

**NOTRE DAME UNIVERSITY
FACULTY OF LAW & POLITICAL SCIENCE**

**ELECTRONIC COMMERCE:
REGULATIONS
AT THE GLOBAL ERA**

by
ROUBA SALIBY

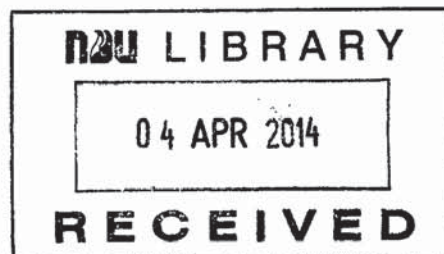
FACULTY OF LAW & POLITICAL SCIENCE



IN PARTIAL FULFILLMENT, THE REQUIEREMENT FOR THE DEGREE OF
MASTER OF ARTS IN INTERNATIONAL AFFAIRS AND DIPLOMACY

NOTRE DAME UNIVERSITY – LEBANON

2013



*NOTRE DAME UNIVERSITY
FACULTY OF LAW & POLITICAL SCIENCE*

ELECTRONIC COMMERCE:
REGULATIONS
AT THE GLOBAL ERA

M.A. THESIS

Prepared by

ROUBA SALIBY

*NOTRE DAME UNIVERSITY
FACULTY OF LAW & POLITICAL SCIENCE*

ELECTRONIC BUSINESS: REGULATIONS AT THE GLOBAL ERA

BY ROUBA H. SALIBY

SUBMITTED TO THE FACULTY OF LAW & POLITICAL SCIENCE

IN PARTIAL FULFILLMENT THE REQUIEREMENT FOR THE
DEGREE OF MASTER OF ARTS IN INTERNATIONAL AFFAIRS AND
DIPLOMACY

NOTRE DAME UNIVERSITY – LEBANON

FALL 2013-2014

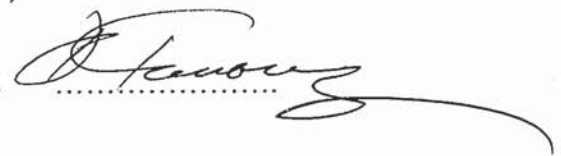
APPROVED BY: DR. GEORGES LABAKI
ADVISOR



DR. MICHEL NEHME
FIRST READER



DR. AKL KAYROUZ
SECOND READER



ELECTRONIC BUSINESS: REGULATIONS AT THE GLOBAL ERA

ACKNOWLEDGMENT

First and foremost, I offer my deepest gratitude to all people who supported me in this project. I would like to express my sincere appreciation to Dr. George Labaki, for helping me in my thesis and for providing me an experienced ear for my doubts about writing the dissertation paper.

Afterward, I so much appreciate Dr. Michel Nehme and Dr. Akil Kayrouz because they helped me through their expertise throughout my years at Notre Dame University.

I am indebted to my parents for supporting me throughout all my studies at the university and for providing me a home to complete my writing up. In addition, I have been blessed with a cheerful group of friends who provided me with a friendly smile and joyful times.

Finally, it is a pleasure to thank all those who provided me with the needed information. I am grateful to all those who contributed directly or indirectly to the realization of this project and for their encouragement when they are needed.

ABSTRACT

The internet has led to major growth in the economy due to its new e-commerce trends along with the dynamics in the advertising industry.

Although e-commerce is an important sector in the world of trading, it has its implications; the companies all over the world have to find solutions to such implications due to the fact that e-commerce is of major importance for companies to promote and sell their products. The purpose of my paper is to highlight the importance of e-commerce in the world trading and propose a solution to the implications associated with trading via the net. I will start by defining E-commerce in international relations, its corporate market values, its corporate practices, and the domain names used. Then I will move on to the history of electronic e-commerce, its applications, the governmental regulation, the global trends, the impacts on markets and retailers and the distribution channels. Besides, I will go over disputes as regards international legislation ; moreover, I will shed the light on self-regulation and taxation. Furthermore, I conducted a survey to investigate the possibility of launching e-commerce section in my business in Lebanon. The forms were filled out by different bank employees and a summary of findings will be included in my paper.

TABLE OF CONTENTS

Contents

ACKNOWLEDGMENT	IV
ABSTRACT.....	II
TABLE OF CONTENTS.....	3
CHAPTER I:INTRODUCTION	5
1. LITERATURE REVIEW	5
2. RESEARCH METHODOLOGY	5
CHAPTER II: E-COMMERCE IN INTERNATIONAL RELATIONS	7
1. INTERNATIONAL RELATIONS AND NON-STATEACTORS.....	10
2. LAW AND THE INTERNET	11
3. A FRAMEWORK FOR ANALYSING STATE-PRIVATE ACTOR RELATIONS.....	11
CHAPTER III : ELECTRONIC COMMERCE.....	13
1. LITERATURE REVIEW OF E-COMMERCE	13
2. APPLICATIONS	16
2.1 <i>Payments Systems</i>	16
2.2 <i>Automated Online Assistance</i>	19
2.3 <i>Online Shopping</i>	19
<i>Information load</i>	22
<i>Consumer needs and expectations</i>	23
<i>User interface</i>	23
<i>Convenience</i>	24
<i>Lack of full cost disclosure</i>	24
2.4 <i>Online Banking</i>	25
<i>Attacks</i>	27
<i>Countermeasures</i>	28
2.5 <i>Teleconferencing</i>	28
2.6 <i>Electronic Tickets</i>	28
2.7 <i>Document Automation and Logistics</i>	29
3. GOVERNMENTAL REGULATION.....	30
3.1 <i>Federal Trade Commission</i>	31
4. GLOBAL TRENDS	33
1. IMPACTS ON MARKETS AND RETAILERS.....	33
2. DISTRIBUTION CHANNELS.....	34
2.1 <i>Pure Click</i>	34
2.2 <i>Brick and Click</i>	34
CHAPTER IV: DISPUTES INTERNATIONAL LEGISLATION.....	36
1. INTRODUCTION.....	36
2. JURISDICTIONS	36
2.1 <i>Introduction</i>	36
2.2 <i>United States Law</i>	40
2.3 <i>Practice Issues</i>	42
3. TYPES OF FORESEEABLE DISPUTES	42
3.1 <i>Contractual disputes</i>	42
3.2 <i>Non-contractual disputes</i>	43
4. CONFLICT MANAGEMENT AND AVOIDANCE.....	44
5. FORM OF DISPUTE RESOLUTION.....	45
5.1 <i>Court Litigation or Alternative Dispute Resolution (ADR)</i>	45

5.2	Other Dispute Resolution Methods.....	45
6.	ONLINE DISPUTE RESOLUTION.....	46
6.1	What is Online Dispute Resolution (ODR).....	46
6.2	Standards for ODR providers.....	47
6.3	Criteria for Selection of ODR Provider.....	47
7.	OTHER LEGAL ISSUES.....	50
8.	TRUSTMARKS.....	51
CHAPTER V: SELF-REGULATION.....		52
1.	THE MIRACLE OF SELF-REGULATION.....	52
1.1	Definition of SR.....	52
1.2	Reasons and Motives for SR.....	54
1.3	Benefits of Drawbacks.....	55
1.4	Types of SR.....	57
1.5	Instruments of SR.....	58
2.	THE CODE OF CONDUCT AS ONLINE SELF REGULATING INSTRUMENTS.....	59
2.1	Definition and Variation.....	60
2.2	A Properly Designed Code.....	61
2.3	Preliminary Questions.....	62
2.4	Spectrum of Government Involvement.....	63
2.5	Principals of Good Code Making.....	64
2.5	Framework for a Code.....	64
3.	CRITICAL SUCCESS FACTORS.....	65
3.1	A Closer Look at Enforcement.....	65
3.2	Trustmark.....	67
CHAPTER VI : PRIVACY IN E-COMMERCE.....		69
1.	E-COMMERCE FRAMEWORK AND PRIVACY ISSUES.....	69
2.	CORPORATE MARKET VALUES.....	69
2.1	Corporate Practices.....	69
CHAPTER VII : SURVEY RESULTS AND ANALYSIS.....		78
1.	SURVEY RESULTS ANALYSIS WITH THREE MAJOR BANKS IN LEBANON AND MANY OF THEIR MANAGERS.....	78
1.1	TRUST.....	78
1.2	Technology.....	79
1.3	Workforce Issues.....	79
1.4	Public Policy.....	79
1.5	Taxation.....	80
1.6	Business Processes.....	80
2.	BARRIERS FACING ELECTRONIC COMMERCE.....	80
2.1	Trust Related Issues.....	80
3.	TRUST EFFECT E- COMMERCE.....	81
3.1	Understanding Electronic Commerce.....	81
3.2	Technology Constraints.....	82
4.	COSTS IN E- COMMERCE.....	82
5.	INTERNAL BUSINESS PROCESS IN E- COMMERCE.....	82
6.	WORKFORCE BARRIERS AND GROWTH IN E- COMMERCE.....	83
7.	TAXES IN E- COMMERCE.....	83
8.	PUBLIC POLICY BARRIER IN E- COMMERCE.....	83
8.1.	State of Privacy Regulation.....	84
8.2.	Internet Privacy Self Regulation Schemes.....	85
9.	BANKS MEMBERS AND CUSTOMERS.....	88
CONCLUSION.....		89
RECOMANDATIONS.....		92
BIBLIOGRAPHY.....		94
APPENDIX.....		98

CHAPTER I:INTRODUCTION

“Electronic commerce (business transactions on the Web) and the information technology (IT) industries that make “e-commerce” possible are growing and changing at breathtaking speed, fundamentally altering the way people produce, consume, communicate and play.”

1. LITERATURE REVIEW

There is no doubt that e-commerce is on the rise globally. While the global B2C¹ e-commerce industry generated between \$400 billion and \$600 billion in 2010, estimates say that the global market will generate between \$700 billion and \$950 billion in 2015.

The pace of technological development and the borderless environment created by the Internet drives a new model for government and private sector responsibilities. Creating the optimal conditions for the new digital economy to increase requires a new, much less restrictive approach to the setting of rules.

2. RESEARCH METHODOLOGY

This research is based on a study of journals, websites, text books and a survey that I myself conducted through banks. Many theories have been proposed to explain the concept of e-commerce and its implementation worldwide. Although the literature covers a wide variety of such definitions and implementations, this review will focus on five major themes. These themes are: international law of e-commerce, disputes in international legislations, self-regulation and privacy in e-commerce. Although the literature presents these themes in a variety of contexts, this paper will primarily focus

¹Business-to-customer : marketing refers to the tactics and best practices used to promote products and services among consumers

on the disputes and legislation of a Global Regulatory Scheme which will Eliminate Conflicts of Law and Promote International E-Commerce Transactions.

I am a businessperson and I chose the topic of e-commerce on the hope of expanding the scope of my business hence. I tried as much as possible to give a comprehensive notion of e-commerce and its regulatory scheme. I conducted a study on the spread of what is called e-commerce in Lebanon, the country where my business is established. I have prepared a questionnaire and I passed it to many officials in three different banks. The following questions will be answered throughout my thesis: what is e-commerce in the notion of international relations? what is electronic commerce? What are its applications? What are the governmental regulations that are implemented among state? What kind of disputes arises in international E-commerce relations? What is the purpose of self regulation? What is the impact of the privacy act on e-commerce? And, will there be a possibility to launch an e-commerce section in my own business in Lebanon?

CHAPTER II: E-COMMERCE IN INTERNATIONAL RELATIONS

There are many worldwide and country specific rules, regulations and laws that govern how websites and in particular ecommerce enabled website should be presented, work and what content should feature on them. The law of International Trade can loosely be divided into three general areas. First, the general rules of Public International Law governing the economic relations of states. This law, which is derived both from general principles and treaty law, sets the framework within which states may legislate and under which International Trade is conducted. Second, the Law of Contracts by which persons, companies and state trading enterprises, order their trading relationship. Third, the laws governing the Importation and Exportation of goods to and from the state. International law can mainly be found in international agreements or conventions, in addition to a set of commonly recognized values, standards and principles, which do not necessarily have to be explicitly referred to in an agreement. International agreements can be bilateral² or multilateral³. Very often, they are prepared and negotiated within an international organization such as the United Nations (UN)⁴, the Council of Europe and many others. An important source of international law is also the case law of international courts. Private international law - or conflict of laws - a set of rules of procedural law which determines which legal system governs and the law of which jurisdiction apply to a given legal dispute. These rules apply when a legal dispute has a crossborder element such as a contract agreed by parties located in different States or when the crossborder element exists in a multi-jurisdictional country such as the United Kingdom.

No-one likes to pay too much tax, and the overall burden of tax in the world's larger business jurisdictions is heavy not just in itself, but also imposes substantial and worsening administrative burdens on a business. Regulation in general just gets more and more complex, in addition. Prior to the

²between two sovereign states

³between more than two states

⁴ an intergovernmental organization

Internet, there was little that most types of business could do to reduce tax and regulation, although individual owners were often able to go 'offshore'⁵ with the proceeds of their work, and increasingly did so as tax levels rose. Individual tax levels have fallen back to some extent, and in some countries, but the taxman has become more efficient, and the classical equation of working onshore and enjoying offshore becomes ever harder to sustain. Let's take this case study to understand how to choose a jurisdiction and in set up an offshore e-commerce operation.

On April 7, 2005, the World Trade Organization's appellate body ruled on a dispute over services between the United States and the state of Antigua and Barbuda⁶. The US had taken various measures that had made it much more difficult for US citizens to access online gambling and betting services based on Antiguan territory. In particular, US authorities had sought to prevent third party businesses, such as banks and credit card agencies, from allowing financial transactions between US-based gamblers and Antiguan gambling websites. This led the Antiguan government to take an action at the World Trade Organization, claiming that US behaviour violated the commitments it had made to free trade in services. The details of the World Trade Organization's final decision (which seemed to favour the US) are of more interest to international trade lawyers than to most scholars of international politics. However, the underlying dispute between the US and Antigua speaks directly to an important lacuna in our theories of international relations - how and when states rely on private actors to achieve policy goals. In pressing credit card agencies and banks into service as regulators of the offshore gambling industry, the US was using private actors as proxies to achieve international outcomes that it would otherwise have had difficulty in achieving. These actions "effectively prohibited all supply of gambling and betting services from Antigua to the US" (Sanders 2004)⁷, although they may prove ineffective in preserving the US gambling regime over the longer term. State-private actor relationships of this kind play a key role in many areas of international economic regulation. States are increasingly willing to use

⁵extraterritorial

⁶ <http://www.wto.org/>

⁷ annual meeting of the Law & Society Association

private actors as proxies to achieve policy goals at second hand. Moreover, the relative ability of states to influence private actors can have important implications for international and domestic political outcomes. In order to understand why, it is necessary first to appreciate the nature of the underlying problem. Briefly put, globalization, and in particular the rapid increase in the flows of financial resources and information across borders, have important consequences both for policy interdependence and the role of the state. The weakening of controls on cross-border information and resource flows is leading to a far greater degree of interdependence between states' domestic policies than had existed. Increasingly, one state's domestic choices over how to regulate information flows have implications for the choices of other states. The rapid development of e-commerce and the Internet have led to international controversy in sensitive social areas such as access to gambling, pornography and extremist political material. Any individual state will find it difficult to control the materials or services that their citizens have access to, when other states allow the dissemination of these materials or services on the Internet. This means, as Suzanne Berger⁸ (2000) has noted, that increased interdependence is leading to a new politicization of the state as a protector of social values that are challenged by economic and informational flows across borders. As information flows across state borders increase, and as the domestic policy choices to regulate certain kinds of information (say, to ban pornography) are undermined, so we may expect increasing demands placed upon states, to regulate these flows and restore the status quo ante. One way in which states can do this is to press private actors into service as regulators on their behalf, in policy areas where the states themselves lack the tools or expertise to provide effective regulation (Mattli and Büthe 2005)⁹. In order to prevent undesired cross-border flows of information, states will often be tempted to turn, as the US did, to key private actors which can then police information flows on their behalf. International relations theory has trouble in answering these questions; it is only in the last decade or so that it has really begun to advance testable propositions about the role of private actors in the global economy. Most work to date has focused on examining how private actors may influence states, or how

⁸ Professor of Political Science <http://web.mit.edu/polisci/people/faculty/suzanne-berger.html>

⁹ The Politics of Private Rule-Making in the Public Interest

private actors might (or might not) be creating separate spheres of governance for themselves, independent of state authority. Until very recently, (Büthe and Mattli 2005), little sustained attention has been paid to the question of how and when states might seek to influence private actors, or work through them. Private actors play an especially important role in the governance of many aspects of e-commerce and the Internet. Legal scholars have engaged in a wide-ranging debate of what this means, but with a few exceptions (Kobrin 1998, Farrell 2003, Drezner 2004)¹⁰, there has been little effort to connect this debate to the arguments being conducted in parallel in political science. While the legal academic literature is largely oriented either towards empirics or towards normative questions, it provides important insights. In particular, some legal scholars (Benkler 2000, Zittrain 2003, Birnhack and Elkin-Koren 2003, Reidenberg 2005)¹¹ have begun to ask interesting questions about the intersection between the formal jurisdiction of states and their ability to influence private actors. Even though this vein of scholarship has sought more to offer a nuanced description than to provide testable propositions, it can be developed to offer some interesting hypotheses.

1. INTERNATIONAL RELATIONS AND NON-STATE ACTORS

International relations theory has historically been a profoundly state-centered discipline, at least in North America. Dominant strains of thought (most prominently realism) have argued that state interaction and the forces which structure it are at the core of international politics. Until quite recently, non-state actors have only been studied at the margins of the discipline. Although some early work (Nye and Keohane 1971, Keohane and Ooms 1975)¹² illustrated that a variety of non-state actors had consequences for international politics, it did not go beyond this observation to create the theoretical basis necessary for a sustained debate. Accordingly, serious debate about the role of private actors and

¹⁰ Study the Problem of Multilateralism Globalization and Politics Organised Interests and the State www.researchgate.net/.../228156934_Regulating_Information_Flows_State.

¹¹ Study Code and other laws of cyberspace

¹² Study the Transnational Relations and World Politics Conclusion www.unc.edu/~lmosley/MosleyFinRegulationMay2005.pdf

their relationship to the state system was usually conducted by international relations scholars who self consciously disassociated themselves from the North American main stream.

2. LAW AND THE INTERNET

Debates among legal scholars over the political implications of ecommerce and the Internet provides an important set of complementary insights into the changing relationship between states and private actors. In addition to discussing how new technological developments would affect specific areas of the law, legal academics have engaged in a far more wide reaching discussion of the implications of the Internet for law, politics and society. These debates have centered around two issues that are of direct relevance to political scientists - the extent to which the Internet and e-commerce have empowered private actors vis-à-vis governments, and the extent to which the Internet and ecommerce challenged basic notions of states' territorial jurisdiction.

3. A FRAMEWORK FOR ANALYSING STATE-PRIVATE ACTOR RELATIONS

Building on the existing literatures in international relations and Internet law, I argue that three factors are likely to affect states' desire and ability to press private actors into service as regulators on their behalf. First, and most obvious, is states' need (or lack of same) to deal with problems of policy interdependence in a given issue area. Building on Fromkin's arguments about regulatory arbitrage, I argue that this will depend on the degree of homogeneity¹³ or heterogeneity of states' regulatory preferences and practices. Second, is the presence or 'absence' of suitable private actors in a given issue area. Here, I borrow from Zittrain¹⁴, and from Birnback and Elkin-Koren, to argue that this will depend on whether or not there are private actors that serve as 'points of control.' Finally, building on the existing literature in international relations theory, I argue that states' bargaining power vis-a-vis private actors will determine their ability to press suitable private actors into service on their behalf.

¹³ the quality or state of being homogeneous

¹⁴ www.law.harvard.edu/faculty/directory/10992/Zittrain

As the introduction argues, globalization and the Internet do not confront states with a loss of authority so much as with a new set of challenges stemming from increased policy interdependence.

Private actors are not empowered vis-a-vis states in any absolute sense, and are highly unlikely to take up the reins of command.

CHAPTER III : ELECTRONIC COMMERCE

1. LITERATURE REVIEW OF E-COMMERCE

The connotation of e-commerce has changed throughout the last 30 years. Initially, electronic commerce was destined to facilitate commercial dealings by electronic means, via technologies introduced in 1970 such as Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT), letting businesses emit marketable files like purchase orders or statements by e-mail. Credit cards, automated teller machines (ATM) and telephone banking in the 1980s were as well methods of automated commerce, not to mention the airline reservation system typified by Sabre¹⁵ in the USA and Travicom¹⁶ in the UK.

Starting the 1990s forwards, electronic commerce comprised company resource development structures (ERP), data removal and data stockpiling of security.

The first physical goods was the Boston Computer Exchange, a marketplace for used computers launched in 1982. Besides, American Information Exchange, an online information marketplace, including online consulting, was introduced in 1991.

The Worldwide Web browser was invented by Tim Berners-Lee¹⁷ In 1990, transforming an academic telecommunication network into a worldwide everyman everyday communication system called internet/www. However, E-commerce commercial business on the Internet was severely banned up until 1991. In spite of the introduction of online shopping, security protocols and DSL weren't available before five years allowing continual connection to the Internet. Several European and American commercial businesses presented their services via the World Wide Web in the late 2000. Ever since, publics started to subordinate a term "e-commerce" with the aptitude of buying different merchandises over the Internet utilizing secure protocols and electronic payment services.

¹⁵ global technology company

¹⁶ first multi-access reservation system

¹⁷ www.w3.org/People/Berners-Lee/

A timeline for the development of e-commerce:

- 1971 or 1972: The ARPANET "the seminal act of e-commerce"
- 1979: Michael Aldrich the first online shopping system.
- 1982: Minitel for online ordering.
- 1983: first hearing on "electronic commerce"
- 1984: first B2C online shopping and
- 1984: the Electronic Mall in the USA and Canada
- 1984: an Electronic Commerce Act defining basic consumer rights online
- 1990: the first web browser, worldwide Web, using a NeXT computer.
- 1992: a commercial sales website selling books online with credit card processing.
- 1992: Future Shop: How New Technologies Will Change the Way We Shop and What We Buy
- 1992: a fully graphical, iconic navigated Bulletin board system online shopping using RoboBOARD/FX
- 1993: the first AppStore, The Electronic AppWrapper
- 1994: the Navigator browser, Mozilla
- Late 1994: Netscape 1.0 with SSL encryption that made transactions secure.
- 1995: The US National Science Foundation lifting its former strict prohibition of commercial enterprise on the Internet
- 1995: the purchase of a book by Paul Stanfield¹⁸, Product Manager for CompuServe UK
- 1995: the first commercial-free 24-hour, internet-only radio stations
Dell and Cisco 's aggressive use of Internet for commercial transactions
EBay founded by Pierre Omidyar¹⁹ as AuctionWeb.
- 1996: IndiaMART B2B marketplace in India.

¹⁸ www.zoominfo.com/p/Paul-Stanfield/3293332

¹⁹ www.biography.com/People

- 1996: ECPlaza B2B marketplace in Korea.
- 1996: Sellerdeck, the UK's first PC/LAN e-commerce platform
- 1998: Electronic postal stamps purchased and downloaded for printing from the Web
- 1999: Alibaba Group in China. Business.com sold for US

The peer-to-peer filesharing software Napster

ATG Stores launches to sell decorative items for the home online.

- 2000: The dot-com bust
- 2001: Alibaba.com achieved profitability
- 2002: eBay acquires PayPal

Niche retail companies Wayfair and NetShops

- 2003: Amazon.com first yearly profit.
- 2004: DHgate.com, China's first online b2b transaction platform
- 2007: Business.com acquired by R.H. Donnelley for \$345 million
- 2009: Zappos.com acquired by Amazon.com

Retail Convergence, operator of private sale website RueLaLa.com, acquired by GSI

Commerce

- 2010: Groupon rejection of a lucrative offer from Google
- 2011: Quidsi.com, parent company of Diapers.com, acquired by Amazon.com

GSI Commerce, a company for brick and mortar businesses, acquired by eBay

- 2012: US eCommerce and Online Retail sales achievement of an increase of 12 percent over 2011
- 2012: US eCommerce and Online Retail holiday soaring sales

2. APPLICATIONS

2.1 Payments Systems

Online Payment Basics

Cash, checks, credit cards, and debit cards

Scrip: Any substitute for currency which is not legal tender, and is often a form of credit, such as Digital cash minted by a company instead of by a government (e.g., Linden Dollars)²⁰, Gift certificates or gift cards, and Subway tokens or arcade tokens.

Payment Cards(all types of plastic cards used to make purchases)

- Credit card which has a spending limit based on a user's credit history
- Debit card which removes an amount from a cardholder's bank account or transfers it to the seller's bank account
- Charge card which carries no spending limit, and amount charged is due at the end of the billing period

Electronic Cash which is a term that describes any value storage and exchange system created by a private entity that does not use paper documents or coins and can serve as a substitute for government-issued physical currency. It is attractive in two arenas: Sale of goods and services of less than \$10 and Sale of goods and services to those without credit cards.

Advantages of electronic cash: Transactions are more efficient and transfer on the Internet costs less than processing credit card transactions. As for the disadvantages, its use provides no audit trail, Problem of money laundering arises, and susceptible to forgery.

Cryptographic algorithms, which are Keys to creating tamperproof electronic cash that can be traced back to its origins, provide security for Electronic Cash

Electronic Cash Systems

CheckFree which is the largest online bill processor in the world and it provides online payment processing services

²⁰ www.investopedia.com/terms/l/linden-dollar.asp

Clickshare which is an electronic cash system aimed at magazine and newspaper publishers

PayPal²¹ which provides payment processing services to businesses and to individuals and Peer-to-peer (P2P) payment system.

Electronic Wallets which hold credit card numbers, electronic cash, owner identification, and contact information; they give consumers the benefit of entering their information just once and make shopping more efficient. It also includes server-side electronic wallet which stores a customer's information on a remote server belonging to a particular merchant or wallet publisher, and Client-side electronic wallet that stores a consumer's information on his or her own computer

Stored Value Cards which can be an elaborate smart card with a microchip that records currency balance and common stored-value cards include: Prepaid phone, copy, subway, and bus cards.

Magnetic strip cards which cannot send or receive information, cannot increment or decrement value of cash stored on the card, and processing must be done on a device into which the card is inserted.

Smart cards which are stored-value cards can hold private user data, such as financial facts, can store about 100 times more information than a magnetic strip plastic card, and are safer than conventional credit cards

Phishing Attacks Other Cards include basic structure where attacker sends e-mail messages to a large number of recipients, message states that an account has been compromised and the matter should be corrected, message includes a link, user enters a login name and password, which the perpetrator captures, and once inside a victim's account, the perpetrator can access personal information.

Counter measures: Most important step that companies can take today is to educate Web site users, many companies contract consulting firms that specialize in anti-phishing work, and anti-phishing technique is to monitor online chat rooms used by criminals.

Enterprise Content Management

The 1990's has provided innovations in network technologies, such as storing and organizing data so that they can be shared by persons and several information systems. Technologies used to

²¹ www.investopedia.com/terms/l/linden-dollar.asp

manage the content of assets like documents, web sites, intranets, and extranets are referred to the term Enterprise Content Management (ECM) which has been broadly implemented by software product sellers and experts in both organizational and inter-organizational settings. However, only little attention has been given to ECM in the information systems research community. According to this editorial, ECM offers a significant and multifaceted subfield of Information Systems as well as a framework to promote and direct future research, and summaries research topics definite to the arena of ECM. The latter covers document management, web content management, search, collaboration, management, digital (DAM), work-flow management, retention and scanning. ECM main target is to manage the life-cycle of information from first publication or creation all the way through archival and ultimately disposal besides covering the management of information within the whole range of a business whether those data are in the form of a paper document, an automated file, a database print stream, or even an electronic mail. Solutions may well offer intranet services to workforces (B2E), in addition to comprising business entries for business-to-business (B2B), business-to-government (B2G), government-to-business (G2B), or other business connections²². Most former document-management groupware and workflow solutions that have not yet entirely transformed their architecture to ECM are included in this category, but offer a web interface. Moreover, numerical asset management is a type of ECM involved in content stockpiled via numerical technology.

Government standards, including HIPAA, SAS 70, BS 7799 and ISO/IEC 27001, are elements in evolving and using ECM. Standards amenability may render subcontracting to licensed service suppliers a feasible substitute to an internal ECM distribution.

The Association for Information and Image Management (AIIM) International, the international organization for Enterprise Content Management, stated the term in 2000. AIIM has enhanced the abbreviation ECM quite a few times to reveal the increasing range and significance of information management.

²² worldwidescience.org/topicpages/n/nebraska+flood+plain+management.html

Microsoft and Oracle Corporation merged with established leaders such as EMC Documentum, Laserfiche & Open text and took part in the entry-level "value" market section of ECM. Open source ECM merchandises are as well accessible, comprising Alfresco, LogicalDOC, Sense/Net, eZ

Nowadays, establishments can implement a particular, adaptable ECM system to administer information in all practical sections, together with consumer service, accounting, human resources, etc. ECM aims to simplify storage, security, version control, process routing, and retention. The welfares to a business require enhanced effectiveness, better jurisdiction, and reduced charges.

2.2 Automated Online Assistance

An automated online assistant is a database that employs manmade aptitude to offer customer service or other help on a website. Such an associate may essentially comprise a negotiation system that is capable of interpreting the human-generated input into a numerical format that the computerized online associate can utilize for supplementary handling by its expert system, an avatar²³, and a professional system to deliver specific proficiency to the consumer that operates to identify the necessities of customers so as to implement appropriate responses by different organized systems. It delivers customer service during 24 hours a day and 7 days a week. automated online subordinates can also be applied via Twitter, or Windows Live Messenger. Popular online portals like eBay and PayPal are correspondingly utilizing multilingual computer-generated negotiators to present online care to their customers.

In the travel segment, certain new age groups are also using computer-generated negotiators to present online transactions and customer care.

2.3 Online Shopping

Business-to-consumer (B2C) online shopping or online retailing: a type of electronic commerce which opens the way for costumers to electronically purchase merchandises or services from a vendor by means of a web browser.

²³an interactive online character or automated character which makes the automated online associate a form of embodied negotiator

E-web-store, e-shop, e-store, Internet shop, web-shop, web-store, online store, online storefront and virtual store: Online store interfaces

Mobile commerce (or m-commerce) : buying from an online merchant's mobile optimized online site or app.

Business-to-business (B2B) online shopping : a business buys from another business

The first World Wide Web server and browser for commercial use, created by Tim Berners-Lee in 1990²⁴

Alibaba, Amazon.com and eBay: The largest online retailing corporations where Online customers have to have access to the Internet and a legal method of payment so as to do a transaction.

Logistics

Essentially, consumers search for a product by visiting the retailer's website using a shopping search engine. Shopping cart software is a program that allows the consumer to pile up manifold stuffs and to regulate amounts, like filling up a corporal shopping cart or basket in a traditional store. Payment and delivery information is collected via a "checkout". However, consumers are permitted to sign up for a permanent online account by some sores so as to some or all of this information only needs to be entered once, noting that the consumer often receives an e-mail validation as soon as the deal is done.

Payment

Online shoppers Payment methods: a credit card or a PayPal

Billing to mobile phones and landlinesCash on delivery (C.O.D.)

Cheque/ Check ,Debitcard

Direct debit in some countries

Electronic money of various types Gift cards

Postal money order

Wiretransfer/delivery on payment

Invoice

²⁴ www.livinginternet.com › [World Wide Web](#) › [History](#)

It is important to note that several online stores will not agree to take international credit cards. Some insist on both the purchaser's billing and shipping address to be in the same country as the online shop's base of operation. Other online shops let consumers from any nation to mail gifts anywhere. It is also essential to be aware of the fact that the financial part of a transaction may be processed in real time , such as letting the consumer know their credit card was declined before they log off, or may be done afterwards as part of the completion procedure.

Product Delivery

The following methods reflect the delivery of goods once a payment has been accepted:

- Downloading/Digital distribution: for digital media products such as software, music, movies, or images.
- Drop shipping: the passage of the order to the manufacturer or third-party distributor, for shipping the item directly to the consumer, bypassing the retailer's physical location to save time, money, and space.
- In-store pick-up: a local store is selected by the customer using a detector software and picks up the provided product at the designated location

Shipping: The shipment of the product to a customer-designated address.

Will call, ICOBO25, or "at the door"²⁶ pickup: picking up of pre-purchased tickets for an event, such as a play, sporting event, or concert, either just before the event or in advance.

Shopping cart system

²⁵ in Care Of Box Office

²⁶ www.fortricks.in/what-about-online-shopping-and-how-to-use/

- Plain systems permit the off-line administration of products and categories. The store is then created as HTML documents and visuals that can be transferred to a web space, noting that the systems do not use an online database.
- A sophisticated solution can be purchased or borrowed as a separate program or as an supplement to an business resource planning program. It is generally connected to the company's webserver and may incorporate into the existing supply chain so as to ordering, payment, delivery, accounting and warehousing can be computerized considerably.
- Other solutions let the consumer sign up and create an online store on a portal that hosts manifold shops concurrently
- Open source shopping cart packages consist of cutting-edge platforms such as Interchang .
- Commercial systems can as well be custom-made thus the store does not have to be created from scratch. By utilizing an existing framework, software components for different functionalities necessary for a web shop to be adjusted and united.

Design

Customers are attracted to online shopping owing to wide-ranging choices, competitive pricing, and greater access to information. Business organizations search for offering online shopping for the reason that it offers entry to a international market, improves customer value, and shapes supportable abilities.

Information load

Creators of online shops are worried about the side effects of data load. Information load is a creation of the three-dimensional and temporal engagements of motivations in the webstore. Compared with standard retail shopping, the data atmosphere of computer-generated shopping is improved by offering

supplementary product information such as relative products and services, along with different substitutes and features of each alternative, etc.

Consumer needs and expectations

A successful webstore in addition to publishing information is about creating a connection with consumers and making money. Oftentimes, businesses create webstores that back up the establishments' culture and brand name without fulfilling consumer expectations. Understanding the customer's requirements and wants is indispensable. Fulfilling the company's promises offers customers a motive to return and meeting their expectations offers them a cause to keep on, noting that age, gender, experience and culture are all chief elements.

User interface

The most significant elements defining whether consumers come back to a website are easiness of use and the availability of user-friendly features. Usability testing is essential for discovering complications and enhancements in a web site, such as heuristic evaluation, cognitive walkthrough, and user testing.

MarketShare

- Forrester Research²⁷ estimates that the United States online retail industry will be worth \$279 billion in 2015.
- There were 242 million people shopping on-line in China in 2012

²⁷ www.forrester.com/

Advantages

Convenience

Online stores are usually accessible 24 hours a day, and several customers have Internet access equally at work and at home in addition to other enterprises such as internet cafes and schools which provide internet access as well.

Information and reviews

Online stores describe products for sale with text, photos, and multimedia files

Price and selection

One advantage of shopping online is being able to quickly search for transactions for stuffs or services delivered by various sellers.

Disadvantages

Fraud and security concerns

Given the lack of ability to inspect merchandise before purchase, consumers are at higher risk of fraud than face-to-face transactions. Merchants also risk fraudulent purchases using stolen credit cards or fraudulent repudiation of the online purchase

Lack of full cost disclosure

While it may be easy to compare the base price of an item online, it may not be easy to see the total cost up front. Additional fees such as shipping are often not visible until the final step in the checkout process.

Privacy of personal information

Many consumers wish to avoid spam and telemarketing which could result from supplying contact information to an online merchant.

Many websites keep track of consumer shopping habits in order to suggest items and other websites to view.

Product suitability

Products less suitable for e-commerce include products that have a low value-to-weight ratio, products that have a smell, taste, or touch component, products that need trial fittings—most notably clothing—and products where colour integrity appears important.

Impact of reviews on consumer behaviour

One of the great benefits of online shopping is the ability to read product reviews, written either by experts or fellow online shoppers.

2.4 Online Banking

Online banking²⁸ lets customers of a financial institution to handle monetary transactions on a protected website functioned by the institution, which can be a retail or virtual bank, credit union or building society.

A customer must register with the institution with passwords under various names to access a financial institution's online banking facility. The password for online banking is normally not the same as for telephone banking. Financial institutions now routinely allocate customer numbers (also under various names), whether or not customers intend to access their online banking facility. Some financial institutions have set up additional security steps for access, but there is no consistency to the approach adopted.

Features of online banking

Online banking facilities offered by various financial institutions have many features and capabilities in common, but also have some that are application specific.

²⁸ Internet banking or E-banking en.wikipedia.org/wiki/Online_banking

The common features fall broadly into several categories:

A bank customer can perform non-transactional tasks through online banking, including -viewing account balances, viewing recent transactions, downloading bank statements, viewing images of paid cheques, ordering cheque books, download periodic account statements, Downloading applications for M-banking, E-banking etc.

Bank customers can transact banking tasks through online banking, including -

Funds transfers between the customer's linked accounts ,Paying third parties, including bill payments and telegraphic/wire transfers Investment purchase or sale ,Loan applications and transactions, such as repayments of enrollments ,Register utility billers and make bill payments. Some financial institutions offer unique Internet banking services, such as importing data into personal accounting software. Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions.

Modern home online banking

The precursor for the modern home online banking services were the distance banking services over electronic media from the early 1980s²⁹.

The term online became popular in the late '80s and referred to the use of a terminal, keyboard and TV (or monitor) to access the banking system using a phone line.

Online services started in New York in 1981 when four of the city's major banks offered home banking services using the videotext system

The UK's first home online banking services known as Homelink were set up by Bank of Scotland for customers of the Nottingham Building Society³⁰ (NBS) in 1983. The system allowed on-line viewing of

²⁹ ebank.li/history.html

³⁰ a building society

statements, bank transfers and bill payments. The NBS set the details up on the Homelink system.

Typical recipients were gas, electricity and telephone companies and accounts with other banks.

Stanford Federal Credit Union was the first financial institution to offer online internet banking services to all of its members in October 1994.

Security

Financial institutions have set up various security processes to reduce the risk of unauthorized online access to a customer's records, nonetheless there is no consistency to the various approaches adopted.

The use of a secure website has become almost universally adopted. Though single password authentication is still in use, it by itself is not considered secure enough for online banking in some countries.

The PIN/TAN³¹ system is used for the login and TANs representing one-time passwords to authenticate transactions. The most secure way of using TANs is to generate them by need using a security token. Usually online banking with PIN/TAN³² is done via a web browser using SSL secured connections, so that there is no additional encryption needed. The Keys for the signature generation and encryption can be stored on smartcards or any memory medium, depending on the concrete implementation.

Attacks

Phishing and pharming are the attacks used to deceive the user and steal login information. Cross-site scripting and keylogger/Trojan horses can also be used.

They manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background. The most recent kind of attack is the so-called Man in the Browser attack, where a Trojan horse permits a remote attacker to modify the destination account number and also the amount.

³¹ Password and Transaction authentication number

³² www.tutorgigipedia.com/ed/Online_banking

Countermeasures

Several countermeasures are being tried to avoid attacks. Digital certificates are used against phishing and pharming, the use of class-3 card readers is also a measure to avoid manipulation of transactions by the software in signature based online banking variants. To protect their systems against Trojan horses³³, users should use virus scanners and be careful with downloaded software or e-mail attachments.

2.5 Teleconferencing

A teleconference or teleseminar is the live exchange and mass articulation of information among several persons and machines remote from one another but linked by a telecommunications system. The telecommunications system may support the teleconference by providing one or more of the following: audio, video, and/or data services by one or more means, such as telephone, computer, telegraph, teletypewriter, radio, and television. Internet teleconferencing includes Internet Telephone Conferencing, Videoconferencing, Web Conferencing, And Augmented Reality Conferencing. Internet telephony involves conducting a teleconference over the Internet or a Wide Area Network. One key technology in this area is Voice (VOIP). Popular software for personal use includes Skype, Google Talk, Windows Live Messenger and Yahoo Messenger.

Software and Service Provider

Notable vendors are: Act Conferencing, Adobe Acrobat Connect, Co2 Neutral Conferencing, Elluminate, Glance, Gotomeeting, Intercall, Iocom, Lifesize, Meetingzone, Microsoft Office Live Meeting, My Global Conference, Polycom, Powwownow, Premiere Global Services.

2.6 Electronic Tickets

An electronic ticket is a digital ticket most commonly associated with airline issued tickets. E-ticketing has largely replaced the older multi-layered paper ticketing systems, and since 1 June 2008, it has been

³³ a non-self-replicating type of malware program

mandatory for IATA members³⁴. Where paper tickets are still available, some airlines charge a fee for issuing paper tickets. When a reservation is confirmed, the airline keeps a record of the booking in its computer reservations system.

Checking in with an e-ticket To check in for a flight with an e-ticket, the passenger usually goes to the check-in counter in the usual manner. There they may be required to present some personal identification, a credit card or the e-ticket itinerary receipt. At the check-in counter, the passenger checks-in his/her luggage and receives a boarding pass.

2.7 Document Automation and Logistics

Document automation is the design of systems and workflows that assist in the creation of electronic documents. These include logic based systems that use segments of pre-existing text and/or data to assemble a new document. Automation systems allow companies to minimize data entry, reduce the time spent proof-reading, and reduce the risks associated with human error. Additional benefits include: savings due to decreased paper handling, document loading, storage, distribution, postage/shipping, faxes, telephone, labor and waste.

In legal services

The role of automation technology in the production of legal documents has been widely recognized. For example, Richard Susskind's book 'The End of Lawyers' looks at the use of document automation software that enables clients to generate employment contracts and Wills with the use of an online interview or decision tree. Most of these companies use some element of document automation technology to provide legal document services over the Web.

³⁴ open to airlines operating scheduled and non-scheduled air services
www.iata.org › [Home](#) › [About Us](#) › [Members](#)

In insurance

Nowadays, a lot of work can go into putting one packet together. In most policy admin systems, the system will generate some kind of policy statement as a starting point, but might need to be customized and enhanced with other required materials.

3. GOVERNMENTAL REGULATION

In the United States, some electronic commerce activities are regulated by the Federal Trade Commission (FTC). These activities include the use of commercial e-mails, online advertising and consumer privacy. The CAN-SPAM Act³⁵ of 2003 establishes national standards for direct marketing over e-mail. The Federal Trade Commission Act regulates all forms of advertising, including online advertising, and states that advertising must be truthful and non-deceptive.

Internationally, there is the International Consumer Protection and Enforcement Network (ICPEN), which was formed in 1991 from an informal network of government customer fair trade organizations. The purpose was stated as being to find ways of co-operating on tackling consumer problems connected with cross-border transactions in both goods and services, and to help ensure exchanges of information among the participants for mutual benefit and understanding. Econsumer.gov, an ICPEN initiative since April 2001, is a portal to report complaints about online and related transactions with foreign companies.

Asia Pacific Economic Cooperation (APEC)³⁶ was established in 1989 with the vision of achieving stability, security and prosperity for the region through free and open trade and investment.

In **Australia**, Trade is covered under Australian Treasury Guidelines for electronic commerce, and the Australian Competition and Consumer Commission regulates and offers advice on how to deal with businesses online, and offers specific advice on what happens if things go wrong.

³⁵ first national standards for the sending of commercial e-mail and requires the Federal Trade Commission (FTC) to enforce its provisions www.business.ftc.gov/.../bus61-can-spam-act-compliance-guide-business

³⁶ www.apec.org/

In the **United Kingdom**, The FSA (Financial Services Authority)³⁷ is the competent authority for most aspects of the Payment Services Directive (PSD)³⁸. The UK implemented the PSD through the Payment Services Regulations 2009 (PSRs), which came into effect on 1 November 2009. The PSR affects firms providing payment services and their customers. These firms include banks, non-bank credit card issuers and non-bank merchant acquirers, e-money issuers, etc.

3.1 Federal Trade Commission

The **Federal Trade Commission (FTC)**, established in 1914, is an independent agency of the United States government, whose principal mission is the promotion of consumer protection and the elimination and prevention of anti-competitive business practices, such as coercive monopoly. Over time, the FTC has been delegated the enforcement of additional business regulation statutes and has promulgated a number of regulations.

a. Asia Pacific Economic Corporation

Asia-Pacific Economic Cooperation (APEC) is a forum for 21 Pacific Rim member economies that seeks to promote free trade and economic cooperation throughout the Asia-Pacific region. It was established in 1989 in response to the growing interdependence of Asia-Pacific economies and the advent of regional trade blocs in other parts of the world. APEC works are to raise living standards and education levels through sustainable economic growth and to foster a sense of community and an appreciation of shared interests among Asia-Pacific countries.

In January 1989, Australian Prime Minister Bob Hawke called for more effective economic cooperation across the Pacific Rim region. This led to the first meeting of APEC in the Australian capital of Canberra in November, chaired by Australian Foreign Affairs Minister Gareth

³⁷ www.fsa.gov.uk/

³⁸ www.fca.org.uk/static/fca/documents/fsa-psd-approach-latest.pdf

Evans. Attended by political ministers from twelve countries, the meeting concluded with commitments for future annual meetings in Singapore and Korea.

Countries of the Association of Southeast Asian Nations (ASEAN)³⁹ opposed the initial proposal, instead proposing the East Asia Economic Caucus which would exclude non-Asian countries such as the United States, Canada, Australia, and New Zealand. This plan was opposed and strongly criticized by Japan and the United States.

The first APEC Economic Leaders' Meeting occurred in 1993⁴⁰ during which some leaders called for continued reduction of barriers to trade and investment, envisioning a community in the Asia-Pacific region that might promote prosperity through cooperation. During the meeting in 1994 in Bogor, Indonesia, APEC leaders adopted the Bogor Goals that aim for free and open trade and investment in the Asia-Pacific by 2010 for industrialized economies and by 2020 for developing economies.

Member economies

The economies include: Former South Korean President Roh Moo-hyun with Japanese Prime Minister Shinzo Abe and U.S. President George W. Bush at APEC 2006 in Hanoi, Vietnam. APEC currently has 21 members, including most countries with a coastline on the Pacific Ocean. However, the criterion for membership is that the member is a separate *economy*, rather than a state. Membership of the forum includes Taiwan as well as Hong Kong, which entered APEC as a British colony but it is now a Special Administrative Region of the People's Republic of China. Besides, APEC includes three official observers: ASEAN, the Pacific Islands Forum and the Pacific Economic Cooperation Council.

³⁹ www.aseansec.org/

⁴⁰ www.apec.org/Meeting.../2006/2006.../economy_representatives.aspx

4. GLOBAL TRENDS

- In 2010, the United Kingdom had the biggest e-commerce market in the world when measured by the amount spent per capita.
- The Czech Republic is the European country where ecommerce delivers the biggest contribution to the enterprises' total revenue.
- With 384 million internet users, China's online shopping sales rose to \$36.6 billion in 2009
- E-commerce transactions between China and other countries increased 32% to 2.3 trillion yuan (\$375.8 billion) in 2012 and accounted for 9.6% of China's total international trade
- In Russia, the total ecommerce market is projected to total somewhere between 690 billion rubles (\$23 billion) and 900 billion rubles (\$30 billion) in 2015, at 2010 values.
- Brazil's eCommerce is growing quickly with retail eCommerce sales expected to grow at a healthy double-digit pace through 2014.
- India's ecommerce growth, on the other hand, has been slower although the country's potential remains solid considering its surging economy E-commerce traffic grew about 50% from 2011 to 2012, from 26.1 million to 37.5 million.
- E-Commerce is also expanding across the Middle East. Having recorded the world's fastest growth in internet usage between 2000 and 2009, the region is now home to more than 60 million internet users.
- In 2012, ecommerce sales topped \$1 trillion for the first time in history⁴¹

1. IMPACTS ON MARKETS AND RETAILERS

E-commerce, according to economists, ought to lead to increased price competition, as it intensifies consumers' ability to collect data about products and prices. Research by four

⁴¹ www.toptenwholesale.com/.../ecommerce-sales-reach-1-trillion-in-2012

economists at the University of Chicago has discovered that the development of online shopping has also had an effect on industry structure in two fields that have seen important growth in e-commerce, bookshops and travel agencies. In general, larger companies are capable of using economies of scale and offering lower prices. The only exception to this pattern has been the very smallest category of bookseller, shops with between one and four employees, which seem to have endured the trend.

2. DISTRIBUTION CHANNELS

E-commerce has grown in significance as businesses have implemented Pure-Click or Pureplay in which companies have launched a website without any previous existence as a firm and Brick and Click in which existing companies have added an online site for e-commerce.

2.1 Pure Click

Pure click companies are the companies with virtual presence or present in the internet only. Search engines, Internet service providers, commerce sites enabler sites, transaction sites etc. are the companies included in pure click company category. Amazon.com, eBay, Fabmart.com are the famous commerce sites⁴²; a transaction site which facilitate auction and brokerage. PureClick maintains high standards of data privacy and security for advertiser placement data.

2.2 Brick and Click

Bricks and clicks or WAMBAM is a business model by which a company incorporates equally offline (*bricks*) and online (*clicks*) presences, at times with the third extra *flips* (physical catalogs). In addition, many will also offer telephone ordering as well, or at least provide telephone sales support. A popular example of the *bricks and clicks* model is when a chain of stores allows the customer to order products either online or physically in one of their stores, also allowing them to either pick-up their order directly at a local branch of the store or get it delivered to their home.

⁴² managementterminology.blogspot.com/

The bricks and clicks model by maintaining a physical presence as premises and staff is still needed for the reason that some customers may wish to see the goods directly before purchase; on the other hand, online shopping may require a different convenience of shopping online and getting the order delivered when it suits them ; a bricks and clicks business model to be successful is determined by a company's ability to manage the trade-offs between separation and integration" of their retail and online businesses.

CHAPTER IV: DISPUTES INTERNATIONAL LEGISLATION

1. INTRODUCTION

Enterprise Content Management (ECM)⁴³ is the policies, techniques and implements applied to arrest, cope with, accumulate, maintain, and provide content and official papers associated with administrative procedures. ECM defends the controlling of information within the whole range of a business whether that information is in the form of a paper document, an automated file, an archive print stream, or even an electronic mail. How does the enterprise contend with such wide-ranging coverage? Validating the consumer's setting is practically difficult, particularly if the shopper profit from the various "anonymizer" tools which shield identity in Internet⁴⁴. A consumer may well have the funds for services secretly by means of the numerical equivalent of cash e.g. eCash⁴⁵ or via a service such as PrivateBuy.com⁴⁶. An online enterprise can limit its purchaser base to those authorities where it is inclined to succumb to regulation especially where merchandises necessitate a physical transport, an online enterprise. If this is the case, the enterprise may have to depend on the straightforwardness of the customer's data as regards to their setting. Several e-commerce enterprises, obviously, have come electronically precisely pursuing a global market. This section will study the efforts to settle cyberspace's jurisdictional dilemma and will reflect on other approaches for solving divergences and objections in a worldwide online marketplace.

2. JURISDICTIONS

2.1 Introduction

The creation of the Internet as a global network has raised significant jurisdictional issues at both the US interstate and international levels. According to Henry Perritt, Dean of Chicago-Kent Law

⁴³ www.aiim.org/Research-and-Publications/Glossary

⁴⁴ See Matthew P. Graven, Anonymous Browsing

⁴⁵ eCash

⁴⁶ PrivateBuy.com

School⁴⁷, jurisdiction is generally divided into three types: "Prescriptive jurisdiction limits legislative power. When a sovereign state has jurisdiction to prescribe, it legitimately may apply its legal norms to conduct. Adjudicative jurisdiction limits judicial power. When a state has jurisdiction to adjudicate, its tribunals may resolve disputes. Enforcement jurisdiction limits executive power. When a state has jurisdiction to enforce, its police, and customs authorities may restrict the flow of trade, detain individuals, and alter property interests."⁴⁸

Factually, jurisdiction was restricted by the inconvenience of implementing a verdict against someone or something over which the Federal Court has no power. Nevertheless, a supreme ruler can expand its dogmatic jurisdiction⁹ further than its implementation jurisdiction in two approaches. It can request other rulers to put in force its judgments and, where it does not have adjudicative jurisdiction, it can solicit other rulers to apply its regulations to particular disagreements. Equally courts and sovereigns, knowing restrictions on proposing regulation to controversies that have no association with the ruler, have established choice of law regulations to determine which sovereign's laws to apply. Choice of law and the enforcement of judgments are also ruled by global contract along with norms of international law. As international law has developed, esteeming the sovereignty of other nations has become an significant prevailing norm in restraining prescriptive jurisdiction and inhibiting overreaching.

International jurisdiction disputes habitually seem approximating to the "minimum contacts" matters noticed in American lawsuits, as considered below. To be applicable, jurisdiction over distant residents or companies must depend on international agreements or joint implementation treaties. These agreements often study the associates that the foreign person has within the independent region so as to define if the sovereign's concentration in the issue is genuine. For a more complete discussion of international jurisdiction and the Internet⁴⁹.The European Union ("EU") recently implemented a

⁴⁷ articles.chicagotribune.com › [Featured Articles](#) › [Legal Education](#)

⁴⁸ Perritt1

⁴⁹ please review Dean Perritt's presentation at Internet Law and Policy Forum (Website) (Perritt2) and/or the article by Stephan Wilske & Teresa Schiller (Website) (Wilske).

rule, in effect in March 2002, permitting an EU customer who buys merchandises or services online to take legal action against the vendor either in the EU state in which the customer lives or in the EU country in which the supplier is tangibly located, albeit the seller has no commercial businesses or workforces in that state.⁵⁰ In an explanatory note to the Regulation, two key EU bodies have indicated that a passive website alone (which advertises products but does not allow the consumer to order or download the products online) will not invoke the consumer jurisdiction clause.

Yahoo and the French ban on Nazi memorabilia

The most thoroughly surveyed worldwide jurisdiction case encompasses the website Yahoo and sales on its site of Nazi memorabilia. A French law court delivered a verdict that the deals, which could be salvaged by French Internet consumers, ravaged French law. After listening to a jury of specialists that it was strictly conceivable to block 70 to 90 percent of French customers from a website, the court of law allotted Yahoo 90 days to stop French users or come to terms with a fine of \$13,000 per day.⁵¹

Enforcing the ruling may be impossible for the French court, given that Yahoo has no resources in France (granting it does have an interest in Yahoo-France). Yahoo is previously opposing the verdict in U.S. in Federal District Court in San Jose, Calif., debating that the French order cannot be applied for quite a few reasons, comprising struggles with the First Amendment. Temporarily, it has willingly barred the transaction of hate group associated goods.⁵²

Most ecommerce traders want customers from all over, whether that means the 50 U.S. states, Canada, Mexico, Europe, or the world. However, e-retailers must think over local laws when they ask for business in another state or another country, noting that it is important to recognize which rules might apply to a certain online business deals. In many circumstances, laws from the consumer's state are the ones that will apply when it comes to a problem that arises. The same applies as regards the laws of

⁵⁰See the coverage in *The Industry Standard*

⁵¹For a summary of the case, see *The Industry Standard*

⁵²See the CNET article

other countries. For instance, in several European states selling anything related to the Nazis is illegal. This may appear to be rational but the law also applies to World War II souvenirs dealers. So a business holder in the United States who vends World War II collectables could confront lawful complications from European countries if anybody in one of those countries were to buy a Nazi item from him. Such a transaction occurs via the Internet and from an e-business owner. Therefore, U.S.-based ecommerce dealers should be chiefly cautious when vending in a foreign country, being sure to know each country's rules. Being aware of which state law ought to apply to a transaction in the United States may as well be a challenge. For example, if one is living in Ohio and vend a product to somebody in California and a problem occurs with the transaction, will the laws of Ohio or California apply? To further set hurdles, what if that person has a depository in Colorado and you ship from that place, now which law should apply? What if the server is located in Utah, does that state now have rule over the business deal? What Jurisdiction Applies? Jurisdiction is the process of interpreting and applying the law by a Court in a certain geographic location. Jurisdiction can be achieved by conducting business in a state. What is conducting business? The act of buying, selling, or proposing to vend something is sufficient to be measured transacting business and to convey jurisdiction. Why should one care about jurisdiction? If he comes to pass in lawsuit over his product, the worst thing is to travel across country and hire a lawyer in another state. It is much easier on both parties from a financial and time viewpoint to have a lawsuit sued in your home state. Similarly, if the other party is wanted to travel to the dealer's country to start lawsuit, they are less likely to go to court. You Want Your State's Law to Apply How can one guarantee where the lawsuit takes place? No guarantees of any kind, but he can take steps to increase the chance of his home state being the place of resolving a dispute. 1. If one is using an agreement with another party, he has to make sure to list that any dispute must be filed in his home country and that both parties to the contract approve of jurisdiction in that country. 2. On the dealer's website, when a customer is purchasing an item as one of the terms and conditions of the transaction, he should make them agree to jurisdiction in his home state in case a

dispute arise. This can be done with check box next to the statement and make them check it off prior to completing the purchase.

E-commerce jurisdiction in the EU: what law applies? Two important considerations are to be noticed when suing or being sued: which laws apply and in which country should the action take place? In Europe, there is continuing debate about these principles of jurisdiction. The E-commerce Directive, which is meant to be adopted in all Member States before 17th January 2002, necessitates EU businesses to obey only with the laws of the country in which they are based when dealing with customers, a method recognized as the country of origin standard. However, the question of where actions can take place is proving more difficult to answer.

2.2 United States Law

In the U.S., each of the 50 states has its own functional profitable laws and Federal Court structures. Every state has a rule called a "long-arm statute" which defines the people and the objects over which the native courts have authority. Under the Full Faith and Credit article of the United States Constitution⁵³ and the Implementing Act of 1790, 28 U.S.C. §1738, rulings in one state are imposed by force in all the others. Although this renders jurisdiction over people of another state practical, states are limited in their jurisdictional reach. Under the Due Process article of the Constitution, as explained by the Supreme Court in *International Shoe Company v. Washington*⁵⁴, each state court of law can only exert subjective jurisdiction over a non-resident perpetrator if the suspect has had adequate "least possible associates" with the state to validate jurisdiction. In the context of interstate commerce, a corporation from another state that sells products directly within another state is "decisively availing" itself of the laws of the other state, which is satisfactory connection to validate

⁵³Art. IV. Sec. 1

⁵⁴*International Shoe*

jurisdiction. Conversely, a state cannot exert jurisdiction over an out-of-state company that sells merchandises that unpredictably end up in the state. See *World-Wide Volkswagen Corp. v. Woodson*⁵⁵ In the framework of the Internet, a website machinist will not usually restrict its audiences or consumers to those living in a particular state. A important amount of illustrations have addressed this subject, with most following the lead of the court in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*⁵⁶. The Zippo court stated that jurisdiction should be controlled based on "the echelon of interactivity and marketable nature of the exchange of data that take place on the web site." It parted websites into three ranges:

- Fully interactive sites where users purchase goods or services, exchange information or files, or enter into agreements,
- Fully passive websites where information is available for people to view,
- Sites somewhere in the middle, with only limited interaction.

Courts are likely to find jurisdiction over the out-of-state operator of fully interactive sites, unless the operator avoided selling to those within the state or at least did not target them. In *Zippo*, the Pennsylvania court found that it had jurisdiction over the out-of-state vendor from California since the latter's website sold 3,000 passwords over the Internet to Pennsylvania subscribers and entered into seven contracts with Pennsylvania access providers. On the other end, fully passive websites are not likely to be sufficient for jurisdiction. See, for example, *Soma Medical Int'l v. Standard Chartered Bank*⁵⁷ which held that defendant's maintenance of a website accessible in Utah was not sufficient to establish personal jurisdiction where the website was purely passive in nature.

In the middle, courts have surveyed a diversity of features, comprising the number of knockouts a website gets from users within the state or the existence of an electronic mail link or free of charge number on the site. The trend has been not to stumble on jurisdiction even when certain transactions

⁵⁵Volkswagen

⁵⁶Zippo

⁵⁷Soma

have taken place. See, e.g. *Winfield Collection Ltd. v. McCauley*⁵⁸, which believed that two sales to state inhabitants through eBay's online auction was not adequate to create jurisdiction as sales stemmed from the arbitrary offers of parties beyond the perpetrator's control and not from targeting of state inhabitants. The Federal Court also discovered that the enactment of preserving a website with communicating characteristics does not alone expose the site's backer to jurisdiction anywhere in the United States. See also *Mink v. AAAA Dev. LLC*⁵⁹ weakening jurisdiction where defendant's website permitted audiences to deliver email but did not allow them to sign agreements with perpetrators electronically. Consumers were guided to issue order forms and email or fax them to perpetrator.

2.3 Practice Issues

Companies that do not desire to be exposed to jurisdiction in overseas states and republics should take into account restricting their websites to inert action. On the other hand, they could only permit inhabitants of a number of states to order stuffs on their site or partake in it, though in situations where the merchandises or services are served by electronic means it may be a hard and expensive procedure to validate the purchaser's residency. The corporation would also require to firmly restrict any non-Internet connections with overseas states. Similarly, online sellers could utilize roundtable selection and choice of law articles in the Terms of Package for the site, but see the click wrap discussion in Session 3: Transactions for information on enforceability.

3. TYPES OF FORESEEABLE DISPUTES

Heated discussions are unavoidable throughout the life of a business, whether online or offline. The business clashes which the business may come across comprise the following:

3.1 Contractual disputes

- Clashes between the business and the Internet Service Provider (ISP) or web-hosting services provider, together with disputes over disturbances in service, violation in data security etc.

⁵⁸Winfield

⁵⁹Mink

- Business-to-business (B2B) arguments between the business and its traders such as non-performance of votive commitments, misrepresentations, and objections from consumers concerning services delivered by dealers.
- Business-to-consumer (B2C) arguments between the business and its customers such as non-payment for goods or services, non-performance of votive commitments, poor enactment of agreement, misrepresentations, violation of the privacy policy, and violation of security of private information. It is between the business and its consumers that lies the greatest probable range for arguments.

3.2 Non-contractual disputes

These are the common types of non-contractual arguments that may take place in an online business.

- Patent - The business might be predisposed for copyright breach if it abuses copyrighted material in excess of reasonable usage, and with no authorization.
- Data protection - The business might be predisposed for disclosing or revealing private information on consumers, as deliberated in the section on Privacy.
- Right of free expression - The business might be predisposed to defamation outfits for defamatory material displayed online.
- Competition law, Domain name disputes - The business might be predisposed to trademark breach suits if it violates a registered or else lawfully acknowledged trademark. If the business has enumerated a domain name which agrees to a registered or common law trademark, it may be exposed to a objection under ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP)⁶⁰, or the U.S. federal Anticybersquatting Consumer Protection Act. For a discussion of the UDRP process, see the Berkman Center Online Lecture & Discussion Series by Diane Cabell, "Using ICANN's UDRP"⁶¹

⁶⁰ www.icann.org/en/help/dndr/udrp

⁶¹ Cabell.

Even though many of the subjects (e.g. jurisdiction, choice of law, high cost of cross-jurisdictional litigation) which stem with regard to the diverse classifications of arguments are analogous, the problems are possibly more marked with regard to B2C transactional clashes which are frequently of small financial significance. Customary techniques of solving cross-jurisdictional marketable arguments, such as transnational commercial adjudication, are frequently very expensive, not convenient and troublesome in the context of customer arguments. This section will hence emphasize on the controlling of arguments stemming from B2C dealings. It should though be perceived that many of the matters and values discoursed at this point are similarly applicable to other kinds of arguments.

4. CONFLICT MANAGEMENT AND AVOIDANCE

In view of the significance of consumers and referrals in business, particularly in e-commerce, it is frequently in the best interest of businesses and persons to resolve their arguments rapidly.

The enterprise may consider developing an integrated conflict management system. This includes both grievance processes and mediation, but goes beyond them, introducing a systematic approach to preventing, managing, and resolving conflict. The Society of Professionals in Dispute Resolution (SPIDR) has practical guidelines for designing and implementing such systems⁶²

The business should take into consideration creating a consumer satisfaction system. Such a system extends after-sale services by which the consumer is attracted to initially present his or her objection to such a service, for instance a call center or objection services. While consumer experience is the only most significant element in the success of e-commerce, such a system can assist in keeping consumers contented, and retain them as consumers. Nora Femenia has offered an article on how cultural diversities influence customer involvements⁶³ Most codes of practice recommended and adopted by

⁶²SPIDR

⁶³Femenia.

various trademark code owners require online merchants to establish internal complaint resolution procedures that are quick, accessible, free (or low-cost) and fair.

5. FORM OF DISPUTE RESOLUTION

In the event that the dispute is unable to be resolved through the enterprise's internal complaint resolution procedure, third party dispute resolution may be necessary between merchants and their consumers. Traditional dispute resolution processes include court litigation⁶⁴ (court adjudication), arbitration, mediation and other alternative dispute resolution (ADR) procedures. All these processes are face-to-face in a physical environment.

5.1 Court Litigation or Alternative Dispute Resolution (ADR)

It is much better for the enterprise to have the dispute resolved through ADR methods than through court litigation because of law and jurisdictional problems that arise in cross-jurisdictional transactions and by seeking to resolve the dispute through ADR, that reduces the cost of dispute resolution.

Online dispute resolution (ODR) offers the advantage of speed, reduced cost, greater convenience and accessibility without the need to physically meet. ODR therefore has the potential to significantly reduce the transaction costs arising from a dispute.

5.2 Other Dispute Resolution Methods

"Alternative" dispute resolution methods that are available from the perspective of the customer include :

- Credit card charge back mechanisms generally take a long period of time and do not involve cooperation between the consumer and the merchant to resolve the complaint. Instead the credit card company resolves it.
- Merchant complaint resolution mechanisms are complementary to ODR processes, and disputes may be referred to ODR after attempts at resolving them through the merchants' complaint resolution mechanisms have proved unsuccessful.

⁶⁴means court adjudication

- Complaints to governmental authorities and consumer protection agencies have traditionally been a popular method of resolving disputes but it is less accessible to consumers who are located in another jurisdiction.
- While small claims courts may provide a simple and low-cost forum for resolution of disputes involving small amounts, the jurisdictional and choice of law problems which arise in traditional litigation are equally applicable. For e-commerce disputes, ODR may be able to fulfill the role of virtual small claims courts.

6. ONLINE DISPUTE RESOLUTION

6.1 What is Online Dispute Resolution (ODR)

Using computer-networking technology, ODR⁶⁵ brings disputing parties together "online" to participate in a dialogue about resolving their dispute. ODR is still a fairly recent industry. ODR providers include private sector companies, public sector agencies and academic institutions. Currently, the majority of ODR providers are private sector companies.

the complainant begins the ODR process by registering the complaint online with an ODR provider. The ODR provider will then contact the other party using the information provided, and invite that other party to participate in the ODR process. If the other party accepts the invitation, he or she will file a response to the complaint.

The ODR providers employ one or more of the following dispute resolution techniques or mechanisms –first, The arbitration and mediation processes utilize email, chat or messaging software, audio-conferencing or video-conferencing software for communication between the arbitrator/mediator and the parties which parties have agreed by contract to be binding. Second, Mediation involves facilitation of communication and problem-solving by a mediator. A settlement is reached only if both parties consent. Third, Online negotiation may involve use of email or messaging, or may utilize heavily automated systems. Blind bidding refers to a system of settlement in which the ODR

⁶⁵www.consumerprotectionbc.ca/odr

provider's software accepts confidential offers and demands from the parties, and records a settlement if the offer and demand are within a pre-specified range from each other. If there is no settlement, the other party will not know what the submitted bids were. For examples of blind bidding systems⁶⁶, Some providers incorporate a technique that has been called "peer pressure" services which involve the use of publicity about the ongoing dispute to create an incentive for the online merchant to resolve the dispute.

6.2 Standards for ODR providers

In June 2000, the Federal Trade Commission (U.S.) and the Department of Commerce (U.S.) held a public workshop to explore ADR for online consumer transactions⁶⁷. In December 2000, the Organization for Economic Co-operation and Development (OECD), Hague Conference on Private International Law (HCPIIL), and International Chamber of Commerce (ICC) jointly organized a conference entitled "Building Trust in the Online Environment: Business-to-Consumer Dispute Resolution" held at the Hague, Netherlands⁶⁸.

6.3 Criteria for Selection of ODR Provider

the standards which ODR processes and providers ought to meet Independence / Neutrality / Impartiality - The ODR provider must be sufficiently independent from both the online merchant and the consumer in order to guarantee the impartiality of its actions transparently at low cost or free of charge, easily accessible to the consumer, and should provide quick decisions or settlements .

The procedure should provide a reasonable opportunity for all parties to present their viewpoints before the ODR professional and to hear the arguments and facts put forward by the other party and the dispute resolution professionals employed by the ODR provider should be properly qualified in

⁶⁶SeeCybersettle (Website) (Cybersettle) or clickNsettle (Website) (clickNsettle)

⁶⁷FTC.

⁶⁸OECD

dispute resolution. ODR providers may reach decisions or settlements based on equitable principles, and/or on the basis of codes of conduct, rather than strict legal rules.

Principle of representation - The process should permit (but not require) representation by third parties.

Some stakeholders⁶⁹ feel that the ODR process should not be in binding nature Other stakeholders feel that mandatory participation in ODR should be permissible. Some stakeholders want ODR proceedings and results to be confidential, while others want these proceedings, results and statistics to be published, as a means of ensuring public accountability. and no agreement on a universally accepted set of criteria has yet been reached.

Can/Should ODR be Made Mandatory?

An online merchant's terms and conditions for its services may require that all disputes arising from the transaction be submitted to binding arbitration an issue which arises is whether a pre-dispute arbitration agreement by a consumer should be enforceable. A pre-dispute agreement is contrasted with a post-dispute arbitration agreement, which does not create difficulty. A pre-dispute arbitration agreement is also to be distinguished from a pre-dispute agreement by the parties to refer any arising dispute to mediation, as no binding result can be achieved in that situation without the consumer's consent.

A. Enforceability of domestic arbitration agreements in the United States

In the United States The Federal Arbitration Act, 9 U.S.C.⁷⁰ is the arbitration law applicable to transactions involving interstate or foreign commerce. Section 2 of the Federal Arbitration Act provides that:

"[a] written provision in any maritime transaction or a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or

⁶⁹ A person, group or organization that has interest or concern in an organization.

⁷⁰ www.law.cornell.edu/uscode/text/9

the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."

The U.S. Supreme Court has upheld the validity of pre-dispute domestic arbitration agreements contained in commercial contracts, where it pre-empts state statutes invalidating such agreements. In *Allied-Bruce*, the Supreme Court enforced a pre-dispute arbitration agreement contained in the respondent's termite prevention contract.

A contract of adhesion is a standard form contract offered by a party with stronger bargaining power to a party with weaker power on a take-it-or-leave-it basis. Such a contract is not a result of a negotiation between the parties. In *Carnival Cruise Lines, Inc. v. Shute*⁷¹, which was a case involving a forum selection clause in a consumer contract selecting a court forum rather than arbitration, the U.S. Supreme Court enforced the forum selection clause despite the fact that it was contained in a contract of adhesion. Not all contracts of adhesion are unenforceable - only those that are unreasonable. The fact that a consumer does not read the agreement or thereafter claims to have failed to understand or appreciate some term therein does not invalidate the contract.

B. Enforceability of foreign arbitration agreements in the United States

The United States is a party to two treaties requiring the enforcement of international arbitration awards and arbitration agreements:

- United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards ("New York Convention")
- Inter-American Convention on International Commercial Arbitration ("Inter-American Convention").

The provisions of the conventions are incorporated into U.S. law through 9 U.S.C. sections 201 and 301.

⁷¹Carnival

Where a foreign arbitration clause is involved, the Federal Arbitration Act should be construed with due regard for the doctrine that the "emphatic federal policy in favor of arbitral dispute resolution . . . applies with special force in the field of international commerce." The U.S. Supreme Court has held that foreign arbitration clauses selecting a foreign forum are enforceable in the United States.

The expansion of American business and industry will hardly be encouraged, if, notwithstanding solemn contracts, we insist on a parochial concept that all disputes must be resolved under our laws and in our Courts. ... see *Mitsubishi Motors Corp v Solar Chrysler-Plymouth, Inc*, 473 US 614, 638 (1985)⁷² if International arbitral institutions are to take a central place in the international legal order, national courts will need to "shake off the old judicial hostility to arbitration",

7. OTHER LEGAL ISSUES

Enforceability / Remedies - When a dispute is successfully resolved through ODR providers, it may result in a binding or non-binding outcome. Where the dispute was resolved through mediation, the online settlement would be enforceable only to the extent allowed by contract law. One issue which may merit further consideration is the question of which state's contract law determines the validity of the settlement agreement.

Contract Formation: Transactions on enforceability of "clickwrap" agreements.

Choice of Law - The use of ODR providers for dispute resolution minimizes the jurisdictional problems related to cross-jurisdictional disputes, but does not eliminate the need to decide the choice of law question. The parties could agree on the choice of law in exercise of party autonomy, or could leave the decision to the online arbitrator.

Evidence of Agreement (of terms and of acceptance) - The use of ODR does not remove the practical difficulties associated with collecting and presenting evidence of the formation of the contract and the terms thereof.

⁷² laws.findlaw.com/us/473/614.html

Lack of Uniform Regulatory Scheme - Currently, the ODR providers set their own standards, as regulatory regimes are still being discussed and formulated. To enable ODR providers to tap the global market for dispute resolution, there would be a need for a uniform regulatory scheme across national boundaries.

8. TRUSTMARKS

Trustmarks or seals of approval are currently one of the chief mechanisms for promoting consumer confidence and self-regulation in ecommerce. Independent organizations (referred to as Code Owners) establish standards (Codes of Practice) for conducting e-commerce and certify that particular online businesses (Code Subscribers) have met those standards. The Code Subscriber is then permitted to display the Code Owner's seal or trustmark⁷³ on their website. This is expected to improve customer confidence.

Trustmark programs vary considerably in their terms and operation. Some certify only particular aspects of online business, such as privacy, while others certify a broad range of issues including advertising, disclosures, contract terms and performance, and security. Most include provisions concerning internal and/or third-party dispute resolution, and some Code Owners provide or monitor dispute resolution services involving their Subscribers. Some programs certify only that the Subscribers have accurately disclosed their own policies, while others certify that Subscribers follow the Code Owner's standards.

⁷³ cyber.law.harvard.edu › ... › [E-Commerce: An Introduction](#)

CHAPTER V: SELF-REGULATION

1. THE MIRACLE OF SELF-REGULATION

1.1 Definition of SR

Self-regulation in the context of e-commerce are according to Van Driel, “*private rules established – whether or not in cooperation with others – by those to whom they apply, or their representatives, with supervision jointly exercised by these groups.*” As for Prof. Geelhoed⁷⁴, self-regulation is considered as “*binding normative guidelines by representatives from a certain group, who is highly organized, and is able to enforce these guidelines which are based on private law and in the same sense. From the perspective of Prof. Eijlander, in case of pure self-regulation social groups are responsible for their own rules in a certain area and at the same time responsible for execution, control and enforcement of these rules. 139*” while for the Mandelkern report *self-regulation is a control of activities by the private parties concerned without the direct involvement of public authorities.*¹⁴⁰

When considering kinds and instruments of self-regulation, particularly in the context of e-commerce, the aforementioned definitions are not satisfactory. As far as I can see, *Self-regulation is a set of private rules, willingly created by a group of people or their legislatures from a specific segment of actions – on their own initiative or in cooperation with other groups involved, as well as the government– with supervision and implementation separately or cooperatively implemented by these groups.*”

1.1.1 Language Implication

⁷⁴ www.uwa.edu.au/people/elizabeth.geelhoed

The English connotation of the term “self-regulation” is not the same as the Dutch “zelfregulering”⁷⁵ or the German “Selbstregulierung”. The scope of the Dutch and German concept encompasses any “self-adjusting tendency in society” hence comprising intentional contracts, agreements and coast-to-coast organizations for technical principles too, noting that the connotation of the British self-regulation is the same.

1.1.2 The Concept of Voluntary

The voluntary concept in self-regulation legally means “without legal obligation or consideration”⁹. In everyday language the term indicates “one’s own free will”. The voluntary nature of self-regulation is centered on the fact that the self-established regulations are imposed by force on each other. Nevertheless, no organization other than the state could lawfully impose its rules on anybody. As a result, the attainment of self-regulation resides on the *voluntary* collaboration of its partakers, henceforth reaching their lawfulness.

1.1.3 Soft Law

Soft law, which is used by the European Commission to describe self-regulation, refers to operations within the legal system. The concept itself was created from public international law and includes a wide series of instruments, such as declarations of principles, codes of practice, charters, etc.

⁷⁵ www.ivir.nl/publications/sitompoel/iter-summary.pdf

1.2 Reasons and Motives for SR

Many reasons led to the failure of government regulation. The first and major reason is that public authorities are not able to legalize appropriately and in a timely fashion, especially with the fast technological modifications and the fast-tracking innovation in business products and developments caused by the pressure of international rivalry: health, safety, and quality and environment regulation. That is, a certain law could already be out-of-date during the model stage, not to mention the fact that the controller has inadequate knowledge and resources to ratify and impose all rules. The second reason for government failure lies in the fact that the contemporary varied and active society necessitates an adaptable and active modifiable government. Still, where communal control misses the mark and the “Cunning citizen” has made his entry, “above”, regulation turns out to be progressively uncontrollable and hard to impose.

What motives drive private enterprises (or their industrial organizations) to step in and fill the gap?

- The leading motorist is (let’s face it) self-interest, the “carrot”, such as the chance to distinguish a corporation (particularly if there are “cowboys” in the marketplace), or a “stick” (such as pressure and “persuasion” from communal or political groups and organizations like consumer groups) Most self-regulatory structures search for improving customer confidence where it is presently insufficient such as in capacities of new technology or where there have been difficult business practices. The needs for self-regulation will simply surface if the profits of having a self-regulation system prevail over the situation without one.
- Secondly, the most significant element is the continually existent “shadow of the law”⁷⁶: the risk of government interference with all its inadequacies. This is the concern that government regulation will

⁷⁶ en.wikipedia.org/wiki/Shadow_of_the_law

intrude or even hinder everyday industry and re-interpret prevailing rules or create new guidelines that rise costs or decrease incomes.

- The third motive is that self-regulation is not restricted to the authority of one state. State lawmakers are self-conscious for dominance and legitimate motives from creating rules with extra-territorial implementation. Argument resolution is often self-adjusted⁷⁷, to keep away from coming into view in law court in another state.

1.3 Benefits of Drawbacks

1.3.1 benefits

Provided that self-regulation take the place of or supplements government regulation, the parties concerned, led by their (rational) self-interest, benefit in the following areas:

- Self-regulation leads to establishing and changing rules faster, with less official procedure, with more diversity and /or made-to-measure resolutions. Rule implementation is faster and more flexible as it is of specific significance in active marketplaces where consumer preferences vary frequently.
- Choosing instruments for rule making and implementation leads to Freedom of choice.
- Capability of building on communal knowledge of business and consequently being able to keep up-to-date with technological and self-motivated modifications with fewer costs
- Incompatible and unsuitable lawmaking can be avoided with self-regulation
- various political and financial battles surrounding government can be avoided with self- regulation
- the distance between controlling body and to whom rules apply, is less as the benefits of all parties concerned are taken into consideration.
- Readiness to meet the terms of self-imposed rules is much higher, particularly if joined with a fast, familiar and low-priced way of heated discussion resolution
- Lawful assurance for all shareholders

⁷⁷ the so-called Alternative Dispute resolution or ADR

- Ability to implement regulations where there is no national control, especially that self- regulation knows no jurisdictional limits, a serious concern in the global economy

1.3.2 Drawbacks

Private enterprises are driven to make the most of their profits. When it comes to self-regulation, there are some specific drawbacks.

- The market model approach of self-regulation: Businesses often desire to enact their own rules and utilize their dominant rank to propose what has to be done to lesser parties often to avert more pressuring regulation.
- Awareness and practice in the range of self-regulation is limited and in spite of the fact that everybody converses about it, the number of effective application stories is limited.
- No assurance that all of the shareholders are included, so self-regulation is often organized by the large businesses and politicization clubs.
- Prompting and applying self-regulatory techniques requires a lot of time, work and capital, which has to be funded by the business. SMEs are often less capable than larger companies to handle the expenses of partaking in a self-regulatory system, chiefly when the system is sponsored by business tariffs. Bigger industries could engross the expenses, while SMEs have frequently no choice but to transmit these costs to the customer in the kind of higher costs, which might engage them in a competitive drawback to their larger counterparts.
- Often, in several self-regulatory structures, a connection with the “ strong arm of the law is missing”.
- Self-regulation does not provide security against “free-riders” or cowboys: businesses, which do not or will not adhere to the self-regulation system, and, often by misconduct, interrupt the upright intents of those who abide by self-the scheme willingly and have consumed important capitals to join. The danger could well be that government interferes and controls at any rate to penalize the “cowboys” but in so doing penalizing the “good guys” too.

- Unfair competition and even anti-trust problems where two or more companies come up with an agreement concerning the market are a drawback of self-regulation.
- The possible defensive influence of self-regulation could constrain governments to create stricter lawmaking at a later phase.
- Private businesses have their own rules and when legalizing themselves, the danger surfaces to the extent that they create rules stricter and more comprehensive than government rules.

1.4 Types of SR

The differentiation in types of self-regulation is not deprived of complications. The European Commission⁷⁸ differentiates among three groups: self-regulation, intentional arrangements and co-regulation. The general interpretation is the difference between self-regulation with workers in a segment who come to an agreement among themselves on the one hand (pure self-regulation) and on the other hand self-regulation which fits in with a lawful structure (co-regulation). This has been in use as a starting point to make below stated classification.

State regulation and self-regulation

- Rules of self-regulation by private enterprises

To start with, the government does not interfere with codes of conduct whenever they are compatible with the existing rules; the whole initiative lies in the hands of private businesses.

- Rules of self-regulation by an association where the rules are created by the association to represent a business or an activity.

- Negotiated rules of self-regulation where rules are drawn up by the association in collaboration with authorities, and bodies outside the associations are consulted as well.

⁷⁸ Directorate General Health & Consumer Affairs - DG Sanco
ec.europa.eu/consumers/

- Self-regulation as substitute to government regulations: Initiative lies with private businesses but government reserves the right to create rules if benefits of all parties concerned are not defended.
- Conditioned (or imposed rules of) self-regulation (one of the most effective alternatives for government regulation) : initiative lies with the market but government enforces a lawful agenda in which self-regulation has to function.

1.5 Instruments of SR

No single industry model for self-regulation is existent. A effective and operative instrument is designed according to market characteristics hence many instruments of self-regulation must be available. An attempt of classification was made by the UK National Consumer Council, who has identified 8 main types (unilateral codes, customer charters, unilateral sectoral codes, negotiated codes, recognized codes etc.), but they are, in fact, all codes of conduct along the broad spectrum of government involvement. The Dutch Ministry of Economic Affairs has recently authorized a stock-taking survey of self-regulating instruments. The study identified 22 instruments and classified them into clusters, and directed which instrument qualifies for the solution of a particular problem.

- Cluster 1: Technical instruments (regulation by technology)
- Cluster 2: Behavioral instruments (Codes of conduct)
- Cluster 3: Informative instruments (Seal of approval, certification, and recognition schemes)
- Cluster 4: Contractual instruments (Negotiated general terms and conditions)
- Cluster 5: Dispute settlement instruments (Arbitration, binding recommendation, mediation, and ombudsman)

The aforementioned self-regulation implements can be joined in diverse ways.

Later, we may see a combination of behavioral instrument (code of conduct), informative instrument (labelling) and dispute settlement instrument which is a way to ensure an effective self-regulatory mechanism.



2. THE CODE OF CONDUCT AS ONLINE SELF REGULATING INSTRUMENTS

Codes of conduct are the most renowned methods of self-regulation for the on-line environment, specifically ever since the EU made obvious references to them in their effort to legalize the information society. In their "European Initiative in E-Commerce" the European Commission indicated that "*business can increase the level of trust by implementing and abiding by codes of conduct... to win mass approval amid customers and businesses and avoid the creation of new barriers.*" This was subsequently laid down in the Electronic commerce directive where the drawing up of codes of conduct at *Community level* was encouraged.

The consumer connection

The reference to the "customer organization" was first revealed in the Electronic commerce ruling. This produced much disturbance with large business associations, but met with consent by the customer organizations. Van Driel in her 1989 dissertation stated that consumer participation is necessary for the success of a code of conduct. The Data protection directive affirmed the *preference for trade associations and other bodies*⁷⁹ to write codes of conduct as a way of participating in the proper application of EC law. To a certain extent earlier in the past, in 1992, the Commission Recommendation on codes of practices for the protection of customers in distance selling agreements, suggested that trade associations of suppliers should implement codes of practices. In agreement with this recommendation, the Distance selling directive proposes that the least compulsory rules should be supplemented by intentional preparations among merchants concerned. Thus we see that in the Internet age, codes of conduct are chiefly geared towards constructing trust and confidence for the customer.

⁷⁹ www.tradingstandards.gov.uk/cgi-bin/valeofglamorgan/con1item.cgi?...

2.1 Definition and Variation

Codes of conduct as self-regulatory instrument have been existent for a long time. One of the first Internet Codes of Conduct was the code on *Ethics and the Internet*, published in January 1989 by the Network Working Group of the ISOC. It enclosed elementary rules on rational conduct on the Internet. These rules, often implied, were then labeled “Netiquette”. The ICC Code for Advertising Practices was first published by the ICC in 1937 and has been modernized frequently. It laid the grounds for the progress of self-regulatory systems, such as the code utilized by the EASA⁸⁰ and the Dutch Advertising Code Foundation who is a participant in EASA⁸¹.

But what is a code of conduct? Similar to regulation where the norms are well-defined in “black letters”⁸² in self-regulation the code of conduct is used *to explain a series of norms explained by a proficient body and that, without having any explicit compulsory rules, has for purpose to systematize and lead the attitude of businesses.* The code of conduct is defined as behavioral self-regulation implement, i.e. how the “conduct” (or behavior) of an individual (company) or group should be. This is in proportion with the latest explanation of the European Commission as defined in the scheme for the Unfair Commercial Practices directive: *‘code of conduct’ means a contract which describes the behavior of the merchants who undertake to be duty-bound by the code with respect to one or more specific commercial practices or business segments.*

When seeking illustrations of codes of conduct the Internet search engine “Google” reimbursed 2 million hits. Variations appeared and codes are used to promote the business social accountability, preserve the honesty of a proficient group, relate to one company internally, or to a precise segment, or to a whole business, such as the Responsible Care® program, originated by the Canadian chemical manufacturers in 1985 upon the Bhopal incident, to self-regulate the chemical business and it was later adopted by 49 countries, noting that codes can be designed for Outer Space, Cyberspace, in an international, European or national context.

⁸⁰ European Advertising Standards Alliance

⁸¹ www.easa.com/

⁸² the written law

This behavioral instrument comes under many names such as the code of ethics, code of practice, or named a voluntary code, etc. Hence, *codes of conduct are fundamentally voluntary in nature*. Self-regulation is *designed to contribute to the proper implementation of Articles 5 to 15* of the Electronic commerce directive. voluntary industry code of conduct, written by industries (whether or not organized) is meant to self-regulate (all aspects of) doing e-commerce preferably at Community level.

2.2 A Properly Designed Code

Whether or not the consumer is asked when creating a code of conduct, it is well-defined that codes of conduct which are well considered and appropriately applied can assist to attain public interest objectives, be a focus for consumers and reduce supervisory and taxpayer problems to the profit of everyone. Codes can provide assurance to business and consumers, and can, especially, help SMEs who cannot have the funds for the charges of compliance lawyers. Nevertheless, an unwell planned code, unsuitably applied, or used in unsuitable situations, can truly do more damage than good and can lead to a loss of confidence with customers and business that can be problematic to overpower as recognized by the European Commission who initiated the E-Confidence enterprise in May 2000⁸³. A group of customers and business shareholders had been created to talk over key trust matters at risk, thus conversing prevailing self-regulatory patterns and fostering new ones. Several generic code models developed by governments and academics for consumer protection purposes or by consumer agencies

The following model codes of conduct and guidelines have been selected:

⁸³ ec.europa.eu/information_society/newsroom/dae/document.cfm?...

- *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999)* which are meant to assisting governments, businesses and consumer representative to develop codes of conduct.
- *E-Confidence, Guiding Principles for Generic Codes of Practice for the Sale of Goods and Services to Consumers on the Internet*, 2nd draft, 2001⁸⁴
- Selfregulation.info program (IAPCODE) of the Comparative Media Law and Policy Centre (2000 - 2003) funded by the European Commission under the Internet Action Plan to cover a wide range of self-regulatory codes in the area of Internet media
- Canadian Office of Consumer Affairs: *Voluntary Codes, a guide for their development and use (1998)* and *An evaluative framework for voluntary codes (2000)*
- UK: NCC (National Consumer Council) *Models of self-regulation (2000)*, providing a best practice checklist
- Australia: *Draft Guidelines for developing and endorsing effective voluntary industry codes, October 2003*, drawn by the ACCC (Australian Competition and Consumer Commission)⁸⁵

2.3 Preliminary Questions

Before starting to draft a code of conduct, we have to do a thorough analysis of nature, background and extent of subject to be regulated, if the code of conduct the most effective way to reach the desired objective? Are the objectives practical? What can and cannot be achieved?

- Consensus: the need for consensus amongst key players on subject, objective and scope of the code of conduct.

⁸⁴ www.mediate.com/articles/awiener5.cfm

⁸⁵ www.austlii.edu.au › [Databases](#)

- Scope and content: the extent to which something is already regulated by law, whether the scope of the code is national, regional (European) or international.
- Reason: a clearly formulated reason of the code of conduct: consumer or other market or public pressure, nature of “self-interest”⁸⁶ of the industries a real or perceived threat of new regulation.
- Actors and legitimacy of authors: a legal framework a decision should be made what actors should be involved in the drafting process: regulator, special industry groups, industry bodies (national, regional or international), SMEs, consumers and the existence and coverage of an industry association
- Finally, funding is important. Who will pay the code making, implementation, monitoring etc.

2.4 Spectrum of Government Involvement

Codes of conduct are often developed without help or supervision from government. Still the codes are existent within a legitimate framework. The jurisdictional and private law environment comprises customer fortification, health and safety, employment, environment, contract or wrongdoing law. A code can be planned to evade lawmaking, may be used to foresee legislation; may help to apply legislation; and may increase or supplement legislation, the tendency of European and national controllers is towards co-regulation, whereby the controller joins his power with the private sector, thus offering trustworthiness and devotion to the code of conduct. The spectrum of government participation ranges from no or little involvement.

Governments can act as:

- Catalyst and Facilitator: buoy up parties to discover voluntary methods and take into consideration the benefits of different concerned parties, produce encouragements to use a code, train and promote an understanding of self-regulation to industry and customers, and support international cooperation and harmonization. Government can provide facilities, information, advice and monetary help.

⁸⁶ www.ifac.org/.../publications/.../Defining-and-Developing-an-Effective-...

- Co-regulator: Supplier of framework rules, guidelines and controlling support to help attaining (regulatory) goals. Government can also recommend obligatory codes, or clearly validate codes, and provide a agenda to supervise obedience, guaranteeing that the code benefits all related shareholders.

2.5 Principals of Good Code Making

Self-regulation is regulation and has to follow rules. Codes make an analogous function as regulation, they try to set rules. To guarantee legitimate certainty, liability, proportionality and transparency when planning a code, the structure and codes of regulatory systems (“good law making”) have been taken as point of departure.

1. Rulemaking: the improvement of rules should be a self-ruled process, open, obvious, counseling and wide-ranging
2. Communication: rules must be known and related publicly
3. Monitoring and enforcement: obedience with rules and actions must be ensured in case of non-compliance
4. Adjudication: official decision-taking about penalties of nonconformity or settlement of disputes and complaints
5. Sanctions: imposing penalties in case of noncompliance, such as fines or imprisonment (this penal sanction is a prerogative of the State)
6. Evaluation and revision: regular evaluation and changes.

2.5 Framework for a Code

- Objective: The ECP model code was designed as broad outline to serve
(1) as example and source of inspiration for organizations in drafting their own codes of conduct for e-business and

(2) a checklist in assessing the degree to which contracts, general terms and conditions, and regulations help to increase trust and confidence in e-commerce.

- Consensus: to develop trust by focusing on reliability, transparency and confidentiality and privacy.
- Scope and content: Self-regulation in combination with regulation can create an effective level of trust when doing business online.
- Reason: a survey was conducted in 1998 on the scope of introducing a self-regulating instrument for e-commerce.
- Actors and legitimacy of authors: Code making was a process in which large and small enterprises, consumers and academics were involved during drafting.
- Funding: Membership of ECP.NL⁸⁷ is subject to a fee.

3. CRITICAL SUCCESS FACTORS

Now that an outline for a code has been created, we have to dedicate ourselves to schemes, which really deliver trust and confidence in the code. Several procedures available to communicate the code to potential consumers, implement the code by suitable ways, and provide satisfactory objection and heated discussion resolution prospects. Those procedures improve the efficiency of the code considerably.

3.1 A Closer Look at Enforcement

The success of self-regulatory measures like the code of conduct relies greatly on the operational implementation of the rules. Self-regulation, according to Geelhoed presumes satisfactory self-enforcement. Such enforcement comprises two levels : internally (against the members, in the form of

⁸⁷ ec.europa.eu/enterprise/sectors/ict/files/reply-en-ecp-nl_en.pdf

sanctions) and externally (against the public), whereby contractual and non-contractual methods can be monitored, depending on the obligatory nature of the code.

Internal enforcement

Internal: Membership to a subdivision or business association, or the society, who releases the code (SRO), is often exposed to a membership agreement. Enforcement and The European Commission identified seven codes on out-of-court arrangement: independence, transparency, adverse principle, effectiveness, legality, liberty and representation. For example, the Maghribi traders in the eleventh century imposed a commercial code by dismissing and retaliating against members found in violation. The vulnerability of such a method is that this cannot be done against those who did not join the association or the code. Positive implementation could be attained by competitive compensations for subscribers to the code. The most influential enforcement is, actually, a competitive market and the risk of government invention.

External enforcement

External: A corporate method of implementation is the insertion of the code in the overall terms and conditions. Non obedience would escort to a violation of contract. In case the code is not part of the contract, thus far only misdeed law remained. For customers, this might vary with the scheme for the Unfair Commercial Practices directive.

Cross-border enforcement

To prevent cross-border fraud, mainly on the Internet, and to fight against the scoundrel merchant, the OECD created Guidelines for defending customers from fake and deceiving marketable practices across borders, delineating an outline for global collaboration. Based upon these rules, the European Commission did not remain behind and create a scheme for a

Regulation on customer fortification cooperation proposed to enter into force in 2005.

The suggested rule is applicable to the Electronic commerce directive and the scheme for the Unfair Commercial Practices directive.

3.2 Trustmark

One of the most popular methods of connecting with prospective invitees of the website that the business they are trading with is reliable and obeys a code of conduct is done by trustmarks (or labels, web seals, trust seals, e-hallmark, etc.). Additionally, trustmarks can be used as a promoting instrument to be distinct from the rivalry that has no such label. A “trustmark” or “webseal” is a label (graphic display) on a website designating that a trader constrains to obeying with a number of best business practices. Similar to a code of conduct, a trustmark is an instrument that promotes confidence. Codes of conduct are often not supplemented by a trustmark, but trustmarks are continuously supported by certain kind of a code. Trustmarks have been around for some time currently. The most primitive online seals comprise TRUSTe (1997) and BBBOnline⁸⁸, both US based. In the following years trustmarks were created to verify a comprehensive series of subjects like confidentiality (like TRUSTe), security, good business practices along with heated discussion resolution. The consequential accumulation of trustmarks complicated industries and customers equally.

Which trustmark is reliable and which is a scam? An attempt to stop this chaotic progress was made by the European Commission with their E-Confidence scheme, objective was (inter alia) to find practical clarifications for trustmarks. Under this umbrella, a collaboration with BEUC (European Consumer Organization) and UNICE (European Employers' Organization) was introduced in 2001 to create an outline for an e-commerce trustmark scheme but it wasn't feasible. More attempts have been made to create pan-European labels (as called for by the Electronic commerce directive), but thus far they flunked to develop.

One of the European trustmarks which is effective, is Euro-Label, supported by a European Code of Conduct, created by EuroCommerce, the European Association for retail, wholesale and international

⁸⁸ www.sans.org/reading.../comparison-online-privacy-seal-programs_685

trade. While all trustmarks are directed towards creating customer trust and confidence, SMEs could really benefit from a deep-rooted trustmark, not only by locating it on their own website, but depending on a trustmark from another dealer when buying on the web. It is significant to have an operative code of conduct, which offers a trustmark for those who want to take part in the scheme. Indeed, it is debated that to obtain a trust mark might be the most significant motivation to abide by a code and apply its rules.

CHAPTER VI : PRIVACY IN E-COMMERCE

1. E-COMMERCE FRAMEWORK AND PRIVACY ISSUES

By the year 2000, there were many companies in the United States which got involved in e-commerce for the promotion of their businesses. The western parts of Europe too had gained much advantage of this system of trading and all of them began their first ever underlying websites for e-commerce. There was a huge change in the definition of e-commerce when the most successful enterprises of the world had involved in e-commerce. Since then e-commerce emerged as one of the best forms of trading.

After the definition of e-commerce in general it was the turn of b2b e-commerce definition that had the most importance as it was largely followed e-commerce techniques since the beginning. There were a number of companies who after discovering the round the clock stint of the Web had begun to sell their products to other companies so that they may reach the target customers more easily. This was when there was a new B2B e-commerce definition put forth.

2. CORPORATE MARKET VALUES

2.1 Corporate Practices

Privacy – the control over one's personal data – and **security** – the attempted access to data by unauthorized others – are two critical problems for both e-commerce consumers and sites alike. Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both. This chapter reviews the current state of the art and the relevance for privacy and security respectively. We examine privacy from social psychological, organizational, technical, regulatory, and economic perspectives. We then examine security from technical, social and organizational, and economic perspectives.

Privacy is a serious issue in electronic commerce, no matter what source one examines. Fisher [2001] reported "Forty-one percent of Web buyers surveyed last year by Forrester Research of Cambridge,

Mass., said they have contacted a site to be taken off their databases because they felt that the organization used their information unwisely. (pp. 20-21).” A Business Week/Harris Poll found that over forty percent of online shoppers were very concerned over the use of personal information, and 57% wanted some sort of laws regulating how personal information is collected and used [Harris Poll 2000]. Similarly, Culnan [2000]⁸⁹ argued that privacy concerns were a critical reason why people do not go online and provide false information online.

Why this concern about privacy? The answer is simple. As of 1998, the FTC found that the majority of online businesses “had failed to adopt even the most fundamental elements of fair information practices. ([Culnan 2000], p. 8).” Indeed, relatively few consumers believe that they have very much control over how personal information, revealed online, is used or sold by businesses [Culnan and Armstrong 1999]. The combination of current business practices, consumer fears, and media pressure has combined to make privacy a potent problem for electronic commerce.

Tackling privacy, however, is no easy matter. If nothing else, privacy discussions often turn heated very quickly. Some people consider privacy to be a fundamental right; others consider it to be a tradable commodity. Detailed arguments about the historical progression of privacy can be found, for example, in [Davies 1997] and [Etzioni 1999]⁹⁰. (Even these historical accounts have sharply differing viewpoints. For example Etzioni argues that privacy is societally illegitimate or infeasible, while Davies argues that it has become a squandered right.) For the purposes of this article, we will explore the potential space of privacy concerns, not privileging any particular viewpoint. In our view, both consumers and businesses may have legitimate viewpoints, sometimes conflicting. This is in the nature of most societal issues. We also restrict ourselves to the privacy issues that accrue in electronic commerce; we omit, for examples, the issues emerging from vehicle tracking chips, the wholesale monitoring of telephone and other communication mechanisms, and image recognition from public cameras.

⁸⁹ econ.ucsb.edu/~doug/245a/Papers/ECommerce%20Privacy.pdf

⁹⁰ world.std.com/~dtd/ec_handbook/ec_handbook_39.pdf

Culnan [2000], following Westin, defines privacy as “the ability of an individual to control the terms under which their personal information is acquired and used.” An individual’s privacy, as such, is always in an inherent state of tension, since it must be defined in conjunction with capabilities of others to transact business and even to control their own privacy. As Clarke [1999] noted, privacy may have to be traded off in certain transactions, such as the access to credit or to maintain the quality of health care. Indeed, societal needs may also transcend an individual’s privacy concerns, as in the case of public health.

Nonetheless, individuals as e-commerce consumers, even with its inherent tradeoffs, still wish to control their personal information. Goffman [1961] noted that people must control their presentation of self, their face, to others. People need to be able to control what others think of them, and find it disconcerting when they cannot. Even more, people find it disconcerting when the rules of everyday conduct appear to change, as they can with new technologies. In these situations, people may feel that they have been unfairly treated or that they have not received proper notice [Culnan 2000].

Besides “privacy”, a number of terms -- such as notice, choice, identification, digital persona, authentication, anonymity, pseudonymity and trust -- are used in privacy discussions. However, because of space limitations we cannot hope to carefully to define each. See [Clarke 1999] for a useful introduction. Note, however, that there is a vigorous research debate surrounding many of these concepts.

Why is privacy of concern to e-commerce? We believe this concern stems from a new technical environment for consumers and businesses, the resulting data flow with substantial benefits to businesses and consumers, consumer concerns in this new environment, and regulatory attempts to govern this environment. It is important to understand each one of these, and to understand the tradeoffs. Privacy as a business issue is extremely sensitive to changes in the surrounding context. Changes in people’s expectations (such as when they become accustomed to data transfer in

commercial settings) or in regulatory governance (such as new laws, governmental regulations, or even case law in the US) can dramatically alter business issues and possibilities.

Below is an overview of the research and business issues. This will include the consumers' concerns, technical issues, and regulatory attempts to ameliorate privacy concerns. In this examination, our attempt is not to predict what will happen or should happen, but to present issues to guide further research and business activity.

Clearly, there are many business opportunities in the changing technical environment. The use of digital systems allows data capture at a much larger rate and scope than previously; e-commerce sites could potentially collect an immense amount of data about personal preferences, shopping patterns, patterns of information search and use, and the like about consumers, especially if aggregated across sites. Not only is it easier than ever to collect the data, it is also much easier to search these data [Dhillon and Moores 2001]. New computational techniques allow data mining for buying patterns and other personal trends. These data can be used to personalize a customer's e-commerce experience, augment an organization's customer support, or improve a customer's specific e-site experience. The data are valuable for reuse, for example, in finding potential sales to existing customers. As well, the data are also valuable to aggregators (who may look for other personal trends and patterns) or for other types of resale. Indeed, reuse and resale are simultaneously both potential opportunities and problems. "Ironically, the same practices that provide value to organizations and their customers also raise privacy concerns (p. 5)." [Culnan and Armstrong 1999]

From the viewpoint of customers, many e-commerce sites have done foolish things with their customers' data [Fisher 2001]. Consumers' opinions in this have been confirmed by media stories of particularly egregious privacy failures and public relations nightmares. Broadly speaking, consumers are merely confirmed in their opinions by the media. As mentioned, few consumers trust companies to keep their data private. In one survey, 92% of respondents indicated that even when companies promised to keep personal data private, they would not actually do so [Light 2001].

Culnan and Armstrong [1999] make the argument that consumers have two kinds of privacy concerns. First, they are concerned over unauthorized access to personal data because of security breaches (see below) or the lack of internal controls. Second, consumers are concerned about the risk of secondary use – the reuse of their personal data for unrelated purposes without their consent. This includes sharing with third parties who were not part of the transaction in which the consumer related his or her personal data. It also includes the aggregation of a consumers' transaction data and other personal data to create a profile. Smith, Milberg, and Burke [1996]⁹¹ raise two additional concerns based on Delphi studies, general concerns about personal data being collected and concerns over one's inability to correct any errors.

Beyond the research literature describing a general anxiety (and its extent), there is some research literature providing more detail. A persistent finding, over several decades, is that it is fruitful to consider US consumers not as a general block but as consisting of 3 groups [Westin 1991]: privacy fundamentalists, the pragmatic majority, and the marginally concerned. These groupings have been consistent across studies (e.g., [Ackerman, Cranor, and Reagle 1999], [Spiekermann, Grossklags, and Berendt 2001])⁹². (Spiekermann et al. divided the pragmatics into those who were considered with revealing their identity and those who were more concerned about making their personal profiles available.) In Ackerman et al., these groups were 17%, 56%, and 27% of the sample respectively. Spiekermann et al. noted a larger group of privacy fundamentalists and fewer marginally concerned in Germany. The groups differ significantly in their privacy preferences and attitudes. The marginally concerned group is mostly indifferent to privacy concerns; privacy fundamentalists, on the other hand, are quite uncompromising about their privacy. The majority of the US population, however, is concerned about its privacy, but is willing to trade personal data for some benefit (e.g., customer service). Nonetheless, consumers still want adequate measures to protect their information from

⁹¹ www.acrwebsite.org/volumes/v31/acr_vol31_118.pdf

⁹² www.personal.psu.edu/sap246/Ackerman_group-cib-workshop.v2.pdf

inappropriate sale, accidental leakage or loss, and deliberate attack [Dhillon and Moores 2001]. In [Ackerman, Cranor, and Reagle 1999], the concerns of pragmatists were often significantly reduced by the presence of privacy protection measures such as privacy laws or privacy policies on Web sites

Another interesting finding, also quite persistent, is that there is a large gap between most people's stated preferences and their actual behavior ([Ackerman, Cranor, and Reagle 1999], [Spiekermann, Grossklags, and Berendt 2001]). While this is often the case in social studies [Bernard 2000], it is of particular interest here. It is not yet known, however, whether this gap is permanent, in that it is unlikely to change, or is the symptom of people's frustration with current technologies.

The next consideration is technology. A number of technologies have altered the current privacy debates. Clark [2001] divides the technologies in question into 4 groups. Clarke argues that there are technologies used for surveillance, the technologies for forming agreements (contracting) about the release of private data, the technologies for labeling and trust, and privacy-enhancing technologies (PETs).

The technologies for surveillance and for data capture are used by companies for business purposes, but they have the side effect of endangering personal privacy. These include generating data trails, data warehousing and data mining, and biometrics. Many of these technical mechanisms can lead to consumer profiles that "are no longer based only on the individual's dealings with a single organization, because their data is shared by multiple merchants.... [Clarke2001]"

Balancing these tracking mechanisms are privacy enhancing technologies (PETs), which attempt to defeat or neutralize the surveillance or tracking technologies. Basic PETs include cookie-managers and personal firewalls. Other PETs attempt to provide genuine anonymity, and include anonymous remailers (e.g., Mixmaster) and digital cash (e.g., ECash). An active area of research and development are systems to provide non-traceable identifiers (e.g., ZKS Freedom, AT&T Crowds, anonymizer.com, anonymous remailers). Yet other PETs, which Clarke calls "gentle PETs", try to balance privacy and accountability. These include systems to provide some level of pseudonymity, allowing users to hide

behind the pseudonyms but allowing actions to be traced back to a person if necessary. In addition, privacy seals (e.g., from TRUSTe or the Better Business Bureau) indicate that the company follows the privacy practices stated on their web site.

A new area of research includes the so-called labeling protocols, such as the MIT/World WideWeb Consortium's Platform for Privacy Preferences (P3P) [Cranor and Reagle 1998, Cranor2002, P3P 2002]. P3P allows sites to describe their data handling policies (P3P statements) and permits users to describe their preferences for releasing private data (P3P preferences). As sites label themselves with P3P and as user clients (such as Internet Explorer) handle P3P statements and preferences, it will be possible to create technologies to form contracts for the release of private data. Other technologies, such as those to help users understand contractual terms or even contract-related fraud, will also emerge. Ackerman and Cranor [1999] outline one such technology. Their browser-based agents watch for privacy violations, privacy scams, and the like on behalf of the user.

The final consideration is regulation. In this, we include the varying governmental attempts, whether by law or by decree, to regulate this new environment on behalf of their citizens. It also includes emerging legal precedents and case law for governing privacy in cyberspace. Currently, regulation is a warren of overlapping and conflicting attempts. Fortunately, these attempts are slowly consolidating. (Around 1997, it was thought possible that even municipalities might have their own, specific privacy regulations, holding ISPs and web services responsible for any violations.) Nonetheless, currently, there are wide differences between the United States and the European Union. To continue e-commerce, there has emerged a notion of "safe harbor"⁹³ internationally, although it is not known how long this will continue.

In the US, privacy is largely a matter of economics, with the admonition that caveat emptor is the rule for consumers. Once data are provided by an individual to an e-commerce or anyone else, all rights to

⁹³ export.gov › [Safe Harbor](#)

that data are lost. US consumers have no recourse, which may result in surveys' showing a lack of trust. A company can use that data in any way, including selling the data to third parties for subsequent reuse. There are, however, specific areas of greater protection, for example in medical records. In addition, the Federal Trade Commission (FTC), which regulates consumer and inter-state trade in the US, has taken upon itself to take particularly egregious privacy cases to court. For example, the FTC has taken large companies to court when they have violated their own sites' privacy statements. While many researchers and analysts (e.g., [Reidenberg 1999], [Culnan 2000]) have argued that self-regulation has largely failed, it is unlikely that there will be significant change under the current US administration. It is possible, however, that greater penalties may accrue to companies violating their own privacy statements.

In contrast, "Privacy rules are strikingly different in the European Union, and the differences threaten to hamper the ability of US companies to engage in transactions with European Union countries without risk of incurring penalties. Europeans must unambiguously give consent after being informed as to why the information will be used; this is not the case in the United States. According to European Union rules, consumers must be informed of the entity collecting the data, purposes of the processing, recipients of the data, and any rights they (the customers) have. Furthermore, one must ask for specific consent for "sensitive information" (person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, and sexual preference). Unlike in the US, European customers can have incorrect, or unlawfully processed data corrected, blocked, or erased, and consumers can even require that third parties who have seen incorrect data be notified.

The extent to which European Union privacy rules hold for companies is unclear. Technically, not only do the European Union rules apply to European Union citizens, they also apply even if the customer is outside the European Union if the data will be processed within the European Union. The onus is on the data user (i.e., the company or electronic commerce site), and the penalty can be the blockage of data transfers to the offending company. Currently, however, these European Union rules

are suspended for American and international companies, and little if any enforcement is occurring for European Union companies. Not even all European Union countries have complied As a “safe harbor”, which has been the point of contention between the US and European Union governments, US and international companies must merely embrace a substantially diluted version of the privacy standards.

Thus far, we have largely examined privacy from a sociological stance; that is, as socially constructed expectations and sets of norms and regulations. Privacy can also be as an economic good. There has been considerable research recently in examining a marketplace for personal data. A general analysis of markets for data, including personal data, can be found in [Shapiro and Varian 1999]. An example of potential economic mechanisms for privacy data markets, including negotiation protocols, can be found in [Cranor and Resnick 2000]⁹⁴.

Very recently, researchers have moved towards advocating approaches towards privacy that combines technology, regulation, and social change. The technologies may include economic mechanisms. Increasingly, privacy is considered a complex social phenomenon with interactions among new technologies, regulatory structures, and citizens’ perceptions of privacy and social norms. Reidenberg [1999] and Cranor and Reagle [1998] have argued that e-commerce privacy requires a combination of law and technology, and Ackerman, Darrell, and Weitzner. [2002] have argued that solutions for privacy must simultaneously consider technology, social structures, and regulation in a co-design space.

As mentioned, security is also a major concern for e-commerce sites and consumers alike. Consumers fear the loss of their financial data, and e-commerce sites fear the financial losses associated with break-ins and any resulting bad publicity. Not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved. We cover each in turn.

⁹⁴presnick.people.si.umich.edu/

CHAPTER VII : SURVEY RESULTS AND ANALYSIS

I used interviews of e-commerce experts as a starting point for my research. The main data were collected through series of interviews with different actors coming from various financial institutions. The target group for our research included: private banks, universal banks, consulting politicians experts in economy. The specifics of the financial sector – highly reserved character of the IT security policy, due to confidentiality issues -make quantitative research almost impractical: e-commerce applications managers consider this subject as too sensible strategically to accept answering general surveys. That is why our interviewed actors was limited to the three major banks in Lebanon Audi, Byblos ,and blom Banks. Then I applied content analyses to interviews results. The way the research was carried out can be depicted by the following figure

1. SURVEY RESULTS ANALYSIS WITH THREE MAJOR BANKS IN LEBANON AND MANY OF THEIR MANAGERS

The results of this study show that the information technology industry and regulatory bodies have much work still to do before electronic commerce achieves its full potential. In particular, the survey identified eight issues that need special attention:

1.1 TRUST

Security of payments is of paramount importance in the corporate acceptance, adoption and widespread deployment of electronic commerce. Developing countries cited low levels of credit card use and restrictions on using credit cards over the telephone as a problem in implementing consumer electronic commerce. Privacy ranked next among their concerns, followed by authentication – being sure of the identity and credentials of the party you are communicating with. Some three-quarters of

the countries that took part in the survey believe that improving trust is vital to the development of electronic commerce.

1.2 Technology

Although Internet technology is still relatively new in many markets, BANKS were confident that technical difficulties thrown up by a largely immature medium could be overcome. Respondents identified a wide range of technological barriers that need to be addressed. Top of the list was a need to make security systems more widely available and to ensure they are more widely used. Efforts to integrate electronic commerce systems with existing enterprise systems and the lack of internationally recognised standards covering such activities as transaction processing, security and authentication were also identified. Networking bandwidth was a prominent concern among developing countries, many of who are still developing basic telecommunications infrastructures

1.3 Workforce Issues

There was a strong consensus among BANKS members that people issues will play an important part in the development of electronic commerce. The shortage of skilled workers, a perennial problem for the IT industry, is the most important issue for the majority of respondents. The leadership of business executives was also called in question with a significant proportion of BANKS members believing that those who run enterprises are too averse to taking risks. Training and the cost of employing skilled workers were also high on the agenda, although there were some members who did not see the workforce as a stumbling block at all to the growth of electronic commerce.

1.4 Public Policy

As industry associations, BANKS members are closely involved in influencing public policy in their countries. Leading public policy issues highlighted by respondents included the development of standards for authentication that would ensure trading partners are legitimate; the impact on electronic commerce of the taxation of online sales and the confusion caused by conflicting international contractual and legal frameworks. Respondents also pointed to limits on the use of encryption by

governments concerned about national security and crime fighting. The ability of governments to influence the growth of electronic commerce is underlined by the fact that over 70% of BANKS members say public policy is critical to the growth of electronic commerce.

1.5 Taxation

Although taxation scores highly in the public policy arena, overall it is perceived as less of a barrier than any other issue related to electronic commerce. Local sales taxes are perceived as most harmful to electronic commerce. Despite a lack of clarity on taxation in many countries, the majority view was that taxes were not an important barrier to electronic commerce.

1.6 Business Processes

While new internet only businesses such as auction sites and share dealing services have been launched, the majority of organisations trading on the internet are established businesses that must integrate their electronic activity with existing business processes. The biggest problem, identified by the survey, is a fear of opening corporate systems to outsiders: both customers and suppliers. BANKS members also pointed to a lack of business models for newcomers to adopt. Respondents also identified the logistical challenges of the real time environment of electronic commerce and the need to be sure of quality business results from electronic information exchanges.

2. BARRIERS FACING ELECTRONIC COMMERCE

Unavailability of skilled workers Existing internal business processes10%Costs of implementation10%Emerging regulations in such areas as tax and privacy8%Insufficient corporate budget7%Other6%Limitations of technology1%No barriers to electronic commerce1%Lack of trust in or familiarity with electronic commerce26%Lack of understanding of electronic commerce21%

2.1 Trust Related Issues

From the start of its emergence as a commercial network in the early nineties, the trustworthiness of the Internet has been a key issue for both businesses and consumers. Trust still remains a significant

stumbling block in its development. Electronic commerce is global and its international reach means that participants must deal with unknown or anonymous individuals and companies. Being sure about the probity of these partners in what may be a fleeting business transaction is a significant problem.

The BANKS study identifies reliable systems for payment as the number one concern for parties wishing to engage in electronic commerce. BANKS members also identified other concerns such as the fear that the infrastructure is not secure enough to resist attacks or that personal or corporate privacy may be invaded. Respondents are well aware of high profile attacks that have seen household names on the World Wide Web overwhelmed by malicious hackers. Developing countries cited low levels of credit card use and restrictions on using credit cards over the telephone as a problem in implementing consumer electronic commerce by members.

Equally, however, BANKS members are aware that legitimate concerns over payments security and privacy must not be allowed to prevent the expansion of electronic commerce. Respondents were convinced that with effective initiatives from the private and public sectors electronic commerce could be a secure business environment.

3. TRUST EFFECT E- COMMERCE

3.1 Understanding Electronic Commerce

Fear, uncertainty and doubt is still an all too common reaction to electronic commerce, among those who see it as a threat to the status quo, or who do not understand it. Encouragingly, BANKS countries report a reasonably high awareness in their markets of electronic commerce. The majority of businesses (62%) and of consumers (55%) is moderately aware of online trading.

However, it is clear from the study that the jargon of the internet, the changing business models of internet companies and other novelties of electronic commerce such as sharing previously confidential information make it difficult for some executives to exploit the full potential of electronic commerce.

3.2 Technology Constraints

Security is the number one technical issue for BANKS members and one that is intimately connected with making the Internet more trust worthy. Just over one fifth of respondents said that methods to protect transactions and information are not available. Respondents mentioned difficulties with obtaining effective encryption devices, maintaining firewalls and the hacker culture among a number of security issues.

Information technology has always struggled to develop standards for fast emerging technologies that do not choke off growing markets. Electronic commerce is no exception. Differing standards especially in the finance area make it difficult to set up networks. Difficulties with standardisation also hinder the ready integration of electronic commerce with existing systems.

At present developing countries often lack the basic telecommunications infrastructure required to support electronic trading. In Latin America, for example, costs and technical difficulties are paramount.

4. COSTS IN E-COMMERCE

Adapting existing systems14%Building new systems and buying new products and services11%Finding and/or training new workers10%Cost of running dual systems or hybrid operations10%Don't know5%Addressing a changing corporate culture22%Changing business processes23%There are no cost barriers to the growth of electronic commerce2%Gaining technological expertise3%.

5. INTERNAL BUSINESS PROCESS IN E-COMMERCE

Employee fear uncertainty and doubt12%No internal business process barriers4%Other4%Logistical challenges of going into real-time environment18%Don't know4%Exchanging data will not ensure

quality business results4%Analytical challenge of turning data into meaningful information4%Few accepted business models in practice24%Fear of opening up corporate systems to business partners26% .

6. WORKFORCE BARRIERS AND GROWTH IN E-COMMERCE

Skilled workers swap jobs18%Skilled Internet workers assimilate poorly with business-driven culture7%Other2%Immigration restrictions stops access to skilled workers elsewhere5%Training of skilled workers to bring them up-to-date with technology is difficult15%Skilled workers too expensive4%No workforce barriers exist4%Shortage of skilled workers, regardless of compensation25%Risk averse nature of business leaders20% .

7. TAXES IN E-COMMERCE

Foreign taxes16.3%National or federal income taxes11.6%Other national or federal taxes such as excise taxes9.3%Local or state income taxes4.7%Local or state franchise or excise (non-income) taxes4.7%Local or state payroll and employment taxes4.7%Local or state business personal property taxes2.3%Don't know2.3%Local or state sales and use taxes16.3%Taxes are not a significant barrier to electronic commerce25.6%Other2.3% .

8. PUBLIC POLICY BARRIER IN E-COMMERCE

Conflicting international contractual and legal frameworks16%Limits on the use of encryption10%Privacy restrictions on the availability and use of information10%Lack of clarity on public policy10%Regulation by national telecoms authorities9%Lack of strong copyright laws6%There are no public policy barriers1%Tax issues relating to Internet sales17%Authentication standards to ensure businesses and customers are legitimate20%Don't know1%.

8.1. State of Privacy Regulation

The Internet is rapidly moving from a period of experimentation and rapid expansion to one of consolidation as participants aim to set in place protocols that facilitate the conduct of business. So far, self regulation has been the model that has made most of the running.

In the US, the Clinton administration has opted for self-regulation on privacy. The only exception being sites targeted at children, which by law are required to gain parental approval before collecting data on young surfers under the age of 13. US trade body the Direct Marketing Association has introduced guidelines for online marketers that require them to notify visitors when third-party ad servers are collecting information during the visitor's time on that site. The companies should provide the names of the ad servers and give the visitor a link to the server to get more information. They should also give visitors the option to opt out of personally identifiable information exchanges. The DMA also provides a Privacy Policy Generator on its Web site that helps businesses create and post privacy policy statements.

In Europe, the privacy issue is more complex. European Commission ministers are attempting to reach agreement on a European wide legislative framework that would be adopted by all European Union members. The 15 member states have already declared their intention to introduce data protection and privacy legislation that would protect citizens by ensuring that suppliers provide tools to enable users to control the information that can be accessed about them. However, the situation is complicated by the likelihood that individual countries will introduce additional legislation in these areas. Germany, for example, plans to add its own electronic commerce laws to the proposed European Commission legislation.

European parliamentarians have established an independent, non partisan Internet policy think tank. The European Internet Foundation is comprised of more than 50 Members of the European Parliament and a large group of associate members, including some of Europe's biggest technology and Internet companies. The new organisation will focus on developing electronic democracy and making the Internet accessible and affordable for all Europeans. Elsewhere in the world many countries are

considering or have enacted legislation to regulate the Internet. Typical of government measures is Hong Kong's Electronic Transaction Bill, due to go before the state's Legislative Council late in 1999. Sponsored by the Department of IT Services, the bill seeks to establish certification authorities that will authenticate the identity of those involved in electronic transactions. The proposed law will make electronic commerce contracts legally binding by recognising electronic documents and digital signatures. Singapore has introduced two laws to regulate electronic commerce: the Electronic Transactions Act (ETA) 1998 and the Electronic Transactions (Certification Authority) Regulations 1999. They cover the validity of electronic documents and signatures, authentication of the identity of senders of electronic messages, integrity of transmitted documents, identification of the date, time, place of despatch and receipt, cross-border legal issues, and the liability of network service providers.

8.2. Internet Privacy Self Regulation Schemes

Along side efforts at public regulation, private initiatives to reassure Internet users have been gaining ground. Private sector self regulation is allowed in over two thirds of the countries covered by the BANKS Electronic Commerce Survey. So far, twelve of those countries have implemented industry schemes to protect privacy. Efforts at self regulation have proved effective in building trust in electronic commerce in many countries, although significant numbers have yet to see such measures having a major impact on consumer attitudes. Significantly, 18 BANKS members forecast that self regulation will become a viable alternative to government regulation within five years.

Certainly, commercial Internet sites are making a concerted effort to reassure customers that privacy is a top priority. A survey by Professor Mary Culnan of Georgetown University in the US found that two out of every three Web sites now have privacy statements or post information about policies for disclosing information to third parties. Of the top 100 electronic commerce sites world-wide, 94 percent of them let users know that they are collecting information on customers and say how they will use that information. Three quarters of those sites give users some control over how information gathered on users will be used

Many of the privacy policies adopted by individual sites are the result of the activities of industry bodies such as TRUSTe; an independent privacy foundation set up by the Electronic Frontier Foundation and the CommerceNet Consortium in the US. TRUSTe issues 'trust marks' to sites that adopt its principles and agree to abide by its rulings when disputes arise. In the UK, the Alliance for Electronic Business, a consortium of five trade associations including CSSA, has established TrustUK as a similar service to identify and brand sites with compliant policies and practices.

Arrangements for Security of Transactions and Access to Security Tools

While security is one of the most important elements in raising confidence in electronic commerce and ensuring acceptance among users, the tools to prevent unauthorised access to transactions, emails and Web servers are not readily available. Some 22 per cent of organisations polled in the BANKS Electronic Commerce Survey cited a lack of methods to protect transactions as the most significant technological barrier to electronic commerce.

Markets for Internet security software such as firewalls, encryption technology, antivirus packages, authentication routines and security administration systems have been growing apace. Proof of the demand for secure Internet traffic. However, security scares over widely used systems software such as Windows NT, coupled with a continuing threat from hackers have ensured that security concerns remain high on the agenda for most electronic commerce sites.

Even those with the highest levels of protection are not immune from attempts by hackers to gain access to confidential information. Rapidly changing technology makes it difficult for those responsible for security to keep up with developments, while access to reliable advice on appropriate security measures is difficult to come by, particularly in parts of the world where expertise in this area is at a premium. Ready access to effective security on the internet has been impeded by the open nature of the internet, by a determination by some governments to restrict access to the latest encryption techniques and difficulties in implementing security products that slow up internet

transactions. Competing standards for secure communications have also made it difficult for online traders to do business with one another in a secure fashion.

The encryption issue has been particularly divisive with the US seeking to restrict access outside its borders to encryption algorithms employing more than 64bit keys because of fears that the technology might be used by terrorists to conceal their activities. In general keys with less than 64bits are not considered strong enough to ensure secure communications.

In 1999, the US announced it would relax the restrictions. The Government decided to allow companies to export their strongest retail security software without obtaining individual licenses for each customer. Exceptions will be made for destinations in seven 'enemy' countries. Companies will still have to seek a one-time licence for their software and help the government track the sales of the strongest security products around the world.

Efforts to secure Internet communications have also run foul of government security agencies determined to maintain the ability to read encrypted communications. In the UK proposals to insist that users of encryption should lodge keys with trusted third parties so that government agencies could access them to decrypt intercepted messages were dropped only after heated debate.

Security will remain a key factor in the growth of the Internet for some time to come. A recent report issued by Rockbridge Associates, intended to measure consumer acceptance and confidence in various technologies, has revealed reluctance among many consumers to embrace electronic commerce, based partially on concerns over security issues. Consumers are worried about the privacy and security of their online transactions; more than half (58 percent) do not consider it safe to do any kind of financial transaction online. In addition, 67 per cent do not feel confident doing business with a place that can only be reached online, while 77 percent do not consider it safe to give out a credit card number over a computer, and 87 percent want their electronic business transactions confirmed in writing.

9. BANKS MEMBERS AND CUSTOMERS

Attitudes to Trans-Border Data Flows

Many countries are uneasy about the implications of the free flow of information and trade implicit in electronic commerce. Concerns range from a perception that the Internet may be used to destabilise governments through the threat it poses to local industries to potential loss of tax revenue. As a result some states, particularly in the developing world, have set out to restrict trans-border data flows by controlling who has access to services, by censoring content and curbing the activities of ISPs.

In an effort to facilitate trans-border electronic commerce, the Consumer Policy Division of OECD is drawing up guidelines for its member countries. The blueprint for online transactions has been two years in the making and addresses issues such as jurisdiction, collection of personal information and how complaints are handled.

In China, which has some 1.5m users online the Internet remains heavily monitored. In November of 1998, Beijing Telecom blocked out the BBC World News Service Web site and CNN is also banned in the country. Individuals have been prosecuted for distributing anti-government material on the Web. Elsewhere, Cuba has only this year allowed its citizens to access the Internet, while the citizens of other countries must make international calls to access Internet facilities.

However, trans-border data flows are also threatened by incompatible legislation on data protection. For example, a European directive that forbids the transfer of personal information to countries that do not provide similar levels of privacy protection could escalate into a trade dispute because of the restrictions that this puts on US companies. The International Chamber of Commerce has proposed the idea of a model contract that includes the concept for a 'safe harbour' for data. The model contract would enable US companies to access personal data from Europe provided they had agreed to observe European Union practices on data protection.

In the long run it seems unlikely that data flows will be impeded to any great extent. Both businesses and national governments are determined to participate in electronic commerce. They will not be able to do that if they erect legislative and regulatory barriers to the transfer of data.

CONCLUSION

Understanding how to present products and to safely deploy transaction processes is clearly a fundamental element in developing electronic business. Uncertainty over how best to do this explains why even Web sites run by some of the world's largest companies fail to exploit the possibilities to conduct business transactions effectively.

Respondents also highlighted a lack of familiarity with electronic commerce and low levels of understanding of the technology among both businesses and their customers. However, awareness of electronic commerce among the two groups was not seen as a major problem: half of both users and businesses are moderately aware of electronic commerce, while only 28 percent are not aware of electronic commerce.

The reasons for distrusting electronic commerce. security of payments and authentication are of paramount importance to the corporate acceptance, adoption and widespread deployment of electronic commerce in their region. It is clear that trading partners need reassurance of each other's true identity and to be more certain that payment, particularly across borders, can be executed securely. Developing countries cited low levels of credit card use and restrictions on using credit cards over the telephone as a problem in implementing consumer electronic commerce.

Although Internet technology is still relatively new in many markets, technology issues will only have a moderate impact on the development of electronic commerce. There was a strong consensus among companies that people issues will play an important part in the development of electronic commerce. Here the leadership of business executives was called in question with over a significant number of organizations believing that those running enterprises were too averse to taking risks. Less surprisingly, the shortage of skilled workers remains one of the key workforce issues. Training and the cost of

employing skilled workers are also significant, although there are some members who did not see the workforce as a stumbling block at all to the growth of electronic commerce.

Leading public policy issues highlighted by respondents include the impact on electronic commerce of the need for better authentication standards, the taxation of online sales and the confusion caused by conflicting international contractual and legal frameworks. Respondents also point to the limits on the use of encryption by governments concerned about national security and crime fighting. The ability of governments to influence the growth of electronic commerce is underlined by the fact that public policy barriers will either have a strong or moderate affect on its development.

Although taxation scores highly in the public policy arena, overall it is perceived as less of a barrier than any other issue related to electronic commerce. National or federal taxes are perceived as most of a threat to the conduct of electronic trade, followed by local sales taxes and then by excise taxes. However, the majority view is that taxes are no barrier to electronic commerce.

Although new Internet only businesses such as auction sites and share dealing services have been set up, particularly in the US, the majority of organisationstrading on the Internet are established businesses that must integrate their electronic activity with existing business processes. Here the biggest problem, identified by the survey, is the fear of opening corporate systems to outsiders. Linked to that uncertainty is an understandable lack of business models for newcomers to adopt. the logistical challenges of the real time environment and the need to be sure of quality business results from information exchanges as important business process barriers. So far as the software and services companies are concerned, changing business processes is seen as the most significant cost of expanding into electronic commerce markets. Addressing the issues of a changing corporate culture also scored highly in terms of financial outlay, while the cost of adapting systems, building new systems and buying new products and services are only of concern to a small number of respondents.

The costs incurred by members and their customers are likely to play a significant part in the development of electronic commerce. A third of respondents say that costs could strongly affect the growth of electronic commerce. Costs, however, both of technology and of the skills to implement it are beginning to decline as electronic features are incorporated into existing products and skills become more widely available.

The experiences of companies in convincing customers to adopt electronic commerce highlight some of the reasons for resisting the technology based market. By far and away the most significant objection to electronic commerce is a fear of sending personal information over the Web, followed by a fear of losing money by buying from unknown companies and the lack of regulation governing recourse procedures if things go wrong. Significantly, these complaints point to a need to solve the central issue for businesses: that not enough people understand electronic commerce.

Barriers to the full exploitation of electronic commerce are not insuperable. Awareness of the technology is growing rapidly. However, urgent action is required to counter the perception that electronic commerce is less trustworthy than conventional business methods. Efforts must be made to reassure users that their money is safe, that they can have redress when things go wrong and that their trading partners are trustworthy.

RECOMANDATIONS

Busnisses and banks recommend a number of steps to speed up the adoption of electronic commerce.

They are:

- Industry initiatives to devise standards and codes of practice for payment systems, privacy and consumer protection.
- Business leaders should be encouraged to take a proactive stance in promoting electronic commerce and to share their experience with others
- Removal of government barriers to the deployment of security systems such as encryption
- Establishment of training and educational programmes to increase the availability of skilled workers.
- Efforts to devise standard legal frameworks
- Promotion of schemes for authenticating users
- Public information programmes designed to reassure consumers.

In conclusion then, as I have previously stated e commerce is growing and changing at breath taking speed;however,Throughout this paper, one point should be remembered: there are no firm, legally binding international rules that apply to transactions done through electronic media. In fact today, 'buyers and sellers in different parts of the world have no legal framework for conducting their negotiations, making contracts, arranging for finance, transport or insurance on-line because most of the rules that apply to international trade still presume the use of paper." However, many national and international bodies are working on the legal aspects of this matter and, as in any business transaction; the domestic law of any affected country may become operative. Therefore, commercial laws of the

involved countries must be considered. In any event, businesses involved in international transactions should get legal advice from appropriate international practitioners as well as from specialists in the field of Commerce.

BIBLIOGRAPHY

- 1) Laudon, Kenneth C.; GuercioTraver, Carol (2014). *E-commerce. business. technology. society.* 10th edition. Pearson. ISBN 978-013-302444-9.
- 2) Chaudhury, Abijit; Kuilboer, Jean-Pierre (2002). *e-Business and e-Commerce Infrastructure.* McGraw-Hill. ISBN 0-07-247875-6.
- 3) Frieden, Jonathan D.; Roche, Sean Patrick (19 December 2006). "E-Commerce: Legal Issues of the Online Retailer in Virginia" (PDF). *Richmond Journal of Law and Technology* 13 (2).
- 4) Graham, Mark (2008). "Warped Geographies of Development: The Internet and Theories of Economic Development" (PDF). *GeographyCompass* 2 (3): 771. doi:10.1111/j.1749-8198.2008.00093.x.
- 5) Humeau, Philippe; Jung, Matthieu (21 June 2013). In depth benchmark of 12 ecommerce solutions (PDF).
- 6) Kessler, M (2003), "More shoppers proceed to checkout online", *USA today*, retrieved January 13, 2004.
- 7) Kotler, Philip (2009). *Marketing Management.* Pearson: Prentice-Hall. ISBN 978-81-317-1683-0.
- 8) Miller, Roger (2002). *The Legal and E-Commerce Environment Today* (hardcover ed.). Thomson Learning. ISBN 0-324-06188-9. 741 pp.
- 9) Nissanoff, Daniel (2006). *FutureShop: How the New Auction Culture Will Revolutionize the Way We Buy, Sell and Get the Things We Really Want* (hardcover ed.). The PenguinPress. ISBN 1-59420-077-7.246 pp.

- 10) Seybold, Pat (2001). Customers.com. Crown Business Books (Random House). ISBN 0-609-60772-3.
- 11) Business.gov <http://www.business.gov/>
- 12) Small Biz The Internet's big for small business <http://www.techweb.com/smallbiz/>
- 13) Ecommerce - Small Business Information Net Links Mining Co. Guide to: Small Business Information <http://sbinformation.miningco.com/msub57.htm>
- 14) Idea Cafe's Biz Directory: Starting & Running a Business Web directory to sites that help with starting and operating a business. <http://www.ideacafe.com/BCdir/bgstart.html>
- 15) Homebased Business Channel <http://www.homeofficemag.com>
- 16) SmallOffice.com <http://www.smalloffice.com>
- 17) SBFocus <http://SBFocus.com>
- 18) U.S. Small Business Administration <http://www.sba.gov>
- 19) SCORE - Service Corps Of Retired Executives - A nonprofit association dedicated to encouraging the formation, growth, and success of small business nationwide through counseling and mentor programs <http://www.score.org>
- 20) Microsoft Smallbiz <http://www.microsoft.com/smallbiz>
- 21) Mixed Reports on Small Biz E-Commerce By Paul A. Greenberg E-Commerce Times November 23, 1999 <http://www.ecommercetimes.com/news/articles/991123-3.shtml>
- 22) CNN network: Small business news <http://cnfn.com/news/smbusiness/>
- 23) Learning Fountains A monthly ezine on eBusiness&eCommerce for Small Business. Articles on website design, sales, promotion& linking; also technological trends <http://www.learningfountain.com/select.htm>
- 24) Chapter 14: ecommerce by Philip Greenspun, part of Philip and Alex's Guide to Web Publishing <http://photo.net/wtr/thebook/ecommerce.html>

- 25) Understanding E-Commerce: Strategic Fundamentals for Small Business and Exporters. A U.S. Foreign Commercial Service Seminar (via Webcast)
http://www.globalspeak.com/html/webcast_ecommerce.htm
- 26) Mergers & Acquisitions: On the Net--700 Links <http://whatsonthe.net/mergermks.htm>
- 27) eCommerce for Small Businesses Cost Comparison internet full service provider, marketingspecialists, websitehosting, websitepromotion, webdesign, search engine placement software, business opportunities, merchant accounts and anything else need to be successful <http://linz1.net/eCom10costs.html>
- 28) Small Business Barriers to Ecommerce
<http://cpaweb.com/newsletter/cpanow/dec98/sbbarwebcomm.htm>
- 29) How to market the small firm on the Internet Techniques for marketing and types of strategies small firms should be aware of <http://www.lawguru.com/seminar/index-promo.html>
- 30) E-Commerce: Niche Marketing on the Web Describes strategies for small business people to target market to specific groups of prospective customers on the Internet, and compete with the Wal-Marts of the world. <http://www.wilsonweb.com/articles/niche.htm>
- 31) Small and online business resources <http://www.onlinebizresources.com/>
- 32) easy commerce <http://members.tripod.com/easyCommerce/>
- 33) eCommerce Weekly <http://www.eweekly.com/news/news29.shtml>
- 34) Most publications do an inadequate job of covering smaller players and start-ups. However, Rafe Needleman at Red Herring's "Catch Of The Day" e-mail service fills the void in a major way. <http://www.redherring.com/>
- 35) E-Storefront Options for Small Businesses You need a fully functional commerce site for your small business and you need it pronto. Evany takes you through the different storefront apps you can use to make it so. 15 Jul 1999
<http://www.hotwired.com/webmonkey/99/29/index3a.html?tw=e-business>

36) eStats All the news web marketers and business people need to know -- the one-stop news clipping service that helps webmarketers keep up on the the latest happenings affecting business online. http://www.emarketer.com/estats/011899_challenge.html

37) <http://export.gov/safeharbor/>

APPENDIX

How ready are World Markets for Electronic Commerce?	Very Ready	Not Ready					
What are the Factors Affecting the Growth of Electronic Commerce?	Trust	Technology Limitations	Skills	Existing business processes	Public Policy	Costs	Insufficient Corporate Budget
What are the Most Significant Barriers Facing the Electronic Commerce Industry?	Trust Related Issues	Knowledge Related issues	Budget Related issues				
How strongly will Trust affect the Growth of Electronic Commerce?	Only slightly	Very strongly	No impact	Don't know	Strongly	Moderately	
What are the Most Significant Technology Issues?	Integration	Networking	bandwidth	Security			
What Costs are the Most Significant Barrier to Electronic Commerce?	Adapting existing systems14 %	Building new systems and buying new products and services11%	Finding and/or training new workers10 %	Cost of running dual systems or hybrid operations 10%	Don't know5%	Addressing a changing corporate culture22%	Changing business processes23%
How strongly will Costs Constrain the Growth of Electronic Commerce?	Only slightly	Very strongly	No impact	Don't know	Strongly	Moderately	
How Strongly will Costs hinder the Growth of Electronic Commerce?	Only slightly	Very strongly	No impact	Don't know	Strongly	Moderately	
What Internal Business Process Issues will affect Growth of Electronic Commerce	Employee fear uncertainty and doubt	Logistical challenges of going into real-time environment	Exchanging data will not ensure quality business results	Analytical challenge of turning data into meaningful information	Few accepted business models in practice	Fear of opening up corporate systems to business partners	No internal business process barriers