payment card purchases made over open networks. On December 19, 1997 SET Secure Electronic Transaction LLC (SETCo) was formed to implement the SET Specification. The company is supported by borrowed resources from MasterCard and Moneta. SETCo manages the Specification and coordinates efforts related to the adoption of SET as the global payment standard.

3.2- Some technical elements

The most significant solutions for electronic commerce securization are, according to Haguet's typology (1996): what can be called digital cash (Digicash, Mondex), direct transactions between client and merchant (SET), and intermediation (GlobeID, CyberCash, First Virtual).

The diversity of solutions shows that translation processes are occurring on a bilateral and multilateral basis among actors of this industry. SET exists in the public arena, as a proposed standardized way of reducing risk on Internet payments; but it also exists in the private arena, as a private network able to enrol participants, transforming them in members and network 'citizens'.

<u>3.2.1- A national example</u>

A national example is provided by the French governmental plan for improving security on payment cards. Following a very controversial trial of a hacker, and responding to the consumerist pressure, French government issued a plan. Its aim was to improve security on using payment cards. One of the main items related to the re-positioning of bank card industry under the guardianship and supervision of the Central Bank of France. The Central Bank became a policeman. This law project (to be institutionnalized through legislative process soon after) required infrastructure modernization and securization improvements from the banks, while introducing new consumer insurance schemes.

<u>3.2.2- A regional example</u>

A regional example is offered by European regulation on digital signature. The European directive, dated October 23rd, 1998, ready to be 'translated' into national laws of Member-countries, poses: "Electronic signature has the value of a proof, just as a manuscript signature." This directive has paved the way to the development of standard Internet payments solutions. Smart Card payment has been among the first concrete applications of this conceptualisation of electronic signature. This gives a competitive advantage to organizations that have integrated, from Day 1, European Commission's requirements and propositions in their R&D efforts.

3.3- SET[4] Country by country

The emergence of transnational regulation evolves in parallel with national specificities. Transnational regulation efforts must take into account local payment cultures, Internet usage rate, the advancement of Internet Connectivity Infrastructures. Regulators, public and private, must find compromises, either by 'transporting' a national model (considered by regulators-translators as a best practice), or by finding a lowest cost denominator (Pistor, 2000). The process of standardizing the law can provide ideas for regulators in the cyberpayments' arena. The choice of a particular national legal order may reduce the costs of adaptation, as at least one country already complies with the new standards. However, at least if adopted by States, this approach smells of domination, or 'legal imperialism' (Pistor, 2000, p. 6). Political reasons therefore make it unlikely that this approach is taken openly. Political factors should be taken seriously, not only because they may delay or dwarf the standardization effort, but because they will have a strong impact on reception of the standardized rule. Another method is the lowest cost denominator (LCD). This approach is frequently used for standardizing the law. It avoids some of the problems of choosing a particular legal order because, at least in theory, the LCD should be compatible with pre-existing concepts and rules. However, this approach limits the scope of standardization. The minimum standards that are established do not preclude diversity in different jurisdictions. A compromise between these two approaches is to create a

---

[4] Secured Electronic Transaction

new legal concept based on comparative research and to incorporate it into the standardized rule. This approach is appealing because it avoids, or at least mitigates some of the political problems of using a particular national legal order.

3.4- Interpretation of the SET case through the Translation Theory

Czarniawska and Sevon (1996) have shown that the term of translation (Callon, 1986) calls attention to a richness of meanings associated: transference, linguistic translation, but also transformation, alteration and change. The term of translation is also associated with a constructionist view of power. For Callon and Latour (1981), 'power' stands for range of associations: actors associate with other actors (including non-humans) and the more numerous and important their associations are, the greater is the power of the whole network thus created. In this sense, power is a result and not a cause, and it does not 'belong' to anybody in particular (Czarniawska and Sevon, 1996).

The construction of the SET norm can be analysed as an illustration of the management of a controversy to help move toward a network reinforcement process. The controversy deals with security. The evolution of fraud on the Internet has caused a breakdown of the trust chain. Therefore, translators (bankcard networks, in this instance) endorse the role of putting together Business requirements and 'selling' them to the community. Not as a package, but as a process. A process of negotiation, the confrontation of actors' interests materialized by a Business Requirements 'edited' document (Sahlin-Andersson, 1996) and a physical prototype: a smart card reader connected to a PC. Multiple 'intermediaries' (Callon, 1986) intervene in the process (documents, actors, data). They are being used as factors, and impediments, of consensus building.

3.4.1- The phase of testing

The standardization process goes through a phase of testing. Although often strictly technical, this phase can help build legitimacy for the tested solution. For example, in Australia, four major banks have chosen to participate in the testing of a secured e-commerce solution. Why have they chosen one

partner instead of another? They have invested time, energy and money with the organization with a capability and competencies to supply with the tools to implement the SET program. Implementation is a key element. It is as if Translation's teleology was to facilitate implementation by the actors beyond the borders of the experimentation.

Translation means that there is freedom to conceive the solution (and its appropriate regulation package embedded into it). It is not given or imposed. Translation means also that the process of manipulating requirements and solutions goes through a step of 'mise en équivalence' (equivalence search) between texts, statements in different contexts (Callon, 1986): a market demand in Sweden, to be translated by the London office of a bankcard network into a software functionality by the computer scientists at the World headquarters in the USA.

3.4.2- Legitimacy

Legitimacy is an attribute of the organization. A bankcard network, composed of thousands of banks in more than 100 countries, brings legitimacy every time it undertakes an experiment. It starts the virtuous circle of Translation. Organizational legitimacy encourages banks to become participants in pilot projects. Their participation improves the likeliness of success of such a project, which can pave the way to the development of a de facto standard.

The trust chain of human actors is a risk-reducing factor in the construction of regulation policy. In our example, the international network of bankcard members encourages the participation of Australian banks, provides them with a forum of discussion. These events act in favour of the SET 1.0 protocol. A good way of aligning actors is to expand the frontiers of a pilot to an entire industry, giving the experiment a real life dimension, thus improving the credibility and the readability of the results.

3.4.3- CyberCOMM

In France, Cyber-COMM has taken the role, the posture of a SET translator. It has, in the words of Callon and Latour (1981) "taken the ball and played with it to advance in the field." The power is a

result of actors' associations, not a cause. It does not 'belong' to anyone in particular (Czarniawska and Sevon, 1996). Cyber-COMM has contextualized the French payment culture and problematized the security controversy,operated a formal investment (Boltanski and Thevenot, 1991), namely the creation of a consortium, and instituted a compulsory crossing point ('point de passage obligé'), the payment card. It has taken a political stand, meaning that it has given the banks the opportunity to continue to govern the techno-political networks. Even if telecommunications companies and technology providers become co-conceptors and implementers of payment solutions. The crossing point ('PPO') acts just like a paradigm selection in the Research process: it permits creativity, brings new interpretations, but, at the same time, it impedes creativity. PPO facilitates the conception of innovative solutions, but within the limits it has set.

The translator proposed his/her preferred way of handling the translation. He/She comes with the grammar, the 'repertoire', the 'lingua franca' with which stakeholders must work. It brings the 'ball' (in Callon's metaphor), either soccer or rugby, either full ball or flat ball, either in leather or in plastic. There is only one translator for many actors. But there are 'cascades' of translations, allowing each actor to become someone else's translator. SET Co is a global translator; and a French banker can be the translator for his suppliers and customers. User education is a form of ultimate translation at the end of the trust chain.

Translation comes first, as early as the conception phase of a project. Regulation comes next, in the implementation phase. But it might prove to be good governance to include regulation requirements in the conception phase. Because choices will be irreversible after implementation.

3.5- Summary of the interpretation through the Translation Theory

Let us look now at the steps of the translation process in our example.

First step: Contextualization (actants, challenges, move toward convergence): Professionals and customers demand Internet payment securization to facilitate electronic commerce development.

Actants are banks, Internet merchants; one of challenges is the development of secured online transactions; the convergence is in the common interest in developing a secured solution.

Second step: problematization and emergence of a translator: What unites the actants is the need for security at a reasonable cost (SET seems too costly to some experts); what separates public and private actants is the secret around encryption, and the entry of trust intermediaries (possibly non-banks).

Third step: Compulsory Crossing Point (CCP) and convergence (it can be a location or a piece of text): the major bankcard networks act as CCPs in the collective search for convergence.

Fourth step: Selection of spokespersons of each organization: CyberCOMM, networks, banks, governments, consumerist associations select spokespersons.

Fifth step: Formal investments: external (consortia, economic groups such as GEIE, …) and internal (regional committees; products' groups; coordination bodies; participation in Normalization boards,…).

Sixth step: management of intermediaries: data; technical objects; money; know-how, …). In our example, the intermediaries can be reporting data, chip card and card readers with their software, budget for Cyberpayments' R&D, or organizational learning capabilities in international risk management.

Seventh step: Actors' mobilization (enrolment): alignment through the conception of systems integration and interoperability projects.

Eight step: the search of network irreversibility: the creation of a European consortium, for example.

In summary, translation is an open and constructionist social process, which crosses national borders, and which has significant impacts on law and public policies (law enforcement, money laundering, consumer protection, …). One of the major trends of such a process is the search for common good's construction. There is a conceptual proximity with global information issues (in the GII project for instance).

If we draw an analogy with Internet payment mechanisms, we can propose that regulation is needed in the interest of the consumer. But who will be the consumer's spokesperson? Who will propose a

translation of his/her interests? And how? We have attempted to show an illustration of how it could work. We don't consider it as a best practice, but more as an example of one possibility of management practice to be articulated with transnational regulation policy.

Conclusion

Transnational regulation in the field of cyberpayments cannot be considered as a panacea. However, it may provide, in some cases, the basis for a positive and even fruitful dialogue between public and private organizations. From a Management Research's standpoint, we consider that it can be useful and relevant to analyze transnational regulators as translators (Callon, 1986; Sahlin-Andersson, in Czarniawska and Sevon, 1996). They operate a 'mise en equivalence' between business requirements and political ones. It is fair to say that public regulators have an interest in co-developing regulation policies with private organizations, instead of imposing unrealistic standards. Solutions should be results of translation 'cascades', co-piloted in a constructionist way. The value of such a posture resides in the mobilization of all actors toward a common good, a regulation policy embedded within a techno-political solution to macro and micro-threats posed by the spread of cybertechnologies in a borderless world with a network texture.

References

Andreff W. (1995), *Les multinationales globales*, La Découverte, Paris

Baxter L. (1999) *Bugged : the software development process*, paper presented at the 1st Critical Management Conference, Manchester

Bohle K. and Riehm U. (1999) *Electronic Payment Systems in European Countries*, Second Draft, Forschungszentrum Karlsruhe

Boltanski L and Thevenot L. (1991) *De la justification*, Paris, Métaillé

Callon M. (1986), *Eléments pour une sociologie de la traduction*, Année sociologique, Vol.XXXVI

Callon M. (1986), *Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay*. In: Law, J. (ed.) Power, action and belief, London: Routledge and Kegan Paul, 196-233

Callon M. and Latour B. (1981) *Unscrewing the big Leviathan: How actors macro-structure reality and how sociologists help them to do so*. In Knorr-Cetina K and Cicourel A (eds), Advances in social theory and methodology, London: Routledge and Kegan Paul, 277-303

Campbell A. & Verbeke A., The Globalisation of Service Multinationals, *Long Range Planning*, Vol. 27, N° 2/1994, 95-102

Crawford T.H. (1993) *An interview with Bruno Latour*, Virginia Military Institute, Configurations, 1993, 1.2 :247-268, copyright The Johns Hopkins University Press and the Society for Literature and Science

Czarniawska B. and Sevon G. (1996) *Translating Organizational Change*, De Gruyter, Berlin, New York

Dobers P. and Soderholm A. (1999) *Translation and transcription in Development projects: From vague problems to clear-cut solutions through project organizing*, GRI-report 1999:6, Scancor, Stanford University, 1999

Etiemble, *Parlez-vous franglais ?* , Gallimard, Paris,

Dyson and al. (1994) A Magna Carta for the Knowledge Age, *New Perspectives Quarterly*, 11, 4:26-37

Haguet J., (1996) *L'Internet: guide stratégique pour l'entreprise*, Masson, Paris

Hirst P. and Thompson G. (1996) *Globalization in Question*, Cambridge: Polity

Knorr-Cetina K (1981), *The manufacture of knowledge*, Oxford: Pergamon

Latour B. (1986) The powers of association. In Law J. (ed.), *Power, action and belief*, London: Routledge and Kegan Paul

Latour B. (1988) The politics of explanation: An alternative. In Woolgar S; (ed.), *Knowledge and reflexivity: New frontiers in the sociology of knowledge*, London: Sage

Latour B. (1989) *La Science en Action*, La Découverte, Paris

Latour B. (1992) Technology is society made durable. In Law J. (ed.), *A sociology of monsters: Essays on power, technology and domination*. London: Routledge

Latour B. and Woolgar S. (1979/1986) *Laboratory life*. Princeton: Princeton University Press

Latour B. (1997), *Nous n'avons jamais été modernes*, Editions La Découverte, Paris

Latour B. (1997) *On recalling ANT*, Workshop, Keele University, July 1997, 5 pages

Latour B., Mauguin P., Teil G., *Une méthode nouvelle de suivi socio-technique des innovations: le graphe socio-technique*, papier de recherché du centre de sociologie de l'innovation, 2001, 28 pages

Leyshon A. and Thrift N. (1997) *Money/Space: Geographies of Monetary Transformation*, London: Routledge, p. 225-259

Mé L. and Chaillat R. (1999) *Le commerce électronique: un état de l'art. An overview of electronic commerce*, Supelec School, Paris, unpublished document

Michalet CA. (1985) *Le capitalisme mondial*, PUF, 2ed, Paris

Newman D. (1998) Boundaries, territory and post-modernism: towards shared or separate spaces, *Geopolitics*

Ohmae, K. (1990) *The End of the Nation State*, New York, Free Press, 1995 and *the Borderless World*, New York, Harper Business

Perritt H. (1999) *Role and efficacy of international bodies and agreements: US perspectives on consumer protection in the global electronic marketplace*, Federal Commission Discussion Paper

Pistor K. (2000) *The Standardization of Law and its effect on developing economies*, United Conference on Trade and Development, G-24 Discussion Paper Series, Harvard University, Center for International Development, p. 6-8

Reich, R. (1991) *The Work of Nations: Preparing Ourselves for Twenty First Century Capitalism*, New York: Knopf, p. 77

Reidenberg J. (1996) *Governing networks and rule-making in cyberspace*, Information Security Committee, law.emory.edu

Rovik K.A., (1999) *The translation of popular management ideas: toward a theory*, paper presented at the SCANCOR Workshop

Sahlin-Andersson K. (1996) *Imitating by Editing Success: The Construction of Organization Fields*, in Czarniawska and Sevon: Translating Organizational Change, Walter de Gruyter, Berlin, New York, p. 82

Sahlin-Andersson K. (1996) *National, international and transnational constructions of New Public Management*. In Christensen T. and Laegreid P., Transforming New Public Management

Segal-Horn S. (1993), *The internationalisation of service firms*, in Schwartz (T), Advances in service management, Jai Press, vol.9, 31-55

Tersen D., Bricout JL. (1996) *L'investissement international*, Armand Colin, Paris

Toal, G. (2000) Borderless Worlds? Problematizing discourses of deterritorialization, Chapter for 'Geopolitics and Globalization: The Changing World Political Map", June 1999, in *Geopolitics*, 4 (2)

Vandenengel, G. (1995) Cards on the Internet, *World Card technology magazine*, Volume 1, Issue 1, Feb-March, p. 46-48

Virilio, P and Lotringer, S (1983) *Pure War*, New York: Semiotext

Vandermewe S., Chadwick M., *The internationalization of services*, The Service Industry Journal, 1989, Vol. 9, 79-93